the engine of broadband wireless innovation

A Deliverable by the NGMN Alliance

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

next generation mobile networks

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

INTRODUCTION, GENERIC REQUIREMENTS, MODELING & TOOLING REQUIREMENTS

by NGMN Alliance

Version:	**1.4**
Date:	**2013-07-22**

Version:	**1.4**
Date:	**2013-07-22**
Document Type:	**Final**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Klaus Martiny, Deutsche Telekom**
Contributors:	**T. Benmeriem, Orange** **A. Buschmann, Vodafone D2 GmbH** **J.M. Cornily, Orange** **M. Geipl, Deutsche Telekom** **M. Mackert, Deutsche Telekom** **K. Martiny, Deutsche Telekom** **P. Olli, Telia Sonera** **B. Zeuner, Deutsche Telekom**
Approved by / Date:	**NGMN Board / 7th November 2013**

Abstract: Short introduction and purpose of document

NGCOR Phase 1 & 2 umbrella document containing chapters Introduction, Generic Requirements for Converged Operations, Modelling & Tooling and Appendix.

Document History

Date	Version	Author	Changes
2011/07/18	**V 0.92**	Klaus Martiny, Deutsche Telekom Axel Heck, Deutsche Telekom	1st Distribution to partners
2011/07/29	V 0.93	Andreas Buschman, Vodafone D2 GmbH	Some small changes in the FM section
2011/11/24	V 0.94	Yvonne Doernhofer et al	First compilation of updated sections: - Chapter 1 Introduction K. Martiny / M.Mackert DT - Chapter 2 - GENERIC REQUIREMENTS (GEN) A.Buschmann Vodafone D2 - Chapter 3 - HL REQUIREMENTS for CONVERGED OPERATIONS (CON) T. Benmeriem Orange - Chapter 4 - REQUIREMENT MODELING AND TOOLING (MT) B.Zeuner DT - Chapter 5 - REQUIREMENT FAULT MANAGEMENT INTERFACE A.Buschmann Vodafone D2 - Chapter 6 - REQUIREMENTS FOR INVENTORY MANAGEMENT P.Olli Telia, M.Geipl DT, M.Mackert DT - Chapters 7 & 8 – REFERENCES & APPENDIX
2011/11/26	V 0.95	Yvonne Doernhofer, Deutsche Telekom	Editorial Changes
2011/11/27	V 0.959	Manfred Mackert, Deutsche Telekom	Editorial Changes and distribution for review
2011/11/28	V 0.96	Manfred Mackert, Deutsche Telekom	Editorial Changes
2011/11/30	V 0.961	Manfred Mackert, Deutsche Telekom	Update with changes and comments from: • T. Benmeriem for chapter 3 (28.11.2011 and 30.11.2011) • M. Cornily for whole document (28.11.2011) • P. Olli for chapter 6 (30.11.2011)
2011/12/02	**V 0.97**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Editorial Changes in chapter 6 & Internal Review & Distribution to partners
2012/01/22	V 0.98	Yvonne Doernhofer, Deutsche Telekom	Changes FM (2.02) ,GEN part (1.02), InvM part (1.21), FM use cases, Glossary
2012/01/26	V 0.99	Manfred Mackert, Deutsche Telekom	Updates: Introduction, CON, InvM part (1.25); New: chapters 8.1. & 8.2.; editorial cons.: chapter 7 and complete document; Distributed for Final Review
2012/01/31	**V 1.0**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Updates from Final Review & Distribution to NGMN TAC for final approval
2012/02/28	**V 1.1**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update: Introduction with parts of MT Req abstract, FM chapter 5.5.2, Added comment in CON chapter 3
2012/02/28	**V 1.2**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update chapter 1 and 5
2012/04/16	**V 1.3**	Yvonne Doernhofer, Deutsche Telekom	Update REQ-MT (6), REQ-MT (8), REQ-MT (34); Add

			Editor's note for INVM requirements
2013/07/22	**V 1.4**	Thomas Kulik, Deutsche Telekom AG Klaus Martiny, Deutsche Telekom AG	Chapters CON and FM transfered to separate documents; Chapter INV was revised in NGCOR project phase 2 and also transfered to a separate document; numeration of chapters, figures and tables changed; smaller editorial changes Introduction updated by Klaus Martiny.

Contents

Figures

Tables

1 Introduction to NGMN NGCOR

The Telecommunication Market is changing faster and faster. The introductions of new technologies are going shorter and shorter. GSM, HSDPA and UMTS, well understood technologies but good examples regarding the change of customers needs, reflect the change from voice services to the usage of data services. Common to all these technologies is that the network architecture didn't change. The impact onto OSS was low.

With the introduction of LTE the requirements for OSS Capabilities and solutions changed completely. The network architecture became more flat. “Box” monitoring isn't the solution in order to deliver a high service quality to the customer. The challenge is to operate services with high quality, end to end, effectively and efficiently. Additional challenges are monitoring of the service and the introduction of new services. A shorter time to market is always requested.

But, unfortunately, the introduction of LTE as new mobile technology is not the only challenge. The convergence of mobile and fixed networks is another difficulty. The complexity of operating the network will increase dramatically.

Each operator has to consider that - in the same time - the mode of operation is changing. On one hand vendors are offering “Managed Services “ and on the other hand sharing of mobile infrastructure between the operators is becoming more popular.

As a summary the challenge for each operator is to operate their networks in the context of:

- Introduction of LTE (architecture change)
- Convergence of mobile and fixed line (considering various technologies e.g. WiFi, DSL, etc.)
- Change of mode of operations (sharing options (e.g. 3GPP TS 23.251), managed services)
- Heterogeneous Networks
- Considerations of currently implemented networks (GSM, UMTS…)
- New mode of operations e.g Managed Services, Cloud services, Cloud RAN, etc.

This forces operators to start a transformation process.

Considering that OSS solutions, interfaces and models are less standardized as detailed in the following chapter, it is not possible to efficiently and effectively run through this transformation process. Thus a prerequisite is to standardize at least the interface between the element management layer and the OSS layer and to harmonize the information models based on operations requirements.

The target architecture of each operator has to consider:

- Business processes based on industry standards (eTOM/ITIL) see Figure 1-1. The processes in Figure 1-1 are used in the project
- Standardized Interfaces
- OSS tools which are designed for operator specific demands
- OSS architecture see Figure 1-2

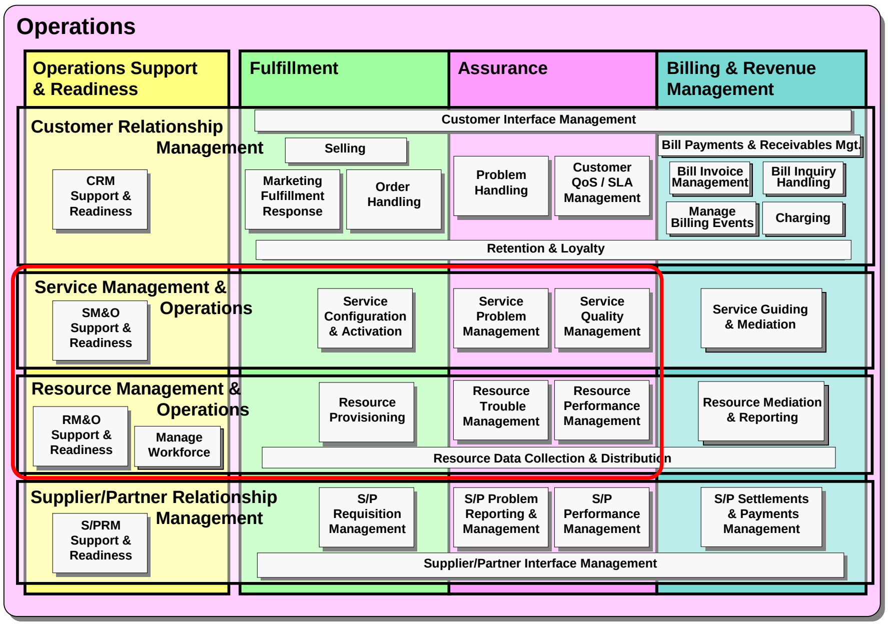


Figure 1-1: Business processes

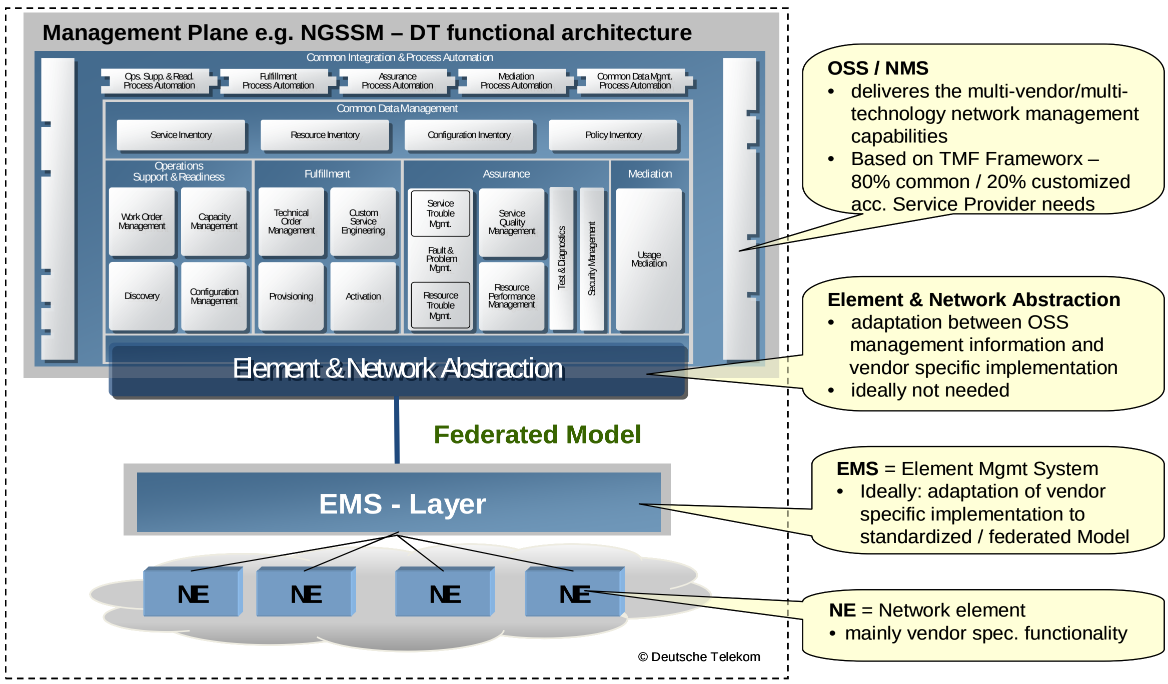


Figure 1-2: OSS architecture - agreed OSS Architecture: 80% based on Frameworx, 20% operator specific

Figure 1-3 defines the complexity of the project.

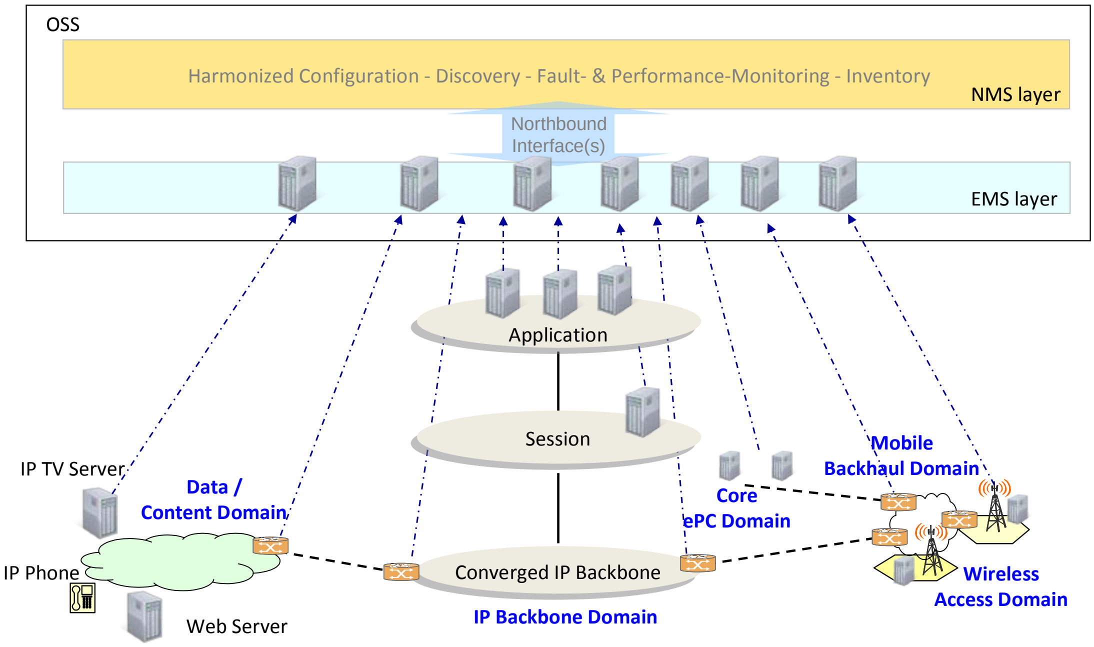


Figure 1-3: Operator's harmonized OSS, end-to-end network multi-domain, multi-technology management view

1.1 The current situation around standards for converged operations

3GPP WG SA5 has specified detailed Network Resource Models (NRMs) [13] for the management of mobile networks, plus a Generic Network Resource Model [9].

TM Forum has done the same for the management of various kinds of fixed networks, as well as a Shared Information & Data (SID) Model [25] providing a "common reference model for enterprise information that service providers, software providers, and integrators use to describe the network data", i.e., also generic definitions for network and service management aspects.

As a consequence the resulting models are different.

Parallel to 3GPP und TM Forum other Standards Development Organisations (SDOs) and organisations such as the Internet Engineering Task Force (IETF), International Telecommunications Union – Telecommunication Standardization Sector (ITU-T), Broadband Forum (BBF), Metro Ethernet Forum (MEF), etc., have defined different management standards/ recommendations for mobile and fixed networks.

Because all sets of specifications have been specified independently, the management of the mobile part and the fixed part is currently structured along silos with different management interfaces, information models, management architectures, and management workflows.

All these different Standards (from SDOs/ organisations) and proprietary solutions (from vendors) use different modelling/tooling, therefore the CAPEX and OPEX for network operators and integrators to integrate all these interfaces have increased dramatically. This heterogeneous modelling/tooling also has a massive influence to scalability, time to market, complexity and applicability of these standards in OSS.

The situation will be more challenged caused of the introduction of new technologies, network architectures or operations models like cloud, NFV, SDM or Managed Services solutions.

The convergence of mobile and fixed networks requires the convergence of the mobile and fixed OSS.

The network operators and the telecommunication industry would greatly benefit from aligned management interfaces, management models, management architectures, and management workflows.

1.2 The NGCOR Project and its Objectives

The Next Generation Converged Operations Requirement (NGCOR) project is approved by the board of NGMN.

The project is a continuation of the projects SON and NGMN Top OPE Recommendations from 2010. SON was focused on radio capabilities of a mobile network, NGMN Top OPE Recommendations specified operations requirement for mobile networks.

Converged operation is one key issue for each operator and service provider because the services will be delivered via a common infrastructure. There is no differentiation which platform (wireline or wireless) is delivering the service.

The current situation is caused by the fact that OA&M capabilities for wire line and wire less network elements are implemented by various different not harmonized standards or aren't standardized at all. Results are huge invests, high operational cost and slow time to market. The expected results from a standardization and unification of interfaces and information models are reduced OPEX and CAPEX and significantly shortened time to market. Without a higher grade of standardization an optimization of commercial figures isn't possible.

The results of both activities are considered in the NGCOR project since these results are essential for the converged management of a next generation mobile networks.

The NGCOR project was split in two phases. NGCOR I delivered the first document of Requirements for converged networks mid 2012. Fault Management, resource inventory management and requirements regarding an harmonized model where outcome of phase 1. The second phase is completing the area of operations requirements for converged networks. This includes requirements for configuration-, performance and service inventory management.

The result of both phases are merged in this set of documents.

NGCOR is an enhancement of OPE because NGCOR details specifications of operations requirements for both wire line and wireless networks. It is obvious that both networks will be merged in the near future. NGCOR is describing requirements for converged operations. It is not the intention to specify the convergence of wireline and wireless networks.

There is a need to define converged OA&M requirements to ensure that the operational activities within the converged networks perform optimally. The project has the claim to give guidance to SDOs and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work. Developing solutions for the most important requirements is the first and specifying the recommendations for the best solutions is the second target.

"An increasing number of service providers (SP) have to operate a variety of network and service production infrastructures, from mobile and fixed network environments up to converged networks and services across

many countries. The increasing demand to maintain and improve customer experience requires full end-to-end service management and hence, multi-technology and multi-vendor network management capabilities. On the other hand, financial downturn has put even more pressure on operational efficiency improvement."
[Source: Deutsche Telekom (DT), Orange (O), Vodafone (VF), BT, Portugal Telecom (PT)]

1.3 Expected benefits and commercial Impact

Currently Operators yearly spend millions of Euros for the adaptation and integration of the element managers with the OSS layer. The commercial impact is huge; from CAPEX- and OPEX-point of view, from an effort point of view to maintain the processes that are - caused by a low level of standardization - more complex as needed, and also from lost revenue due to long time to cash for new services.

One of the most significant changes in software development and procurement practice over the past decade is the greatly increased emphasis being placed on building O&M systems incorporating COTS software in order to keep overall development and maintenance costs as low as possible. Source of COTS software are the equipment vendors and OSS vendors who can supply off-the-shelf or COTS components that can be plugged into a larger software system to provide capabilities that would otherwise have to be custom built.

The rationale for building OSSs based on standardized interfaces and COTS OSS components is that they will involve less development time by taking advantage of existing, market proven, vendor supported products, thereby reducing overall system development costs and time to market for new services.

Having implemented the NGCOR project's main goal - the standardization of the interfaces between the element management layer and the OSS layer and the harmonization of the information models - a cost reduction of up to 70% is achievable. Not to mention the reduction of effort to maintain the OSS landscape and the reduction of process time. The NGCOR requirements are focused on northbound side of the EMS, means between EMS and the OSS/BSS layer. The southbound interface between EMS and the network elements are not in the scope.

The harmonization of at least the northbound interface is a per-requisite for the discussion about new operations models. The estimation of the savings from this way of system development and integration considers costs such as

- Requirements definition,
- Effort needed to understand and select the COTS software,
- Pre-integration assessment and evaluation - standardized and vendor specific,
- Design, code, test design and test - standardized and vendor specific,
- Post-integration certification of compliance with mission critical or safety critical requirements,
- Licensing and royalties and
- Software maintenance.

Savings are rapidly growing in a multi domain and multi vendor environment with a massively reduced number of integration points.

> Vodafone estimates that after the TM Forum Interface Program's RAM interface is adopted by the industry, it will save up to 68 percent in integration costs compared with vendor-specific integration.
>
> *TM Forum Case Study Handbook 2012*

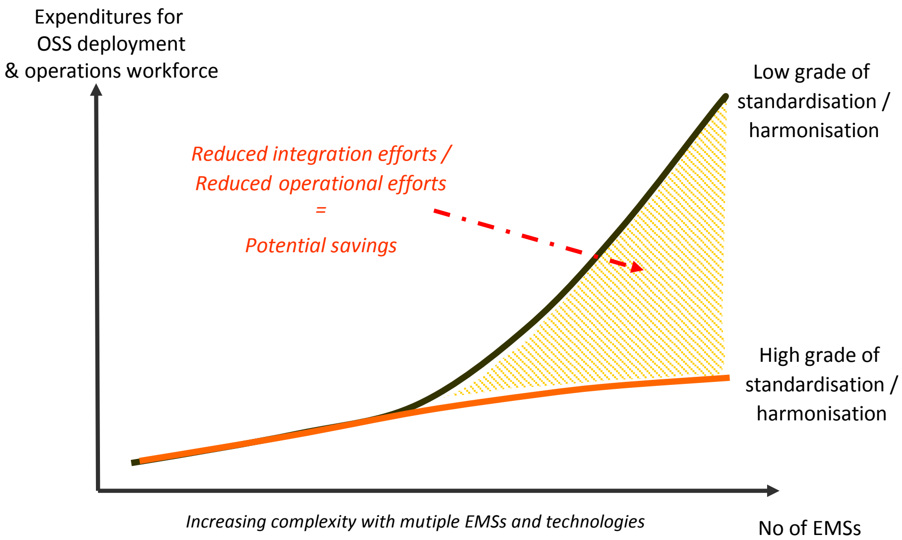


Figure 1-4: Savings through Interface standardisation and Information Model harmonisation

The effort reduction regarding optimized operations processes will be estimated with another 30% with:

1. Benefits from converged Fault-Management process

- reduced OPEX and improved service quality through improved fault qualification
- reduce time & efforts for network diagnosis, repair, extension and swap
- enable cross domain fault correlation and RCA
- shortened network outage time

2. Benefits from converged process for Inventory Mgmt. / Discovery / Reconciliation

- avoid time-consuming manual data collection process to represent “the truth” (Manual audits and commissioning are leading cause of rollout delays)
- Streamlined planning and decision making through complete and real-time visibility of multi-vendor / multi-technology network infrastructure
- reduce the no of “stranded” assets & circuits and costly investments
  RHK study: Typical Capacity Utilization is less than 70% (RHK),
  Recent Tier I audit: 16% of all routers in inventory were de-commissioned, redeployed, or non-existent
- faster time to market for new services
- avoid inflated maintenance charges from key hardware vendor, based on inaccurate installed base view (purchase records vs. actual ‘in use’ inventory)
- a proper inventory data base is a prerequisite for financial processes. Like depreciation, warranty management, etc. The management of financial processes based on proper inventory is crucial for each operator.

1.4 Methodology

The methodology applied to derive and deliver business requirements in NGCOR is relying on a requirements life cycle.

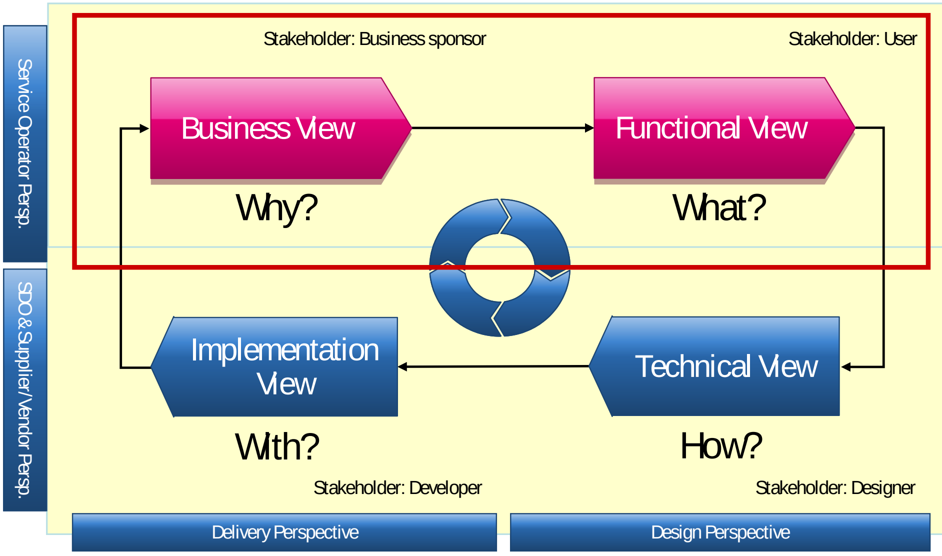


Figure 1-5: Requirements life cycle adopted in NGCOR & NGCOR focus area

Two responsibility areas / perspectives are defined in this life cycle:

- Service Operators perspective - focussing onto the business & functional view
- SDOs & Organizations - focussing onto the technical & implementation view

with a clear split between the service operator's perspective and the SDO & standardization perspective.

The requirements delivered by the NGCOR project are based on the business view (Why?) and the functional view (What?) of the lifecycle. The implementation and technical view isn't in the scope of the project.

The NGCOR requirements aren't independent from each other. The understanding how they are linked to each other is defined in the "business pyramid". The pyramid is shown in Figure 1-6: Business pyramid (general view).

- Business scenarios are the basis for architecture scenarios
- Inventory management is the common information base for the FCAPS processes
- For each process use cases are developed which are the basis for the requirements
- Inventory Management has a link to all Operations Processes

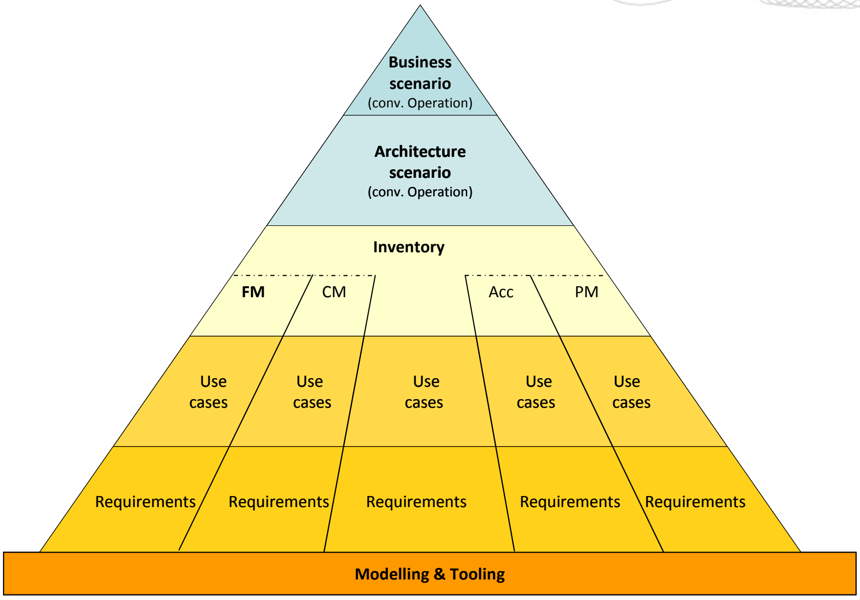


Figure 1-6: Business pyramid (general view)

The use cases are based on a template derived from the use case template defined in ITU-T M.3020 Management interface specification methodology. FM, CM, Inventory and PM based on the description of Business Scenarios.

Usage Scenario Id	<US_<SDO>_DDD_N>
Usage Scenario Name	
Summary	
Actor(s)	
Pre-Conditions	
Begins When	
Description	<Step 1> <Step 2> … <Step n>
Ends When	
Post-Conditions	
Exceptions	Put a reference here to a document or a separate table which lists all the exceptions. Specific exceptions will be explicitly listed in the Description clause.
Traceability	Hyperlinks to the associated requirements

where:

- <SDO> denotes the SDO / organisation
- DDD denotes the specification
- "N" is a 4 digits integer (e.g. 0012).

1.5 Project scope

The answer to the question “what is in and what is out of the project’s scope” is highlighted in Figure 1-7

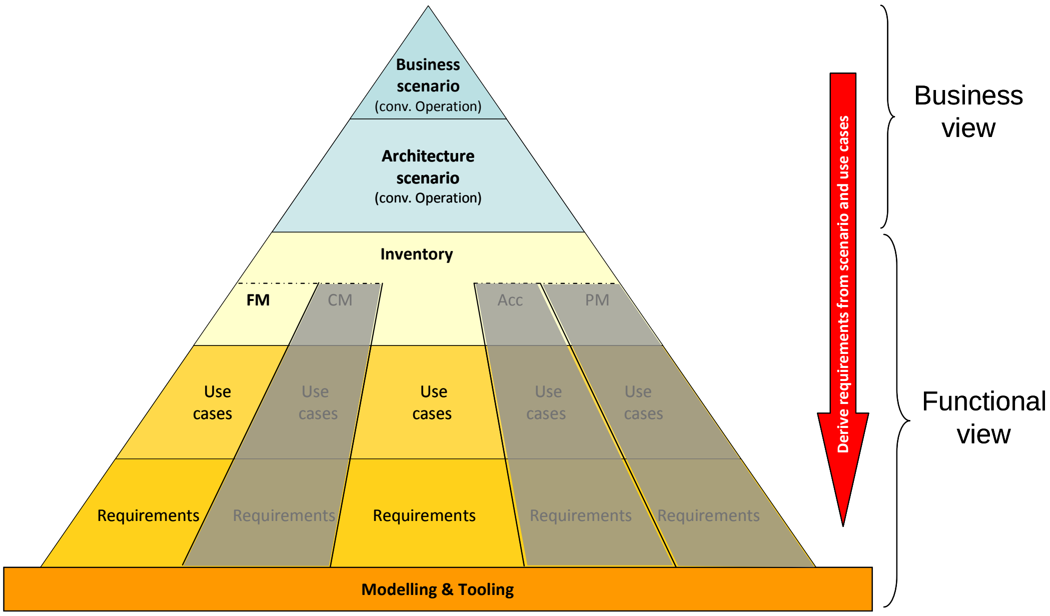


Figure 1-7: Business pyramid (specific view)

The requirements built up in the NGCOR project are derived from use cases that themselves are triggered by **Business Scenarios** and **Architecture Scenarios** which are described in Chapter 3 - High level requirements for Converged Operations (CON).

Base for the standardisation processes are the definitions which are described in the **Modelling and Tooling** chapter and that should give guidance to SDOs/organisations and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work.

In general the operations tasks of service providers are well described and defined as a part of the ISO Telecommunication Management Network

- Fault Management
- Configuration Management
- Administration/Accounting
- Performance Management
- Security Management

together well known as FCAPS. Except Security all other FCAPS are converged in the existing document

The project in its actual shape is focussing on the management domains **Fault Management** and **Inventory Management**.

1.6 The NGCOR document structure

The chapters in the set of NGCOR documents are structured as follows:

This document:

- Chapter 1 - Introduction to NGCOR
- Chapter 2 - Generic Next Generation Converged Operational Requirements (GEN)
- Chapter 3 - Requirements for NGCOR Modeling and Tooling (MT)

Complementary requirements for the topics listed below can be found in separate documents:

- Chapter 4 - High level requirements for Converged Operations (CON)
- Chapter 5 - Requirements for Fault Management Interface (FM)
- Chapter 6 - Requirements for Configuration Management (CM)
- Chapter 7 - Requirements for Performance Management Interface (PM)
- Chapter 8 - Requirements for Resource & Service Inventory Management (INVM)
- Chapter 9 - Business Scenarios for Network Sharing (BSNS)

This document:

- Chapter 10 - References
- Chapter 11 - Appendix with Glossary and Abbreviations and a summary of the NGCOR Requirements and their Addressees

2 Generic Next Generation Converged Operational Requirements (GEN)

2.1 Introduction

The GEN section contains the generic part of the Next Generation Converged Operational Requirements (NGCOR), which are valid for all other specific NGMN NGCOR sections. The intention of the GEN section is to avoid redundant requirement descriptions in different NGMN NGCOR sections.

2.2 Scope

Generic requirements for interfaces in the OSS domain.

2.3 Methodology

Explanation of Prioritization

Essential	→	The standard must fulfil this requirement. It is absolutely necessary and indispensable.
Major	→	The standard should fulfil this requirement. This is an important requirement. The value of the standard is reduced, if it cannot be fulfilled.
Minor:	→	The standard can fulfil this requirement (but must not). This is an optional requirement.

2.4 Non-Functional Interface Requirements

The following topics describe core business driven requirements for interfaces in the OSS domain. The following figure provides the overview.

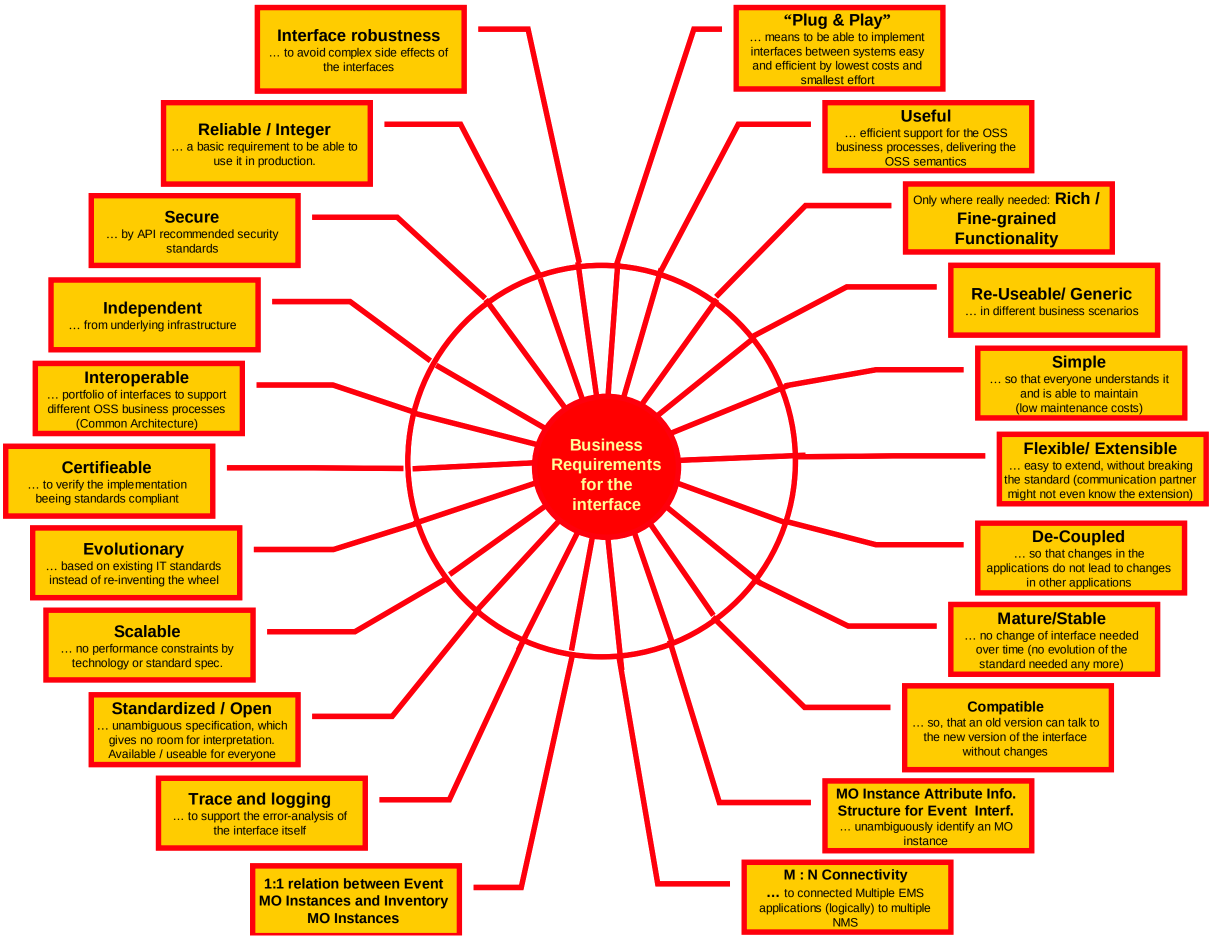


Figure 2-1: Business requirements for the interface

"MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interfaces

REQ-GEN (1) "Plug & Play"

It must be possible to implement the interfaces between the OSS easy and efficient by lowest costs and smallest effort (ideally without any development and/or configuration). The standard specification must enable "Plug&Play" (e.g. by unambiguously defined interface capabilities)

- Comment: Backward compatibility (see related REQ-GEN (13)) is one major prerequisite to support this characteristics during the whole life-cycle of the standard interface (e.g. plug & play must be still possible, if the client of the interface uses version 1.0 and the server uses version 1.2 of the same interface specification)
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (2) Useful

It must deliver efficient support for the OSS business processes. The standard specification interface must deliver the needed OSS semantics to support the process.

- Implementable (not academic) support of business process frameworks (e.g. eTOM and ITIL, or other process frameworks) and common information models (e.g. SID semantic, or information models from other SDOs)
- Clear and unambiguous scope of the interface (e.g. to differentiate from Service Inventory), without mixing different business scenarios (e.g. an interface which supports Resource Configuration Management should not be mixed with a Resource Fault Management Interface, because this might lead to complex interface specifications and expensive implementations)

Priority: Major

REQ-GEN (3) Re-Useable/ Generic

The standard interface specification must be generic enough, to enable the re-use in different integration scenarios.

(e.g. NMS - FM offers a standard interface for communication with other NMS such as trouble ticketing)

- This is a prerequisite to support M : N integrations and to reduce cost and effort for integrations
- Extensions in future versions will not hinder to implement it in a generic way and will not hinder to re-use (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (4) Simple

The standard interface specification must be simple (that means: the interface should offer only really necessary capabilities), so that people which have not been involved in the specification are able to understand it (or even do not need to understand the details), so that they are able to implement, maintain and use the interface.

- This will help to reduce cost and effort for the implementation and the operation/maintenance of the interface.

Priority: Essential

REQ-GEN (5) Flexible/ Extendible

The interface can be extended and refined, from basic setup to more complex implementations without impact on the other communication partners. It must be possible to extend the interface capabilities (methods and attributes), without breaking the standard. The standard interface specification must enable this capability to deliver standard compliant flexibility and extendibility.

- It must be possible to use a very simple, basic setup of the interface-implementation on one side of the communication partners, and a more complex interface-implementation on the other side of the communication partners (which contains the "simple" interface-implementation as the basic core) without disturbing the communication. That means, that there is a stable basic core, which can be extended and optionally used, but there is no dependency on all communication partners to use the extensions (as long as it is not part of the common standard itself).
- (The communication partner might not even know the extension, e.g. the server uses extended attributes, while only a small number of clients are aware about the extension → The interface still works as specified, without any impact on the clients which do not know the extension.) (Proposed solution: This will be supported by modular applications. A common module should be applied to all systems. Any specific requirements (customer or system specific requirements) should be expanded in separate modules without changing the generic/common module)
  (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Rationale

- Avoid strict coupling of server and client. But, at the same time, enable complex interactions, to support complex Network behaviour.
- This capability can be used to implement new versions with extended capabilities without loosing backward compatibility.

Priority: Major

REQ-GEN (6) Fine grained (as far as needed)
Means: Focus on using valid Use case to motivate the interface design. In such case, the standard Interface specification will be of the correct grade of grain.

Fine grained functionality ONLY where really needed and absolutely necessary to support the common basic process. Adding more and more capabilities into the standard interface specification will lead to complex and expensive implementations (which often hinders the adoption of the interface) and might lead to a dilution of the scope of the interface and overlapping functionality with other interfaces.

- Fine grained/ rich functionality must be delivered in specific areas to address e.g. technology specific requirements (e.g. in case of Resource Configuration Management)
- BUT: consideration of the richness to support the business process in an appropriate way vs. business benefit for all standard interface implementers.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (7) Standardized/ Open

The requirement means, that we need an "unambiguously standardized specification" without room for interpretation (which usually hinders Plug & Play, s.o.). This standard can be an existing specification or a new one. NGMN-NGCOR will not specify any standard. The specification and everything needed to make use of the standard (e.g. appendixes to the specification-document which are not part of the document itself, etc.) must be freely available and useable for everyone.

- This is a prerequisite to enable compatibility between interface implementations of different vendors.

Priority: Essential

REQ-GEN (8) Mature/ Stable

The standard interface specification must be stable and mature, to avoid expensive changes on implemented interfaces.
(Ideally there is no requirement for change on the standard interface specification any more).

- Prerequisite: The standard interface specification has to be fault–free before it is released to the market.
- This helps also to avoid backward incompatibility by avoiding continuously changing interface specifications.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (9) De-Coupled

Changes in the application or in the interface implementation at one of the communication partners may not lead to the need for changes in the application or in the interface implementation of the other communication partners. (Please consider that this requirement does not assume any specific type of implementation technology.) The standard interface specification must enable this capability.

- This is a prerequisite to ensure that changes in one OSS will not impact other OSS, to avoid dependencies between OSS applications which might lead to high costs for the impacted communication partners and to enable M : N integrations.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (10) Evolutionary

OSS standard interface specification shall re-use already existing, widely adopted and mature IT standards (e.g. transport protocols) to avoid "reinventing the wheel".

- This will reduce cost and effort to create and to implement new technologies.

Priority: Major

REQ-GEN (11) Independent

The interface standard specification must be independent from underlying infrastructure. The standard must be agnostic to the implementation-platform (e.g. the standard may not rely on capabilities of a specific Operating System).

- This will allow to re-use the same interface implementation in different environments, without dependencies on vendor specific capabilities, (e.g. the specification has to be independent from hardware, operating system bus environment, etc.) to avoid costs for the customization of interface implementations due to environmental dependencies of the specification.

Priority: Essential

REQ-GEN (12) Certifiable

The Interface must be specified in a way that makes it technically possible to validate an implementation compliancy. Beside of that, the standard should include a mechanism to certify the standard compliancy of the interface implementation

- This will allow the verification that the interface implementation is compliant with the standardized interface specification to avoid compatibility problems between interface implementations of different communication partners.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (13) Compatible

It must be possible to implement a new version of an interface specification at one of the communication partners while the other communication partners still use an old version of the interface specification. This “mixed versions” of interface implementations can be used without any impact on the communication partners or the interface implementations of the communication partners. The standard interface specification must enable this capability.

- The implementation of the new interface version at one of the communication partners must ensure the compatibility with the former version of the interface specification.
- This will allow to implement new interface versions in a productive environment without the cost and effort to upgrade all other communication partners (a real business need might lead to the upgrade sooner or later, but this can be decided by the owner of the “old” communication partner itself. Immediate upgrades are often difficult or simply impossible).
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Essential

REQ-GEN (14) Interoperable

The interface implementation shall be based on an interoperable portfolio of standard interfaces/ interface specifications to support different dynamic and configurable OSS business workflow and processes using a common architecture and a common information model. The standard must enable this by delivering the standard portfolio of interfaces and interface specifications

- This will allow the implementation of complex business scenarios, spanning different integrated OSS applications, using a common, well known interface environment without complex mapping of information models.
- (See also TMForum TR 146 Lifecycle Compatibility Release 1-0[1] chapter 3.2.2 : consideration of the approach to the requirements in TR146 chapter 3.2.2 may help to refine and better understand this requirement)

Priority: Major

REQ-GEN (15) Scalable

The standard interface specification must be able to be enlarged to accommodate a growth of traffic.

- The interface specification must enable the accommodation of traffic growth
- The specification or the selected implementation technology may not result in performance issues.

Priority: Essential

REQ-GEN (16) Secure

The standard interface specification has to be able to ensure confidentiality, integrity and availability of the data, which is transferred by the interface.

Priority: Depends on the type of the interface

REQ-GEN (17) Reliable

The interface implementation has to ensure the reliability of the data, which is transferred by the interface. The standard interface specification must enable this capability.

- This is a basic requirement to be able to use an interface in a productive environment.

Priority: Essential

REQ-GEN (18) Interface Robustness

No interface dependencies on availability between NMS and EMS if one of the EMSs (Server) communication partners is not available. The standard interface specification must enable this capability.
Description

- An outage of one or more EMSs (source) may not lead to any impact on the connectivity between NMS and other EMSs.

Rationale:

- Avoid complex behaviour of the interfaces. The interface to the remaining EMSs must still be available during the time then one or more EMSs are down.

Priority: Essential

REQ-GEN (19) Simple Trace and Logging

The standard interface specification must deliver a simple "trace and logging" functionality (in readable text format).

Description

- The standard interface specification must allow logging of all commands (send, receive, query, etc.), including the content in simple, human readable text format (no hex or binary, etc.) to support the error-analysis of the interface itself.
- The logging/tracing functionality is configurable.
- The level of details can be configured
- All attributes of the content can be used as to configure trace– masks
  Masking of attributes
  Masking of attribute- content
  Logging of interface problems/ errors

The standard should define a technology neutral log (perhaps much simpler than standard COTS products) and then map this simple log to various technologies (to be implementation neutral)

Rationale:

- The goal is to enable the operator/administrator to restore a connection problem on the interface very quickly.

Priority: Essential

REQ-GEN (20) 1:1 Relation between Event MO Instances and Inventory MO Instances

Description

- If MO identifiers used/provided by the inventory component of an Element Manager need to be mapped to meet naming requirements of the inventory database, the same mapping must be applied to the MO identifiers in the event. The corresponding is true if mapping is driven by event naming requirements.
- If MO identifiers of events and inventory within an Element Manager are different, the difference must be eliminated before the above mapping can be applied.

Rationale

- MO identifiers used in Event Management Interface and used in Inventory Management Interface must be identical if they are used to identify the same MO instance. The intention of this requirement is just to avoid, that the EMS uses a different NE name for the interface to NMS-Inventory/Config as for the FM interface. This will help to ensure that there is no misalignment of NE-name between NMS-Inventory/Config and the NE-Name used in the EMS –Alarm.

Priority: Major

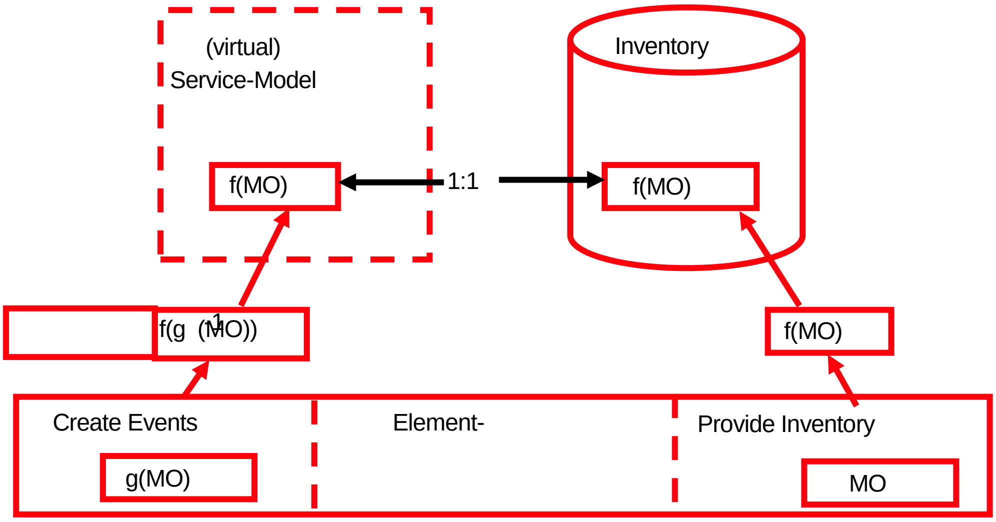


Figure 2-2: Managed Objects in the Context of Service Model and Inventory

REQ-GEN (21) "MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interfaces

<u>Description</u>
MO Identifiers carried or used across the Interface (e.g. used in protocols or used in models) must unambiguously identify an MO instance (that is a representation of HW, SW or any other entities as the case may be) The main goal of this requirement is to ensure a clear identification of the entity, by avoiding complex object structures, which usually drive complexity and costs/effort to implement the interface without real additional benefit.

- The managed object, as an attribute of the event – object, shall not contain any detailed topology information. The assumption is that the NMS will use an inventory database (internal or external) to map between Managed Object Instance and inventory topology tree if needed.
- The basic assumption for this is that there is a one-to-one mapping between Managed Object Instance and the inventory information, so that the instance can be unambiguously identified. If this is not the case, the instance must contain a very simple and standardized methodology to describe the relationship between the first unambiguously identifiable object and the related not-unambiguously identifiable object, which is the originator of the event. One illustrative example to "If there is no one-to-one mapping". Let's assume we get a port – alarm. The port identifier might not be unambiguous (just "Port_1". Different NE's [e.g. Router] might also have Port 1). So there must be additional information in the identifier, which shows the relationship between this port and the unambiguous NE identification where the port is located. Example: Router_XYZ<->Port_1 (assuming that "Router_XYZ" is an unambiguous identification)
- NMS requirement (specific for the NMS layer): As soon as the event information leaves the area of Service Provider 1 (e.g. Network Provider 2 needs that information as well) and (assumption) the Managed Object attribute value does not deliver unambiguously any more, the Network Manager will add additional information, the "NameSpace" - string to the Managed_Object_Identifier attribute (Proposal: Company_Name + Technology-Domain → "Access"), so that it is unambiguous in the larger context again. (Remark: The name of the EMS should be part of the "additional information" attribute, and not part of the MO_ID)
- So the structure must be as simple as possible. Here the <u>**illustrative proposal**</u> for a general proposed structure of the "Managed Object Instance" attribute:
  Managed Object Instance::= <NameSpace.>*<MO_Name> <;MO_Detail>*
  NameSpace::=<Global IdentifierString> (see NMS Requirement above)
  MO_Name ::= <Ressource_Name>|<Inventory_Name>
  The Ressource_Name is delivered by the Ressource or the EMS itself.

Example:

- Inventory_Name::=<Hostname>|<Service>|<Serviceelement>|<ResourceGroup>|<UseCase>|<UseCaseSubtype>| ...
- MO_Detail ::=<Blocknn>|<Racknn>|<Slotnn>|<Portnn>|<IP_address>|…
  (The MO_Detail information is delivered by the resource or the EMS itself. It adds information about the detailed origin of the alarm as far as this is known by the resource or the EMS. There is no limit on the number of topological elements, but it should be limited to an absolute minimum, just to the number which is really necessary to unambiguously identify the defective component.

Priority: Major

REQ-GEN (22) M : N Connectivity

Multiple EMS applications might be connected (logically) to multiple NMS applications (M : N)

Description

- The standard interface specification allows connecting multiple EMS to multiple NMS. (This might have an impact on addressing – mechanisms in the interface-implementation).

Rationale

- This capability allows reducing the effort for the maintenance of several different server- side interfaces.

Priority: Major

2.5 Use Cases

The related Use Cases are covered in the separate documentation for the Fault Management (FM) topic. Please consider that not all requirements are related to a specific Use Case in this document, because some of them are business requirements without a concrete technical implementation (e.g. generic requirements, like “Standardized”, “Mature”, “Useful”, etc…).

3 Requirements for NGCOR Modelling and Tooling (MT)

3.1 Introduction

3.1.1 Background for Modelling and Tooling

The main important future O&M requirements are specified and defined in the NGMN Top OPE Recommendations. Those requirements will need further enhancement with more details for guiding towards well standardized interfaces and interworking solutions throughout O&M/OSS. Resolving misalignments and open questions in the standardization of the area needs immediate actions already in the short term.

There is the need to give guidance to SDOs/organisations and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work. Develop the solutions for most important requirements first and specify the recommendations for the best solutions.

The project should address and achieve a higher level of standardization in the converged (wireline and wireless networks) operations area which will lead to reduced OPEX and CAPEX. In addition a faster time to market is expected through these requirements.

The NGMN Top OPE Recommendations are dealing only with wireless requirements. Wireline and wireless networks will be merged in the near future within many operators. There is a need for the definition of Converged O&M requirements to ensure that the operational activities within the converged networks perform optimally.
The specification of common usable network data and operations for these networks allow reducing CAPEX (harmonised networks) and OPEX (seamless operation processes).

It reduces the integration cost by harmonising the Information Model and reduces the maintenance cost by unifying the Operations Model.

"An increasing number of Service Providers (SP) has to operate a variety of network and service production infrastructures, from mobile and fixed network environments up to converged networks and services across many countries. The increasing demand to maintain and improve customer experience requires full end-to-end service management and hence, multi-technology and multi-vendor network management capabilities. On the other hand, financial downturn has put even more pressure on operational efficiency improvement."

3.1.2 Definitions

The MT section defines or specializes the following terms:

- Federated Model
- Interface

3.1.2.1 Federated Model

The Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. It enables the implementation of convergent network management functions and processes (for example alarm correlation) which need to operate on objects belonging to different network domains (for example wireless and wireline). The Federated Model is composed of the **Federated Information Model** (FIM) containing the data part of the model; i.e., the object classes with their attributes and the **Federated Operations Model** (FOM)

containing the dynamic part of the model; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
The model covers resource and service management layers (according to Figure 3-1) and all their management functions like **Configuration Management** (CM), **Fault Management** (FM), **Performance Management** (PM), **Inventory Management** (InvM) or **provisioning and assurance**.

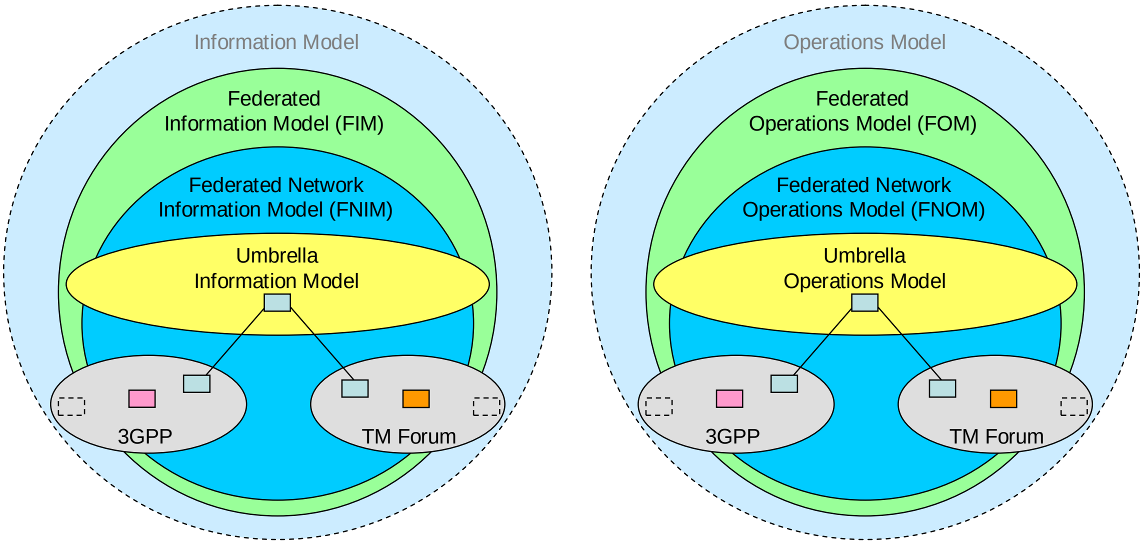


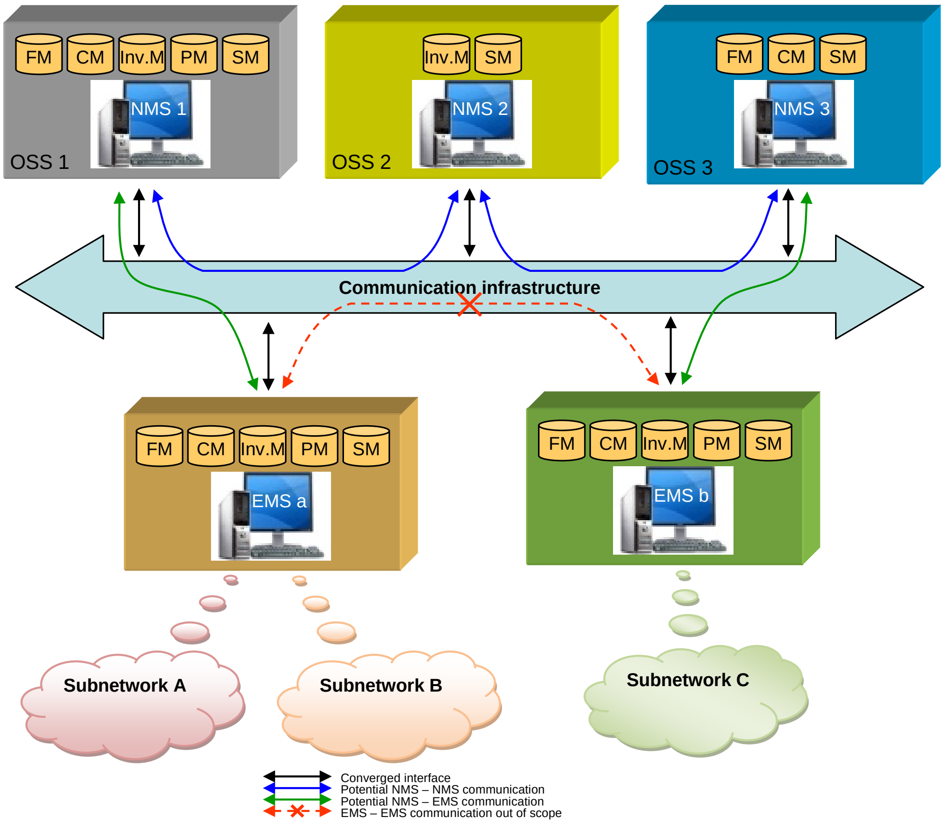
Figure 3-1: Federated Model

Note:
The FIM is similar to the NRM IRPs (Network Resource Model Integration Reference Points) in 3GPP and the Shared Information & Data Model (SID) in TM Forum.
The FOM is similar to the Interface IRPs (Integration Reference Points) in 3GPP and the Business Services in TM Forum.

3.1.2.2 Interface

The term "interface" used in the MT section is a network level management interface between various kinds of operation systems. Consequently, interfaces between Element Management System (EMS) and the Network Elements (NE) are out of scope.

Note:
In 3GPP terms: The term "interface" used in the MT chapter corresponds to 3GPP the northbound interface (Itf-N) between the EMS and the NMS (or operator's OSS for Operations Support System). The southbound interface, between EMS and the network elements is out of scope.
In TM Forum terms: The interface in scope is the MTNM/ MTOSI interface between EMS – NMS and more generally between all kinds of OSSs.


FM
CM
Inv.M
PM
SM
NMS 1
OSS 1
Inv.M
SM
NMS 2
OSS 2
FM
CM
SM
NMS 3
OSS 3
Communication infrastructure
FM
CM
Inv.M
PM
SM
EMS a
FM
CM
Inv.M
PM
SM
EMS b
Subnetwork A
Subnetwork B
Subnetwork C
Converged interface
Potential NMS – NMS communication
Potential NMS – EMS communication
EMS – EMS communication out of scope

Already existing modelling and tooling specifications in 3GPP and TM Forum are taken into account and will be used as input to produce the requirements for the converged interface specification infrastructure.

3.4 Methodology

Methodology of this sub task:

- Definition of the level of details

Examination of the Information Models, design principles and guidelines from 3GPP SA5, TM Forum and their JWGs (See

- Figure 3-3: Model of 3GPP and Figure 3-4: Model of TM Forum)
- Definition of design principals and patterns
- Definition of interface modelling requirements.

Deliverables of this sub task:

- Modelling environment requirements (e.g., specification structure, general design principals and modelling patterns)
- Tooling infrastructure requirements (e.g., interchange file formats)
- Recommendations regarding implementation.

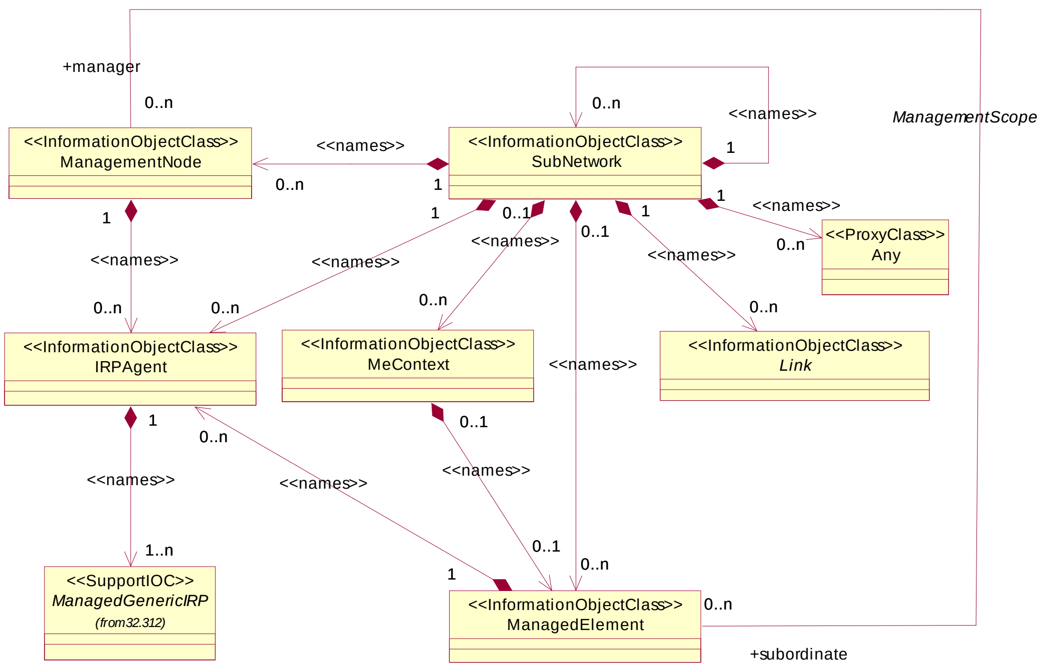


Figure 3-3: Model of 3GPP

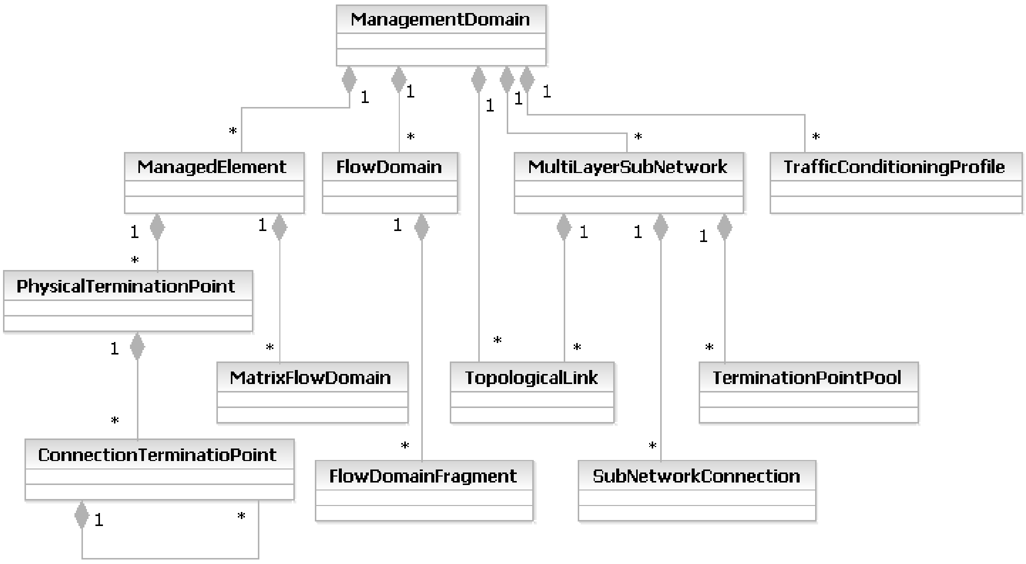


Figure 3-4: Model of TM Forum

The figures
Figure 3-3: Model of 3GPP and Figure 3-4: Model of TM Forum show the containment / naming hierarchy and the associations of the classes defined in the Joint 3GPP/ TMF model alignment project. (Top figure extracted from Figure 6.1: Generic NRM Containment/Naming and Association diagram (3GPP TS 32.622 [12])
Bottom figure extracted from Figure LR.35 - MTOSI/MTNM Containment (TM Forum SID Rel. 9.5 [41])

3.5 Requirements

Abstract:

3GPP WG SA5 has specified detailed **Network Resource Models** (NRMs) [16] for the management of mobile networks, plus a Generic Network Resource Model [12].

TM Forum has done the same for the management of various kinds of fixed networks, as well as a **Shared Information & Data** (SID) Model [28] providing a "common reference model for enterprise information that service providers, software providers, and integrators use to describe the network data", i.e., also generic definitions for network and service management aspects.

It shall be noted that the 3GPP Generic Network Resource Model (Generic NRM) [12] and TM Forum SID [28] have different scopes and have been developed independently from each other. As a consequence the resulting models are different.

Though there will always be a part in the Generic NRM [12] and the SID [28] which is different due to the different network technologies modelled, there are numerous model elements which do not have to be different between the two models because of the different network technologies.

Examples of these common elements are modelling of resource inventory information, modelling of security aspects, modelling techniques and how vendor specific Information Model extensions are managed using NRMs and SID.

Parallel to 3GPP und TM Forum are even more other Standards Development Organisations (SDOs) and organisations such as the Internet Engineering Task Force (IETF), International Telecommunications Union – Telecommunication Standardization Sector (ITU-T), Broadband Forum (BBF), Metro Ethernet Forum (MEF), etc., which have defined different management standards/ recommendations for mobile and fixed networks. In addition to the SDOs/ organisations many vendors deliver Element Management Systems (EMS) with their own proprietary solutions for specific technologies/ networks. It needs to be emphasised that the EMS is another OPEX cost centre that can be reduced thanks to the multi-technology-multi-domain capabilities of the EMSs.

Because all sets of specifications have been specified independently, the management of the mobile part and the fixed part is currently structured along silos with different management interfaces, information models, management architectures, and management workflows.
An additional problem is that even within mobile or fixed networks, we can find different specifications (modelling/ tooling) which are developed by different SDOs/ organisations or vendors.

All these different Standards (from SDOs/ organisations) and proprietary solutions (from vendors) use different modelling/tooling, therefore the CAPEX and OPEX for network operators and integrators to integrate all these interfaces have increased dramatically. A considerable obstacle is the complex mapping mechanism between all the different OSS tools when they need an interface to exchange information.

This heterogeneous modelling/tooling (1/ different models for different network domains/ technologies and 2/ different modelling frameworks (e.g. Stage 1-3 for 3GPP, BA, IA, IIS for TM Forum; UML for TM Forum with an inter-exchangeable format versus picture in 3GPP) also has a massive influence to scalability, time to market, complexity and applicability of these standards in OSS.

In the future the mobile and fixed networks will no longer be managed as separate networks. The convergence of mobile and fixed networks requires the convergence of the mobile and fixed OSSs.

The network operators and the telecommunication industry would greatly benefit from aligned management interfaces, management models, management architectures, and management workflows.

3.5.1 Modelling Requirements

Fixed and mobile networks are growing together → FMC. The specification of common usable network data and converged operations for these networks allow reducing CAPEX and OPEX.
We will be able to reduce integration cost by harmonising the Information Model and reduce the maintenance cost by unifying the Operations Model.

3.5.1.1 General Requirements

REQ-MT (1) The following SDOs/ organisations (at least 3GPP, TM Forum, ITU-T, BBF, MEF, and others) shall strengthen their joint activities regarding the Management topic

REQ-MT (2) It shall be possible to add other SDOs/ organisations in the future

REQ-MT (3) The resulting Umbrella Information Model shall be publicly available

REQ-MT (4) The Umbrella Information Model shall allow SDO/ organisation-specific enhancements based on common modelling patterns

REQ-MT (5) SDO/ organisation-specific enhancements should be realised in a way that enables a drill down process. The drill down process means the ability to identify a more generic class (super class) from the Umbrella Information Model which is enhanced in the SDO/ organisation-specific model. This assures that SDO/ organisation-specific extensions can be clearly identified as a detailed version of the commonly agreed classes and concepts

REQ-MT (6) The interfaces which use the SDO/ organisation-specific Information Model should be compliant with the interfaces defined in the Umbrella Information Model. Compliant means that object classes defined in an SDO/ organisation-specific Information Model need to subclass from the appropriate (abstract) classes defined in the UIM

REQ-MT (7) The proposed mechanism of SDO/ organisation-specific extension is via inheritance and the composition (decomposition) of object modelling design patterns. Direct usage of the Umbrella Information Model objects is desired. (Multi-) Inheritance shall be used for extensions

REQ-MT (8) The other SDOs/ organisations shall be informed of SDO/ organisations-specific enhancements if they believe that these enhancements are generic and should be added to the UIM

REQ-MT (9) The number of SDO/ organisation-specific enhancements shall be reduced to the absolute necessary minimum

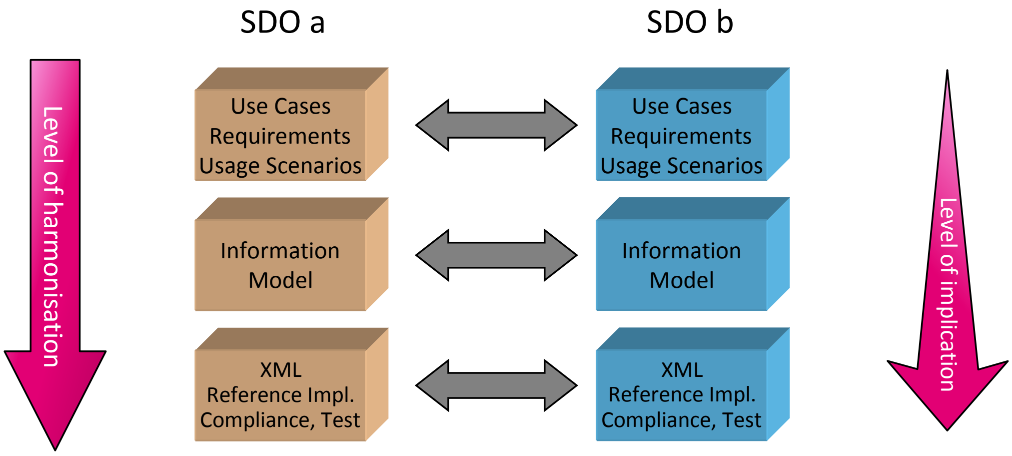
REQ-MT (10) The common management operations for fixed and mobile networks shall be harmonised

REQ-MT (11) SDOs/ organisations shall agree on a common terminology

REQ-MT (12) The functional coverage of the converged specifications shall continuously grow; i.e., shall replace the functions in the SDO/ organisation-specific specifications

REQ-MT (13) The harmonisation shall begin with high level business use cases, requirements and usage scenarios. Followed by the model harmonisation and finished by the protocol harmonisation. (See Figure 3-5)

REQ-MT (14) The modelling shall be able to comprehensively describe the functions in a protocol-neutral way. "Comprehensively" means that the modelling shall be detailed enough to be used as the basis for another protocol-specific specification.
Reason for this is that operators are mainly interested in functions which stay over the time even when the protocol changes.


SDO a
SDO b
Level of harmonisation
Use Cases
Requirements
Usage Scenarios
Information
Model
XML
Reference Impl.
Compliance, Test
Use Cases
Requirements
Usage Scenarios
Information
Model
XML
Reference Impl.
Compliance, Test
Level of implication

REQ-MT (21) Requirement identifiers must be unique within each category

REQ-MT (22) Requirements shall be defined using the following tabular template:

R_<SDO>_DDD_C_N	Description of the requirement
Source	Source of the requirement

where:
- <SDO> denotes the SDO / organisation
- DDD denotes the specification
- "C" designates the category of the requirement and is one of "BR", I, II, III, IV, V
- "N" is a 4 digits integer (e.g. 0012).

REQ-MT (23) A requirement is referred to by its identifier "R_<SDO>_DDD_C_N"

REQ-MT (24) It must be possible to display the definition of a requirement by a simple mouse click from any of its references

3.5.1.2.2 Usage Scenario Template

Based on [45].

REQ-MT (25) Usage scenarios shall be defined in text format

REQ-MT (26) A usage scenario identifier must be unique

REQ-MT (27) Usage scenarios are defined using the following tabular template:

Usage Scenario Id	<US_<SDO>_DDD_N>
Usage Scenario Name	
Summary	
Actor(s)	
Pre-Conditions	
Begins When	
Description	<Step 1> <Step 2> … <Step n>
Ends When	
Post-Conditions	
Exceptions	Put a reference here to a document or a separate table which lists all the exceptions. Specific exceptions will be explicitly listed in the Description clause.
Traceability	Hyperlinks to the associated requirements

where:

- <SDO> denotes the SDO/ organisation
- DDD denotes the specification
- "N" is a 4 digits integer (e.g. 0012).

REQ-MT (28) A usage scenario is referred to by its identifier "US_<SDO>_DDD_N"

REQ-MT (29) It must be possible to display the definition of a use case by a simple mouse click from any of its references

REQ-MT (30) It must be easy to "navigate" from a requirement to the usage scenarios where this requirement applies and vice versa

REQ-MT (31) When a new specification is generated, the "N" part of the usage scenario identifier must be generated in sequence (no "hole"), until the document is released for official approval. From this stage the identifier of a given usage scenario will never change

3.5.1.3 Federated Model Requirements

REQ-MT (32) The SDOs/ organisations shall define a common model for mobile and fixed networks as a shared Umbrella Information Model

REQ-MT (33) The FIM shall enable the modelling of all resources of the mobile and fixed networks

REQ-MT (34) The Umbrella Model containing the network data and operations that are necessary for managing mobile and fixed networks shall be increased (over time). All generic (i.e., not fixed or mobile specific) network data and operations specified outside the Umbrella Model increase the operators OPEX and CAPEX significantly

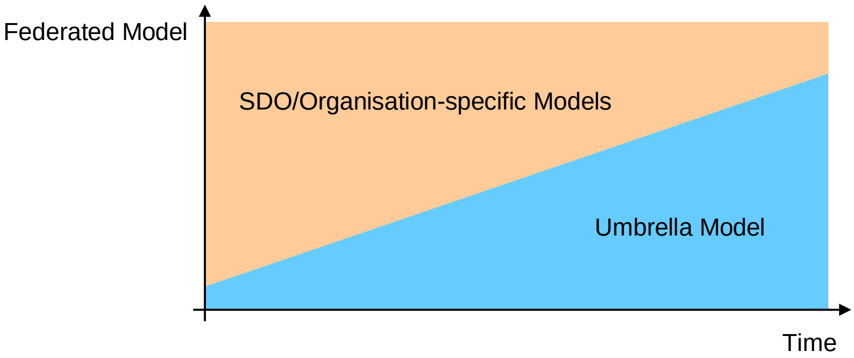


Figure 3-6: Relation between Federated Model – Umbrella Model

REQ-MT (35) The FIM shall enable the modelling of both the connection oriented technologies and connectionless technologies; e.g., model the connection oriented sub network connection and the connectionless flow domain fragment in one single object class. This also includes e.g. mobile access technologies and broadcast technologies

REQ-MT (36) All functionalities in the areas of Fault Management, Performance Management, Configuration Management (incl. Resource Provisioning and Service Configuration & Activation) and Inventory Management which are common to wireline and wireless management interfaces have to be consolidated in the harmonised Federated Model

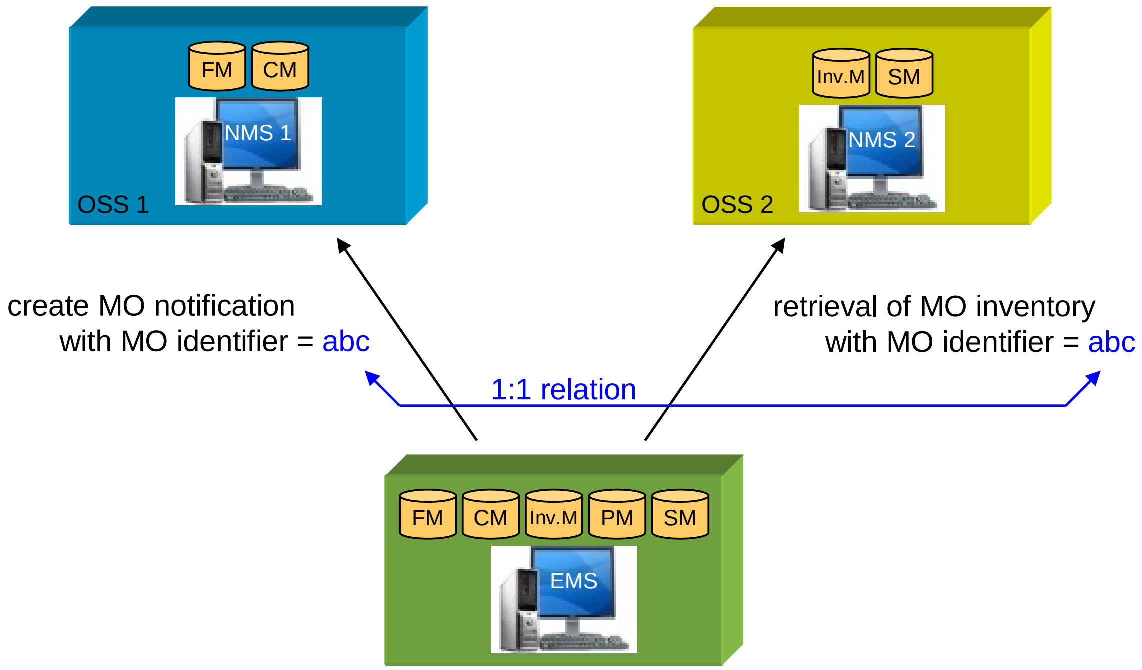
REQ-MT (37) The static Information Models from wireline (e.g. MTOSI) and wireless (e.g. 3GPP) technologies have to be harmonised.
It is acceptable to have wireline and wireless specific parts but these parts shall as much as possible be based on the common Umbrella Information Model

REQ-MT (38) The Federated Model shall offer the necessary network data and operations for all domains such as Operations Support & Readiness (OS&R; which includes Inventory Management), Fulfilment and Assurance [46].

REQ-MT (39) The Umbrella Information Model shall initially contain specifications for networks, network elements, topological links, termination points and sub network connections (eg. id, userLabel)

REQ-MT (40) Network resources (managed objects) shall be named using a harmonised naming convention. The naming convention must uniquely identify the network resources

REQ-MT (41) It is required to have a 1:1 relation between Event Managed Object Instances and Inventory Managed Object Instances. If Managed Object (MO) identifiers used/ provided by the inventory equipment of an element manager need to be mapped to meet naming requirements of the inventory database, the same mapping must be applied to the MO identifiers in the event. The corresponding is true if mapping is driven by event naming requirements.
If MO identifiers of events and inventory within an element manager are different, the difference must be eliminated before the above mapping can be applied.
Rationale:
An event must be unambiguously related to a known Object Instance (in the inventory).



REQ-MT (45) The Federated Model shall enable the correlation of the network data:

- between different layers and technologies in fixed networks (eg, WDM, SDH/S ONET, ATM, IP/MPLS)
- in fixed and mobile networks (eg, IP/ MPLS <-> RAN, WDM <-> core network)
- from different resources in mobile networks (RAN, core network, etc.)
- from different mobile network technologies (eg, WiMAX, WLAN, LTE, UMTS, etc.)

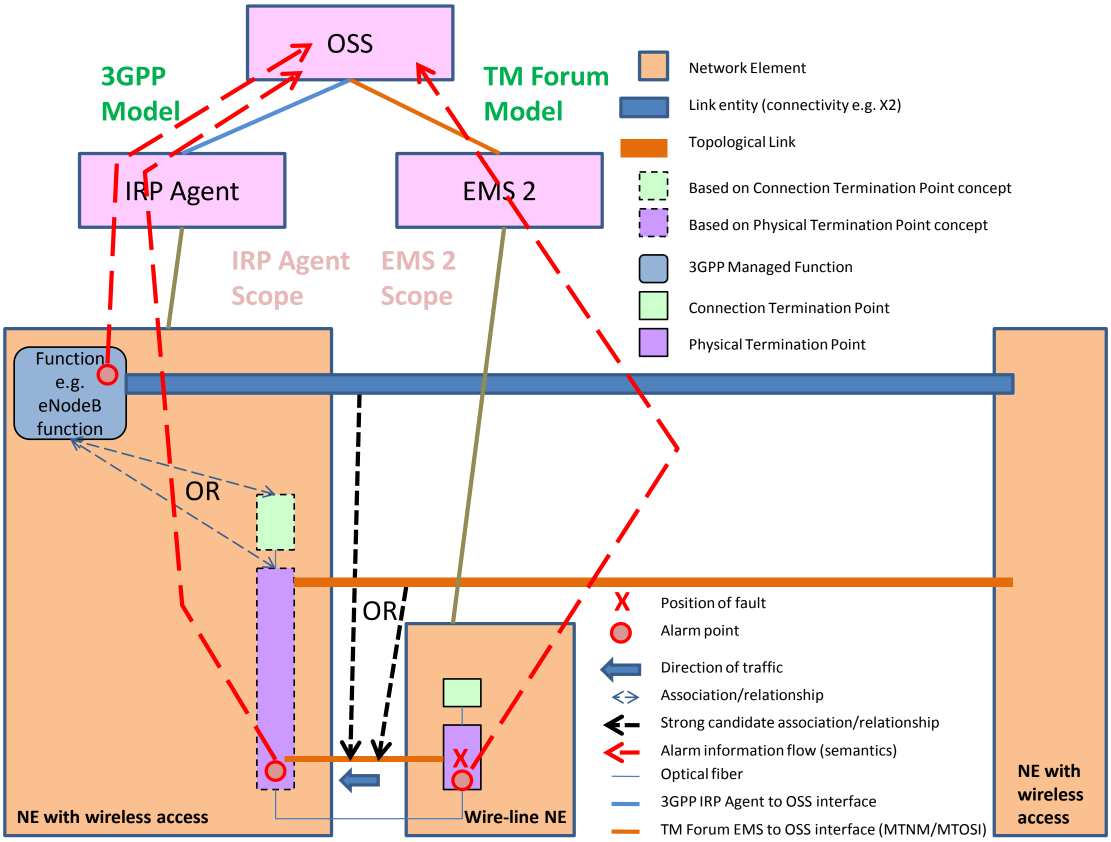


Figure 3-8: Example OSS receives the alarms from different EMS and different models

(Mobile Network model from 3GPP model and Fix Network model from TMF model) (Figure extracted from [37])

REQ-MT (46) The SDOs/ organisations shall specify the Federated Model in a protocol neutral way using UML

REQ-MT (47) The Umbrella Model shall be governed by all participating SDOs/ organisations via a dedicated cross-SDOs/ organisations structure

REQ-MT (48) The Federated Model shall be machine readable

REQ-MT (49) The Federated Model shall also be delivered in the portable document format (PDF)

REQ-MT (50) The modelling of the SDO/ organisation-specific enhancements shall be based on the Umbrella Model

REQ-MT (51) Traceability between model and requirements/ use cases shall be provided in two ways:

1. Where appropriate, a UML artefact should reference the corresponding requirement and/ or use case identifier in the documentation field
2. Traceability matrices shall be provided for:
   - mapping from object classes to requirements
   - mapping from object class attributes to requirements
   - mapping from object class operations to requirements
   - mapping from object class operations to use cases
   - mapping from use cases to requirements

REQ-MT (52) Multiple NMS applications might be connected (logically) to several EMS applications (M : N). The interface specification must allow to connect one NMS to multiple EMS. (This might have an impact on addressing – mechanisms in the interface).
Furthermore the interface specification must allow splitting the incoming event/ alarm traffic between different instances of the same interface implementations to avoid overload situations in one interface instance
Rationale:
This capability allows reducing the effort for the maintenance of several different client-side interfaces

REQ-MT (53) The Federated Model shall cover network resources with dimensions of “physical resources" and "logical resources"

REQ-MT (54) The Federated Model shall provide the relationship of network resources from different networks (e.g., wireless network, core network, transmission network, IP network, switching network, etc.), such as correlation of wireless network resource and transmission network resource can be easily learned

REQ-MT (55) The Federated Model shall support to provide the uniform view of resources from different networks, such as end-to-end topology of network resources

REQ-MT (56) The Federated Model shall be used as an equipment information template, since it is useful to implement large quantities of network equipment instances. An equipment information template can provide information rules of verification and constraints for card/ bay/ slot/ rack, thereby it shall improve the data accuracy and quality of the stock of equipment resources to support network resource lifecycle management

3.5.1.4 Model Artefact Property Requirements

This chapter defines the requirements for the properties of the model artefacts:

- managed object classes
- attributes
- service interfaces (grouping of operations in the FOM)
- operations
- parameters
- notifications
- data types
- relationships between managed object classes
- UML diagrams

Editor's notes: Requirements for extension mechanisms may need to be added. The definition of the multiplicity in the meta model may be too restrictive.

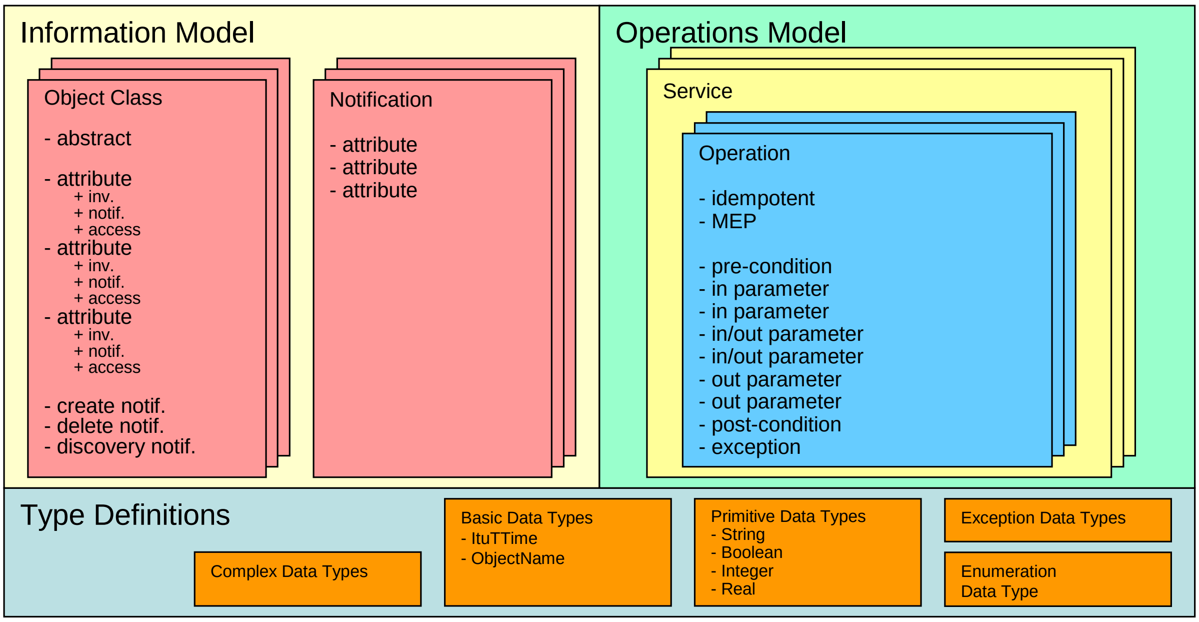


Figure 3-9: Model Artefacts

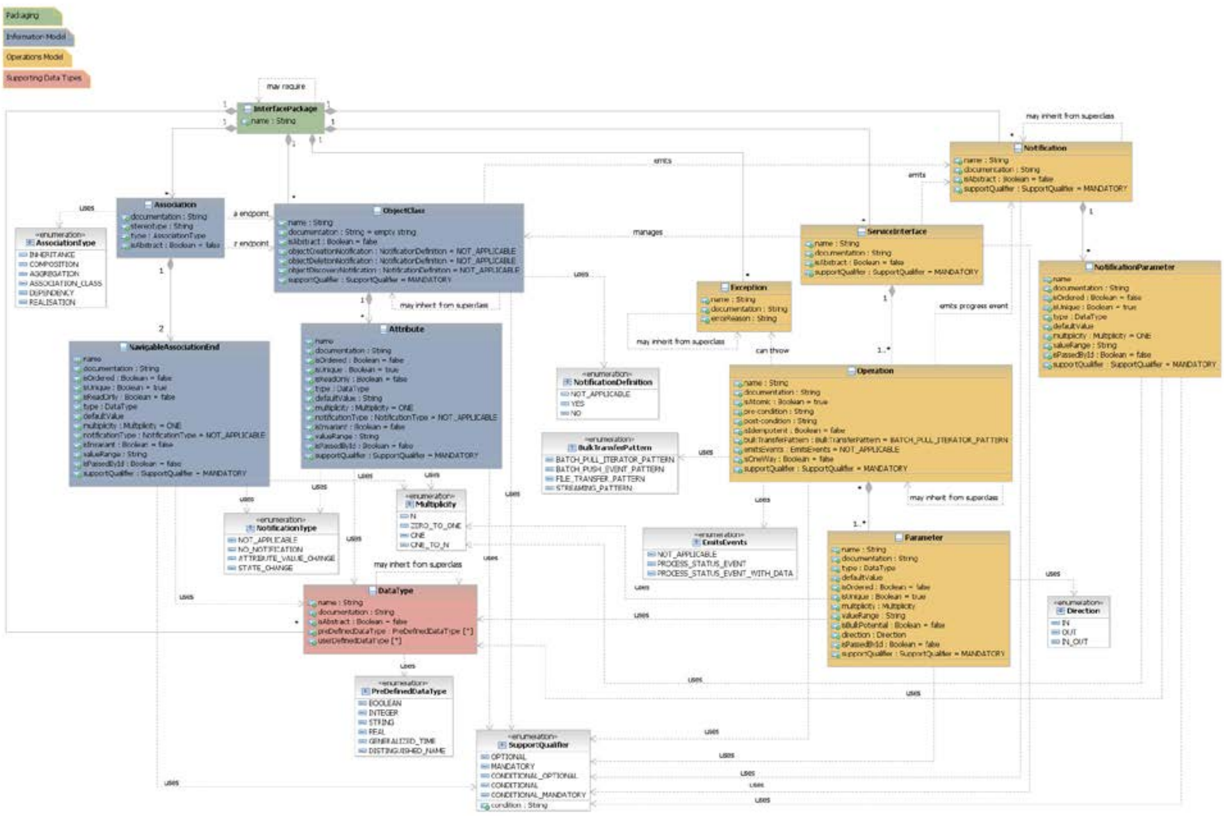


Figure 3-10: Meta-Model

3.5.1.4.1 Object Class Requirements

Object classes are used to model data entities in the Information Model and shall be derived from the static requirements.

REQ-MT (57) An object class shall have the following properties:

- Object Class name
  Shall follow Upper CamelCase (UCC)
  The complete Distinguished Name (DN) having this name as a equipment must be unique across an interface instance
- Object Class description
  Shall contain a textual description of the object class
  Shall refer (to enable traceability) to the appropriate requirement
- Superclass(es)
  Inheritance and multiple inheritance may be used
- Abstract Object Class
  Indicates if the object class can be instantiated or is just used for inheritance
- Required Object Notifications
  Shall identify if creation/ deletion notifications are to be send
  "objectCreationNotification" <NO | YES | NOT_APPLICABLE>
  "objectDeletionNotification" <NO | YES | NOT_APPLICABLE>
  "objectDiscoveryNotification" <NO | YES | NOT_APPLICABLE>
- Support Qualifier
  Identifies the required support of the object class: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

REQ-MT (58) An attribute within an object class shall have the following properties:

- Attribute name
  Shall follow Lower CamelCase (LCC)
  - Boolean typed attribute names shall always start with a verb like 'is', 'must', etc. (e.g., 'isAbstract') and the whole attribute name must be composed in a way that it is possible to answer it by "true" or "false"
  - Enumeration typed attributes always end with "Kind" (e.g., 'aggregationKind')
  - List typed attributes shall end with the word "List"
  - Attributes referencing an instance identifier shall contain the word "Ref"
- Attribute description
  Shall contain a textual description of the attribute
  Shall refer (to enable traceability) to the specific requirement
- Qualifiers
  - Ordered
    For a multi-valued multiplicity; this specifies whether the values in an instantiation of this attribute are sequentially ordered; default value is false
  - Unique
    For a multi-valued multiplicity, this specifies whether the values in an instantiation of this attribute are unique (i.e., no duplicate attribute values are allowed); default value is true

  Excerpt from UML superstructure specification, [44]: *When isUnique is true (the default) the collection of values may not contain duplicates. When isOrdered is true (false being the default) the collection of values is ordered. In combination these two allow the type of a property to represent a collection in the following way:*

isOrdered	isUnique	Collection type
false	True	Set
true	True	OrderedSet
false	False	Bag
true	False	Sequence

Table 3-1: Collection types for properties

(Table extracted from UML Superstructure Specification [44])

- Read Only
  If true, the attribute may only be read, and not written by the client OS. The default value is false
- Type
  Refers to a pre-defined or user-defined data type; see also chapter 3.5.1.4.7
- Default Value
  Provides the value that the attribute has to start with in case the value is not provided during creation or already defined because of a system state
- Multiplicity
  Defines the number of values the attribute can simultaneously have
- Attribute Notifications
  Identifies if a notification has to be sent in case of a value change
- Invariant
  Identifies if the value of the attribute can be changed after it has been created; default value is "False"
- Value Range
  Identifies the allowed values the attribute can have
- Passed by Id
  Identifies if the attribute contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"
- Support Qualifier
  Identifies the required support of the attribute: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

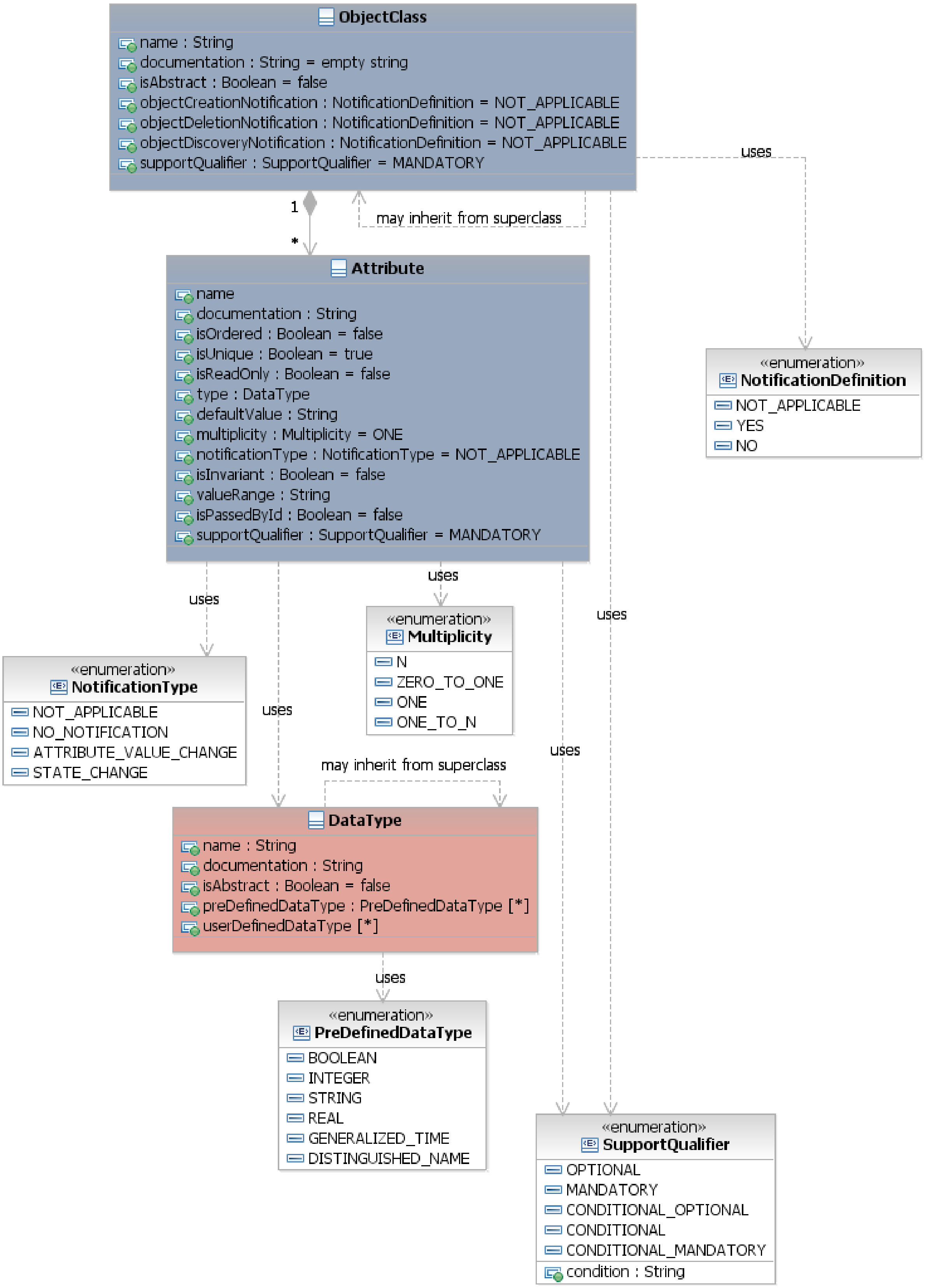


Figure 3-11: Meta Model: Object Class

3.5.1.4.2 Service Interface Requirements

REQ-MT (59) Interface object classes shall be used to model the interfaces in the operations model and shall be derived from the dynamic requirements

REQ-MT (60) A service interface shall have the following properties:
- Service interface name
  Shall follow Upper CamelCase (LCC)
  Shall be expanded by the word "Service"
- Service interface description
  Shall contain a textual description of the service interface
  Shall refer (to enable traceability) to the specific requirement
- Support Qualifier
  Identifies the required support of the service interface: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

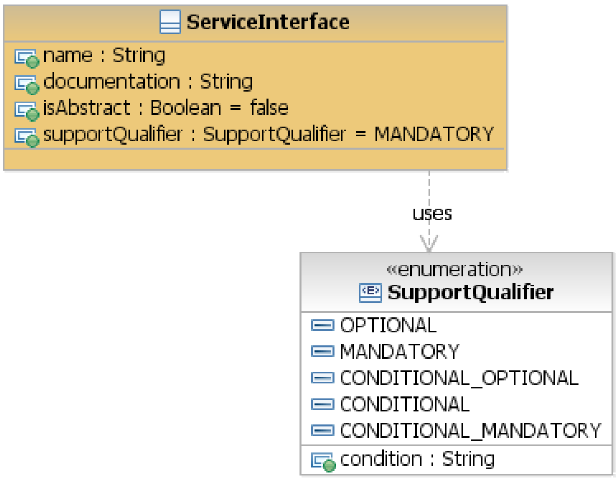


Figure 3-12: Meta-Model: Service Interface

3.5.1.4.3 Operation Requirements

REQ-MT (61) Operations shall be grouped in interface object classes and shall be derived from the dynamic requirements and usage scenarios

REQ-MT (62) An operation shall have the following properties:
- Operation name
  Shall follow Lower CamelCase (LCC)
- Operation description
  Shall contain a textual description of the operation
  Shall refer (to enable traceability) to the specific requirement
- Atomic
  Identifies if the operation is best effort or is successful/ not successful as a whole

- Return Type
  Shall be fixed to "void"
- Pre-condition(s)
  Shall list the conditions that have to be true before the operation can be started (i.e., if not true, the operation will not start at all)
  Note: It is recommended to define the pre-condition in OCL
- Parameter(s)
  Refer to specific requirement below
- Post-condition(s)
  Shall describe the state of the system after the operation has been successfully executed
  Note: It is recommended to define the post-condition in OCL
- Idempotency
  Defines if the operation is idempotent or not
- Bulk Transfer Pattern
  The Bulk Transfer Pattern fully identify the messages and the choreography (sequencing and cardinality) of the messages independently from a business activity; default value is "batch pull iterator pattern"
  The following distinct communication patterns are required:
  - Batch pull iterator pattern
  - Batch push event pattern
  - File transfer pattern
  - Streaming pattern
- Emits events
  Identifies the operation as a process status event with/ or without associated data; default value = "not applicable"
- One way
  The operation is one way, when it has only input parameter or only output parameter; default value = "false"
- Operation Exceptions
  The allowed exceptions together with a failure reason shall be defined for each operation
- Support Qualifier
  Identifies the required support of the operation: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

REQ-MT (63) The following list of common exceptions shall be supported by the operations:

- AlreadyInPostCondition
  This exception can be used by operations which are not defined as idempotent. It is used to indicate that the target OS is already in the post-condition
- AtomicTransactionFailure
  This exception shall be raised when an atomic operation is not successful due to a failure of one of its sub-parts. The failure reason shall indicate which object/ part failed
- CapacityExceeded
  This exception shall be raised when the request will result in resources being created or activated beyond the capacity supported by the NE or target OS
- Duplicate
  This exception shall be raised if an object instance cannot be created because an object with the same identifier/name already exists
- EntityNotFound
  This exception shall be raised when the specified object does not exist

- FilterNotSupported
  This exception shall be raised when a filter definition is not supported by the implemented filter. The failure reason shall indicate the more precise reason
- InventoryOutOfSync
  This exception shall be raised when the operation fails because the inventory data bases from the target and requesting OS are out of sync
- NotInValidState
  This exception shall be raised when the state of the specified object is such that the target OS cannot perform the operation
- ObjectInUse
  This exception shall be raised when the object identified in the request is currently in use
- UnableToNotify
  This exception shall be raised when the target OS is unable to connect to the Notification Service
- CommunicationLoss
  This exception shall be raised when the target OS is unable to communicate with the subordinate OS
- InternalError
  This exception shall be raised when the request has resulted in an OS internal error
- NotImplemented
  This exception shall be raised when the target OS does not support this operation
- UnableToComply
  This exception shall be raised when the target OS cannot respond to the request
- AccessDenied
  This exception shall be raised when the requesting OS is not permitted to perform the operation
- InvalidInput
  This exception shall be raised when the operation contains an input parameter that is syntactically incorrect or identifies an object of the wrong type or is out of range

REQ-MT (64) The following common exceptions shall be supported by all operations:

- AccessDenied
- CommunicationLoss
- InternalError
- InvalidInput
- NotImplemented
- UnableToComply

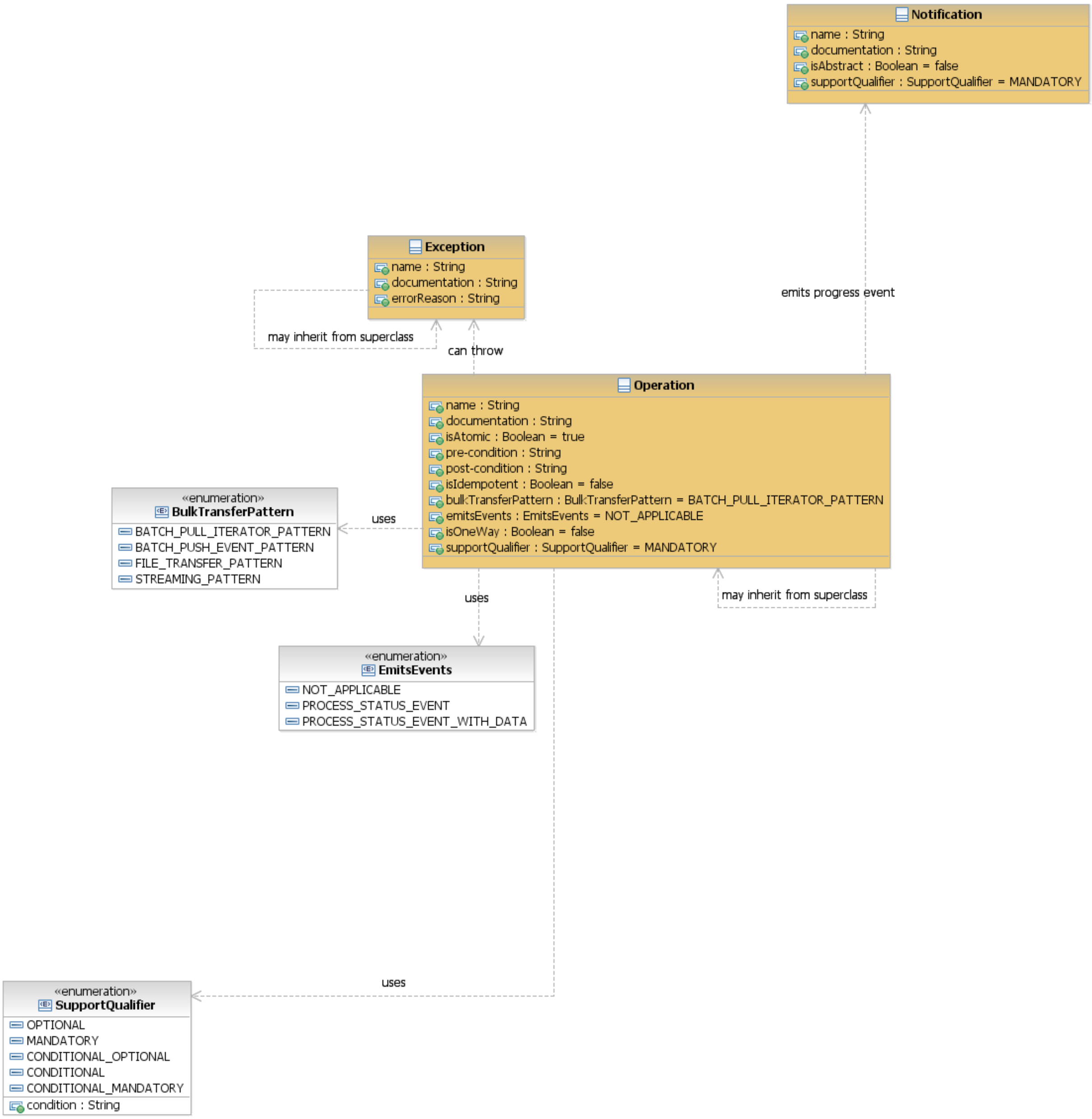


Figure 3-13: Meta-Model: Operation

3.5.1.4.4 Operation Parameter Requirements

REQ-MT (65) Each parameter within an operation shall have the following properties:

- Parameter name
  Shall follow Lower CamelCase (LCC)
- Parameter description
  Contains a textual description of the parameter.
  Shall refer (to enable traceability) to the specific requirement
- Type
  Shall refer to a basic or complex data type

Note: A list of input (in a few cases also output) parameters could also be combined in a data type

- Default Value
  Provides the value that the parameter has to start with in case the value is not provided
- Ordered
  For a multi-valued parameter; the order of the values is important
- Unique
  For a multi-valued parameter, no duplicate values are allowed
- Multiplicity
  Defines the number of values the parameter can simultaneously have
- Value Range
  Identifies the allowed values the attribute can have
- Bulk Potential
  Indicates that this parameter can potentially carry a very large amount of data which will require a bulk data transfer pattern
- Direction
  In | InOut | Out
- Passed by Id
  Identifies if the parameter contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"
- Support Qualifier
  Identifies the required support of the operation: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

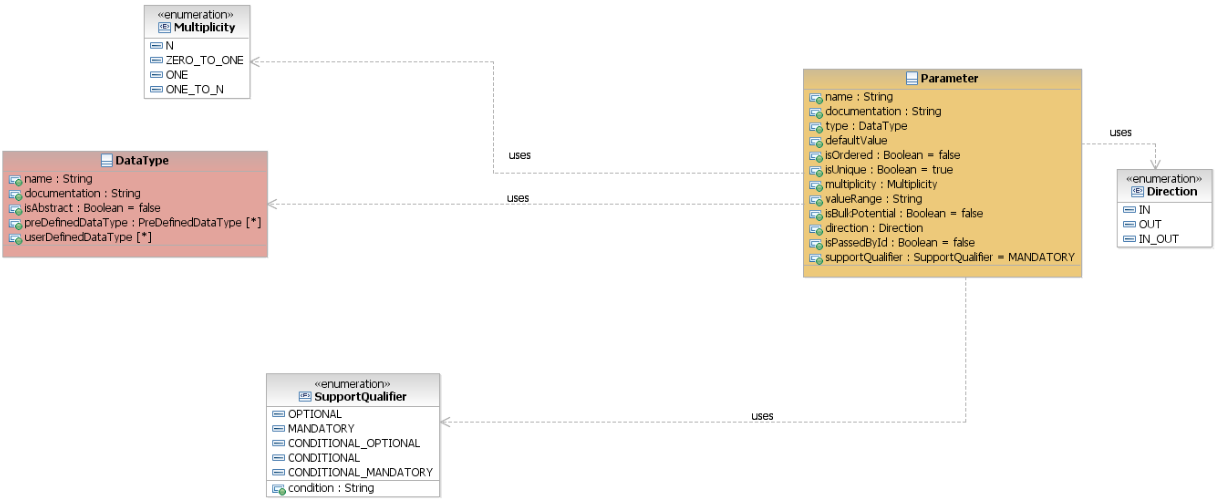


Figure 3-14: Meta-Model: Operation Parameter

3.5.1.4.5 Notification Requirements

REQ-MT (66) Object classes shall be used to model the notifications in the Information Model

REQ-MT (67) Notifications shall have the following properties:

- Notification name
  Shall follow Upper CamelCase (UCC)
  Shall end with the word "Notification" (e.g., EquipmentProtectionSwitchNotification)

- Notification description
  Contains a textual description of the parameter
  Shall refer (to enable traceability) to the appropriate requirement
- Superclass(es)
  Inheritance and multiple inheritance may be used
- Abstract Object Class
  Indicates if the notification can be instantiated or is just used for inheritance
- Support Qualifier
  Identifies the required support of the notification: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

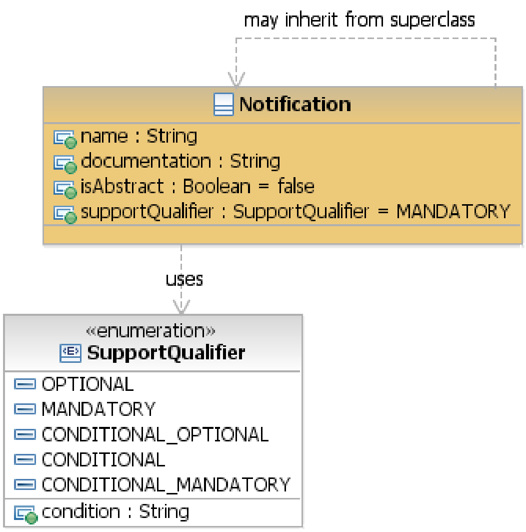


Figure 3-15: Meta-Model: Notification

3.5.1.4.6 Notification Parameter Requirements

The information which has to be provided by a notification is contained in the notification parameters which are modelled as attributes of Notification object classes.

REQ-MT (68) Notification Parameters shall have the following properties:

- Parameter name
  Shall follow Lower CamelCase (LCC)
  Shall follow the naming conventions defined for the object class attribute names defined in chapter 3.5.1.4.1
- Parameter description
  Contains a short textual description of the parameter
  Shall refer (to enable traceability) to the specific requirement
- Type
  Refers to a basic or complex data type
- Passed by Id
  Identifies if the parameter contains just a pointer to the information (passed by id = true) or contains the whole information itself (passed by id = false); default value = "false"

- Support Qualifier
  Identifies the required support of the notification parameter: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

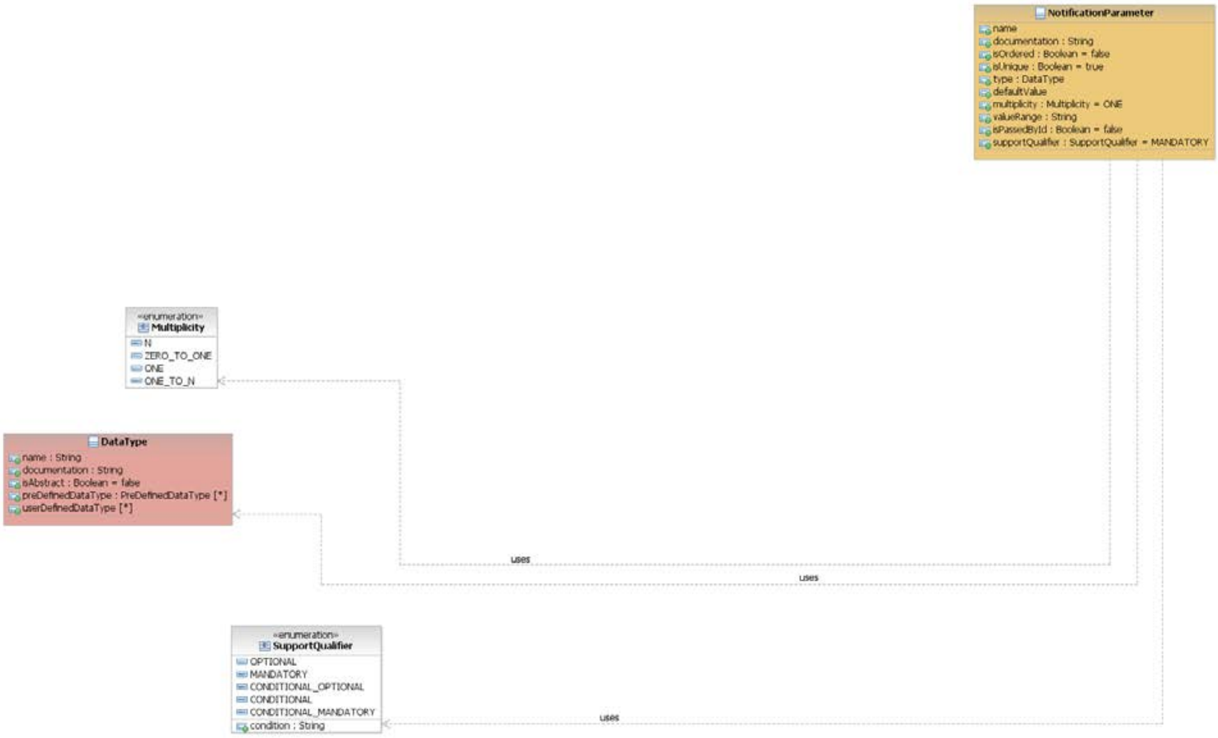


Figure 3-16: Meta-Model: Notification Parameter

3.5.1.4.7 Data Type Requirements

Data Types are distinguished between "pre-defined" and "user-defined" data types.

REQ-MT (69) The following pre-defined data types shall be used:

- Boolean
- Integer
- Real
- String
- DistinguishedName
  The DistinguishedName has to be used for the unique, read-only name of an object. The exact type is protocol specific
- GeneralizedTime
  "yyyyMMddhhmmss.s[Z|{+|-}HHMm]" where:

yyyy	"0000".."9999"	year
MM	"01".."12"	month
dd	"01".."31"	day
hh	"00".."23"	hour
mm	"00".."59"	minute
ss	"00".."59"	second
s	".0"..".9"	tenth of second (set to ".0" if EMS or ME cannot support this

	granularity)		
Z	"Z"	indicates UTC (rather than local time)	
{+|-}		"+" or "-" delta from UTC	
HH		"00".."23"	time zone difference in hours
Mm		"00".."59"	time zone difference in minutes

REQ-MT (70) User-defined data types shall have the following properties:

- Data type name
  Shall follow Upper CamelCase (UCC)
- Data type description
  Shall contain a textual description of the data type
  Shall refer (to enable traceability) to the appropriate requirement
- Attributes within data types
  Data type attributes have the same properties as the object class attributes; see chapter 3.5.1.4.1

REQ-MT (71) The literals of Enumeration data types shall have only upper case characters; words are separated by "_"

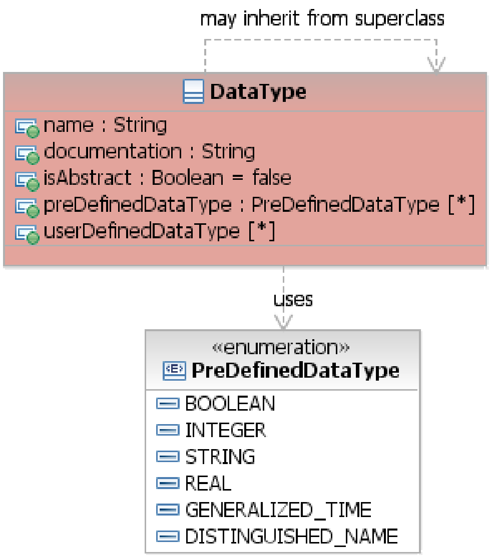


Figure 3-17: Meta-Model: Data Type

3.5.1.4.8 Association Requirements

REQ-MT (72) Associations shall have the following properties:

- Association description
  Shall contain a textual description of the association
  Shall refer (to enable traceability) to the appropriate requirement
- Stereotype
  E.g., <<naming>> shall be used if the association defines the object naming tree
- Association Type
  E.g., inheritance, association (composition, aggregation, and association class), dependency, and realisation

An association may represent a composite aggregation (i.e., a whole/part relationship). Only binary associations can be aggregations. Composite aggregation is a strong form of aggregation that requires a part instance be included in at most one composite at a time. If a composite is deleted, all of its parts are normally deleted with it. Note that a part can (where allowed) be removed from a composite before the composite is deleted, and thus not be deleted as part of the composite. Compositions may be linked in a directed acyclic graph with transitive deletion characteristics; that is, deleting an element in one part of the graph will also result in the deletion of all elements of the sub graph below that element. Composition is represented by the isComposite attribute on the part end of the association being set to true

- Role names

  Identifies the role that the object plays at the navigable end of the relationship

  Shall follow Lower CamelCase (LCC)

  Navigable association ends will lead to an attribute in the remote object class. Therefore, the name shall follow the naming conventions defined for the object class attribute names defined in chapter 3.5.1.4.1

  Note: Only navigable relationships have role names

- Constraint(s)

  List the constraint(s) under which the association can exist

- Abstract

  It is recommended to create associations which are just for explanation to the reader of the model. These associations should be defined as "abstract", they are not navigable and have no role names. They shall not be taken into account in the protocol specific specification. This can for example be used to show the association to the object which is retrieved by a get-operation.

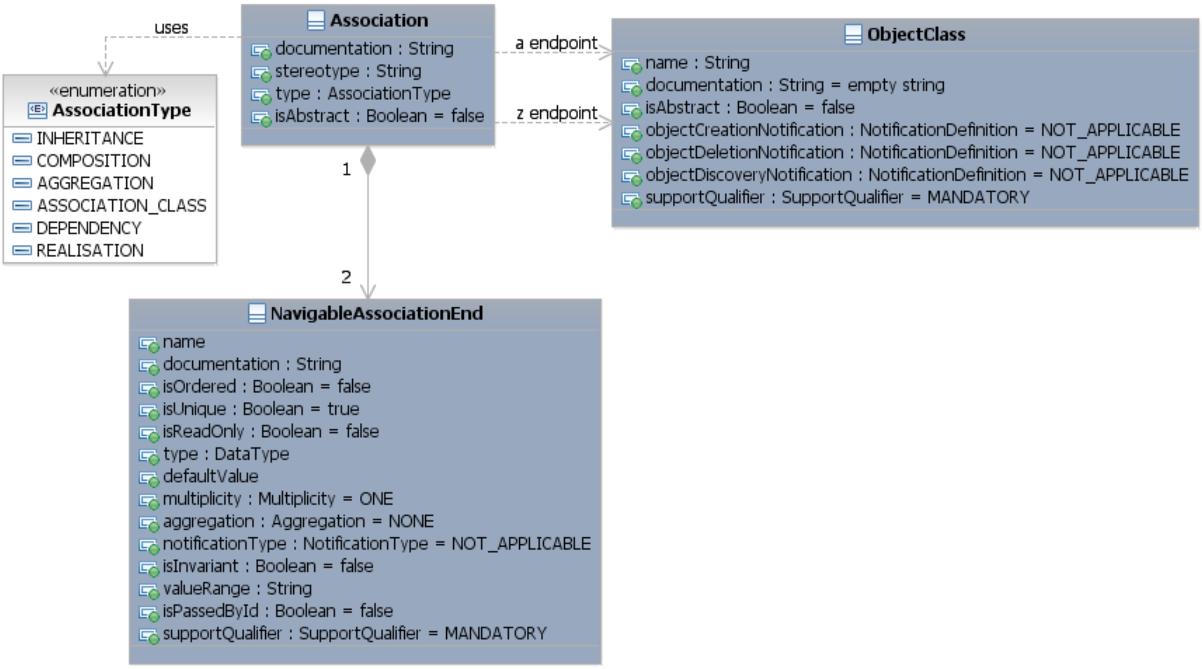


Figure 3-18: Meta-Model: Association

REQ-MT (73) A navigable association end shall have the following properties:

- Name

  Shall follow Lower CamelCase (LCC)

- o Boolean typed association end names shall always start with a verb like 'is', 'must', etc. (e.g., 'isAbstract') and the whole association end name must be composed in a way that it is possible to answer it by "true" or "false"
  - o Enumeration typed association end always end with "Kind" (e.g., 'aggregationKind')
  - o List typed association ends shall end with the word "List"
  - o Association ends referencing an instance identifier shall contain the word "Ref"
- Description

  Shall contain a textual description of the association end

  Shall refer (to enable traceability) to the specific requirement
- Qualifiers
  - o Ordered

    For a multi-valued multiplicity; this specifies whether the values in an instantiation of this association end are sequentially ordered; default value is false
  - o Unique

    For a multi-valued multiplicity, this specifies whether the values in an instantiation of this association end are unique (i.e., no duplicate association end values are allowed); default value is true

Excerpt from UML Superstructure Specification, [44]: *When isUnique is true (the default) the collection of values may not contain duplicates. When isOrdered is true (false being the default) the collection of values is ordered. In combination these two allow the type of a property to represent a collection in the following way:*

isOrdered	isUnique	Collection type
False	True	Set
True	True	OrderedSet
False	False	Bag
True	False	Sequence

Table 3-2: Collection types for properties

(Table extracted from UML Superstructure Specification [44])

  - o Read Only

    If true, the association end may only be read, and not written by the Requesting OS. The default value is false
- Type

  Refers to a pre-defined or user-defined data type; see also chapter 3.5.1.4.7
- Default Value

  Provides the value that the association end has to start with in case the value is not provided during creation or already defined because of a system state
- Multiplicity

  Defines the number of values the association end can simultaneously have
- Notifications

  Identifies if a notification has to be sent in case of a value change
- Invariant

  Identifies if the value of the association end can be changed after it has been created; default value is "False"
- Value Range

  Identifies the allowed values the association end can have
- Passed by Id

  Identifies if the association end that points to an object contains just a pointer to the object (passed by id = true) or contains the whole object information itself (passed by id = false); default value = "false"

- Support Qualifier
  Identifies the required support of the association end: optional, mandatory, conditionalMandatory, conditionalOptional, conditional. It shall also be possible to define the condition. Default value = mandatory

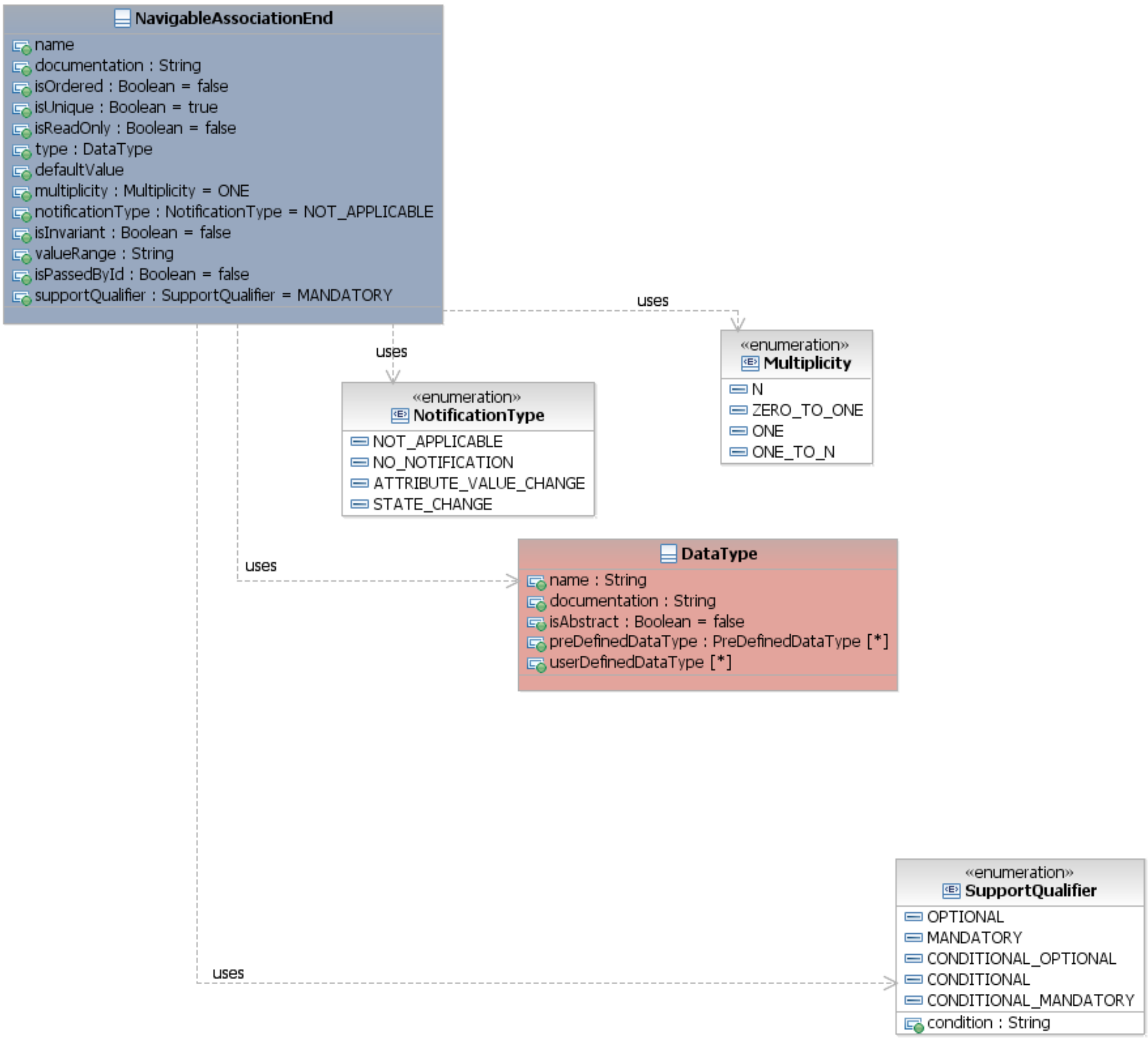


Figure 3-19: Meta-Model: Association End

3.5.1.4.9 UML Diagram Requirements

REQ-MT (74) Objects and their relationships shall be presented in class diagrams

REQ-MT (75) It is recommended to create

- An overview class diagram containing all object classes related to a specific management area (Class Diagram)

- An overview interface diagram containing all interfaces related to a specific management area (Interface Diagram)
- A separate inheritance class diagram in case the overview diagram would be overloaded when showing the inheritance structure (Inheritance Class Diagram)
- A class diagram containing the defined notifications (Notifications Diagram)
- A class diagram containing the defined data types (Type Definitions Diagram)
- Additional class diagrams shall be established to show specific parts of the specification in detail
- State diagrams shall be created for complex state attributes
- Activity diagrams\Sequence Diagrams shall be created for complex operations
- The class name compartment shall contain the "Qualified Name"
- The class attributes and operation shall show the "Signature"

3.5.1.5 Infrastructural Requirements

REQ-MT (76) The SDOs/ organisations shall agree on a list of common modelling patterns defined in a kind of meta-model

REQ-MT (77) The SDOs/ organisations shall integrate the existing models into the Federated Model through "translators" and/ or "adapters". For new technologies, the modelling shall be based on the Federated Model. They shall also define a migration path which allows bringing appropriate parts of the present individual models into the common Umbrella Model

REQ-MT (78) It shall be possible to use the Federated Model (and its SDO/ organisation-specific enhancements) as input to a tool based Interface development process

REQ-MT (79) The SDOs/ organisations shall agree on a common UML version (e.g., 2.3)

REQ-MT (80) The SDOs/ organisations shall use – if possible – open source modelling tools. XMI shall be used as common interchange format

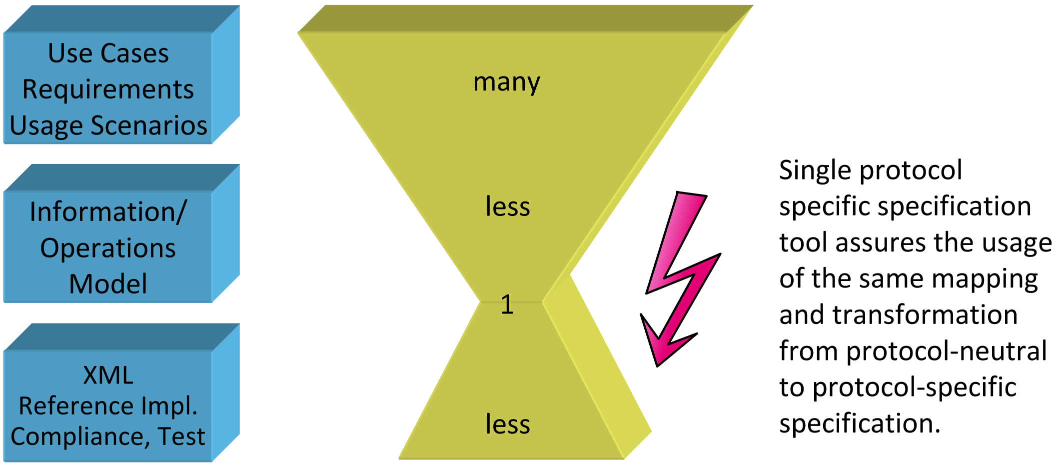
3.5.2 Tooling Requirements

3.5.2.1 General Requirements

REQ-MT (81) The creation of the specification shall be tool supported.

REQ-MT (82) Open interchange formats shall be agreed to export/import data between the tools in the chain.

REQ-MT (83) A **single** tool shall be used to map/transform the protocol-neutral specification into the protocol-specific specification.


Use Cases
Requirements
Usage Scenarios
Information/
Operations
Model
XML
Reference Impl.
Compliance, Test
many
less
1
less
Single protocol specific specification tool assures the usage of the same mapping and transformation from protocol-neutral to protocol-specific specification.

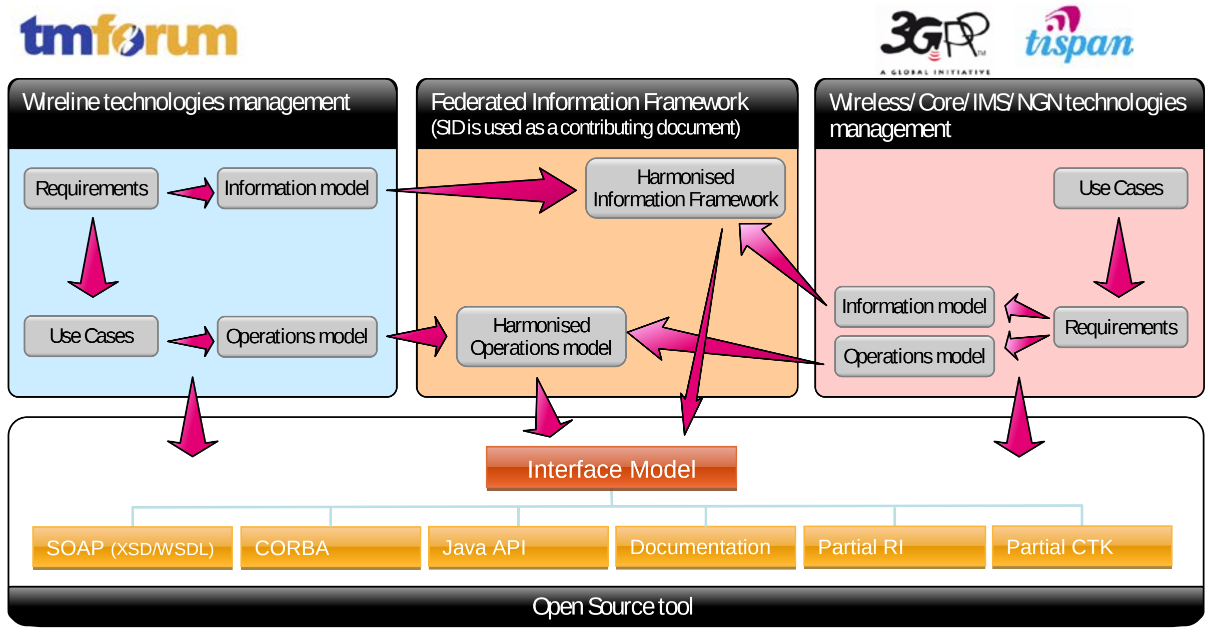


Figure 3-21: Modelling/Tooling Architecture

3.5.2.2 General Pattern Requirements

REQ-MT (90) The tool shall provide general patterns to ensure a common basis for all interfaces

3.5.2.2.1 Object Identifier Pattern

REQ-MT (91) The tool shall add a globally unique object identifier to every object to uniquely identify the object across an interface

REQ-MT (92) The object identifier shall contain a context, a distinguished name and a type

3.5.2.2.2 Common Exceptions Pattern

REQ-MT (93) The tool shall provide two types of common exceptions: predefined common exceptions and optional common exceptions.
The predefined common exceptions shall be automatically inserted into all operations by the tool
The optional common exceptions shall be inserted into the operations by the tool on request

REQ-MT (94) All exceptions shall be able to provide a reason and a details description

REQ-MT (95) The following list of predefined common exceptions shall be automatically inserted into all operations by the tool:

- InternalException (default exception)
- AccessDenied
- CommunicationLoss
- InternalError

- InvalidInput
- NotImplemented
- UnableToComply

For a description of the exceptions see chapter 3.5.1.4.3

REQ-MT (96) The following list of predefined common exceptions shall be automatically inserted into all operations by the tool:

- AlreadyInPostCondition
- AtomicTransactionFailure
- CapacityExceeded
- Duplicate
- EntityNotFound
- FilterNotSupported
- InventoryOutOfSync
- NotInValidState
- ObjectInUse
- UnableToNotify

For a description of the exceptions see chapter 3.5.1.4.3

3.5.2.2.3 Iterator Pattern

REQ-MT (97) The tool shall support a common iterator pattern for bulk data transfer

REQ-MT (98) The iterator pattern shall contain the following functionality:

- IteratorInfo
  This is the Info contained in the first response to a bulk based request
- GetNextResponse
  This is the response object to a getNextRequest
- GetNextRequest
  This is the Iterator getNextRequest to retrieve the next batch of replies
- ReleaseRequest
  This is the Iterator release request to release all the associated resources and invalidate the iterator
- HasNext
  Resturns a Boolean; True meaning that additional data is available; false meaning that this is the last information
- Remove
  Deletes the information contained in the iterator
- IsEmpty
  Returns a Boolean; True meaning that iterator has no information; false meaning that the iterator contains still information
- ReleaseResponse
- IteratorNotFound
- InvalidIteratorContext

3.5.2.2.4 Notification Pattern

REQ-MT (99) The tool shall support common notifications

REQ-MT (100) The following types of notifications shall be provided:
- AttributeValueChangeNotification
- ObjectCreationNotification
- ObjectDeletionNotification
- ObjectDiscoveryNotification

REQ-MT (101) All notifications shall at least provide:
- Object identifier
- Object type
- Source time

3.5.2.2.5 Common Operations Pattern

REQ-MT (102) The tool shall support common operations covering create, delete, set and get associated to a single interface class

REQ-MT (103) It shall be possible for the common create operation to define a reference object (existing instance of a Managed Object). The attribute values associated with the reference object instance shall become the default values for those not specified by the also provided create data attribute values

REQ-MT (104) The tool shall support the following types of get operations:
- Single object get
  Getting the values of a single instance
- Multiple entities get
  Get all entities matching a filter; returning the attributes and values of the entities
- Multiple entities get by ids
  Get all entities matching a filter; returning only the identifiers of the entities

REQ-MT (105) The created Object Instances shall be returned

REQ-MT (106) It shall be possible to have all three types of get operations associated to the same interface class

REQ-MT (107) It shall be possible for the common delete operation to provide a list of Object Instances (object identifiers) to be deleted

REQ-MT (108) The delete operation shall return the list of Object Instances that could not be deleted

REQ-MT (109) The tool shall support the following types of set operations:
- Single object set
  Setting a single object; all attributes should be set in an atomic way
- Multiple entities set, best effort
  Setting all entities matching a filter in a best effort way
- Multiple entities set, atomic
  Setting all entities matching a filter in an atomic way

3.5.2.2.6 Filter Pattern

REQ-MT (110) The tool shall support a common filter construct (based on attribute values) for operations requiring the selection of Object Instances

REQ-MT (111) The filter construct shall be a template or a combination of a template and a query filter

REQ-MT (112) A query filter shall be mapped to a string which is implementation technology specific. For example in XML it is filled by the implementation with an XPATH expression. In Java it is filled by a JPA query expression

REQ-MT (113) A template filter shall be mapped to a sequence of attribute matching filters

3.6 Use cases

No use cases are defined in the Modelling and Tooling sub task.

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

STREAM "CONVERGED OPERATIONS"

by NGMN Alliance

Version:	**1.4**
Date:	**2013-08-13**

Version:	**1.4**
Date:	**2013-08-13**
Document Type:	**Final**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Klaus Martiny, Deutsche Telekom**
Contributors:	**T. Benmeriem, Orange** **A. Buschmann, Vodafone D2 GmbH** **J.M. Cornily, Orange** **M. Geipl, Deutsche Telekom** **M. Mackert, Deutsche Telekom** **K. Martiny, Deutsche Telekom** **P. Olli, Telia Sonera** **B. Zeuner, Deutsche Telekom**
Approved by / Date:	**NGMN Board 7th November 2013**

Abstract: Short introduction and purpose of document

Converged Operations (CON) requirements document.

Document History

Date	Version	Author	Changes
2011/07/18	**V 0.92**	Klaus Martiny, Deutsche Telekom Axel Heck, Deutsche Telekom	1st Distribution to partners
2011/07/29	V 0.93	Andreas Buschman, Vodafone D2 GmbH	Some small changes in the FM section
2011/11/24	V 0.94	Yvonne Doernhofer et al	First compilation of updated sections: - Chapter 1 Introduction K. Martiny / M.Mackert DT - Chapter 2 - GENERIC REQUIREMENTS (GEN) A.Buschmann Vodafone D2 - Chapter 3 - HL REQUIREMENTS for CONVERGED OPERATIONS (CON) T. Benmeriem Orange - Chapter 4 - REQUIREMENT MODELING AND TOOLING (MT) B.Zeuner DT - Chapter 5 - REQUIREMENT FAULT MANAGEMENT INTERFACE A.Buschmann Vodafone D2 - Chapter 6 - REQUIREMENTS FOR INVENTORY MANAGEMENT P.Olli Telia, M.Geipl DT, M.Mackert DT - Chapters 7 & 8 – REFERENCES & APPENDIX
2011/11/26	V 0.95	Yvonne Doernhofer, Deutsche Telekom	Editorial Changes
2011/11/27	V 0.959	Manfred Mackert, Deutsche Telekom	Editorial Changes and distribution for review
2011/11/28	V 0.96	Manfred Mackert, Deutsche Telekom	Editorial Changes
2011/11/30	V 0.961	Manfred Mackert, Deutsche Telekom	Update with changes and comments from: • T. Benmeriem for chapter 3 (28.11.2011 and 30.11.2011) • M. Cornily for whole document (28.11.2011) • P. Olli for chapter 6 (30.11.2011)
2011/12/02	**V 0.97**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Editorial Changes in chapter 6 & Internal Review & Distribution to partners
2012/01/22	V 0.98	Yvonne Doernhofer, Deutsche Telekom	Changes FM (2.02) ,GEN part (1.02), InvM part (1.21), FM use cases, Glossary
2012/01/26	V 0.99	Manfred Mackert, Deutsche Telekom	Updates: Introduction, CON, InvM part (1.25); New: chapters 8.1. & 8.2.; editorial cons.: chapter 7 and complete document; Distributed for Final Review
2012/01/31	**V 1.0**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Updates from Final Review & Distribution to NGMN TAC for final approval
2012/02/28	**V 1.1**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update: Introduction with parts of MT Req abstract, FM chapter 5.5.2, Added comment in CON chapter 3
2012/02/28	**V 1.2**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update chapter 1 and 5
2012/04/16	**V 1.3**	Yvonne Doernhofer, Deutsche Telekom	Update REQ-MT (6), REQ-MT (8), REQ-MT (34); Add Editor's note for INVM requirements

2013/08/13	**V 1.4**	Thomas Kulik	Converged Operations (CON) related content moved from the original PH1 documentation (V1.4) to this separate document; numeration of chapters, figures and tables changed; minor corrections

4 High level requirements for Converged Operations (CON)

4.1 Introduction

This section aims at capturing high level requirements for converged operations. The chosen methodology is:

1. Identify Business Scenarios of high interest to operators (as real use cases) from converged operations perspective;
2. Describe basic architecture scenarios as illustrations of where convergence is of high interest for operators. Hence this description is based on any formal / recognized template. It is a free description;
3. Derive, from aforementioned basic scenarios, combined architecture scenarios, i.e. combinations of two or three basic ones. Hence this description is based on any formal / recognized template as well;
4. Describe the Business Converged Operations Scenarios according to ITU-T use case template and map them on either basic or combined architecture scenarios in order to demonstrate the benefit from the converged operations perspective;
5. Extract high-level requirements relative to convergence at three possible levels: Element Management System, Northbound interface, Network Management System;
6. Identify the expected benefits in terms of CAPEX / OPEX reduction.

Target Business Scenarios:

In this release, we are focusing on three Business Scenarios we are considering of high interest to operators and with high priority as well. This list of Business Scenarios will be extended in a new release.

Business Scenarios	
Business Scenarios within a Single Operator Environment	Business Scenario 1: Element Management System (EMS) Shared between Operators' Affiliates
	Business Scenario 2: Network Management System (NMS) Shared between Operators' Affiliates
Business Scenarios within Multi-Operator Environment	Business Scenario 4: RAN Sharing

Target audience:

This section focuses on three main cost elements on which substantial savings can be achieved. Consequently, depending on where potential savings are achievable, the requirements are addressed to three types of players:

Where convergence is expected	Whom requirements are addressed to
Element Management System	Telecom Equipment Manufacturers
EMS northbound interface	SDOs
Network Management System	OSS vendors, IT integrators

The ultimate objective of operators is to lower their CAPEX and OPEX in network operations. Main levers to achieve this are:

- Convergence at system level and/or interface level, on which this section focuses;

- Automated operations. This can be achieved e.g. by introducing self-management concepts in operators' OA&M / OSS solutions (cf. SON with 3GPP and ETSI Industry Specification Group (ISG) for Autonomic Future Internet (AFI)).

Main focus in RAN (Mobile Network) management in the Business Scenarios

From architecture point of view, RAN NEs have wireline connections and, as such, shall be managed as fixed NEs too. However, if we take the example of LTE NEs (eNodeBs), our main focus is on the management aspects of RAN features only. For the wireline connections b/w eNodeBs and the EPC NEs, we focus on the higher layers (S1-MME, S1-U, etc.) rather than on IP level aspects.

4.2 Scope

Referring to the **eTOM Business Process Framework**, requirements identified in this section focus on the process area named "Operations", which covers the core of operational service and resource management. Within the operations process area, the recommendations made in the current section focus on the following functional process groupings:

- Horizontal:
  - o Resource Management & Operations
  - o Service Management & Operations
- Vertical:
  - o Operations Support & Readiness
  - o Fulfilment
  - o Assurance

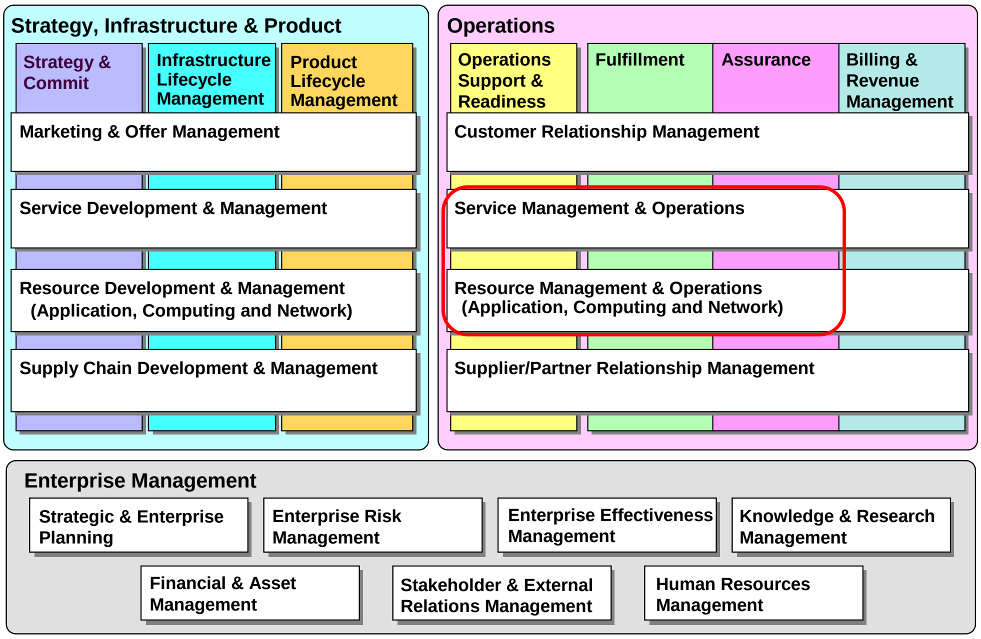


Figure 4-1: Scope of NGCOR within the eTOM framework

Regarding the Mobile network part (RAN) we are considering in the scope, indeed, RAN NEs also have wireline connections and, as such, shall be managed as fixed NEs too. However, our main focus in this Section, is on the management aspects of RAN features (eNodesBs in LTE for instance). For the wireline connections between eNodeBs and the EPC NEs, we focus on the higher layers (S1-MME, S1-U, etc.) rather than on IP level aspects. The whole management aspect of RAN, so called Mobile Backhaul (Mobile nodes as well as their wireline connections) is in the extended scope of this section.

4.3 Architecture Scenarios for Converged Operations

4.3.1 Basic Architecture Scenarios

This section describes "basic converged operations architecture scenarios" which constitute building blocks for elaborating combined architecture scenarios (cf. Section 4.3.2).
This Basic Architecture Scenarios family is broken down into 3 types of scenarios from methodology point of view:

- ***Current Architecture Scenario*** as starting point towards the Target Scenario within a migration path
- ***Intermediate Architecture Scenarios*** paving the way to the Target Architecture Scenario
- ***Target Architecture Scenario*** as ultimate goal of the migration process

4.3.1.1 No Convergence Architecture Scenario (Current Scenario)

Description

In the “no convergence” architecture scenario, convergence does not exist at all, either at the Element Management Layer, or at the EMS Northbound interface (NBI) or at the Network Management Layer, as illustrated in Figure 4-2. This architecture scenario is characterized by:

1. Element Management Systems are dedicated to specific network technologies/ domains/ regions, e.g. the operator’s LTE EMS is different from its 3G EMS, the operator’s EPC core network EMS is different from its IP backhaul EMS;
2. EMS northbound interfaces are specific to network technologies/ domains. Typically, they can be based e.g. on 3GPP IRPs for mobile network domain EMSs and on TMF interface programs for wireline domain EMSs;
3. Operator’s OSS applications are dedicated to network technologies/ domains/ regions and OA&M functional areas. For example, for legacy reasons, it may happen that the network operator has got one OSS application for fault management of its 2G network, another OSS application for fault management of its 3G network and yet another OSS application for fault management of its IP backhaul network.

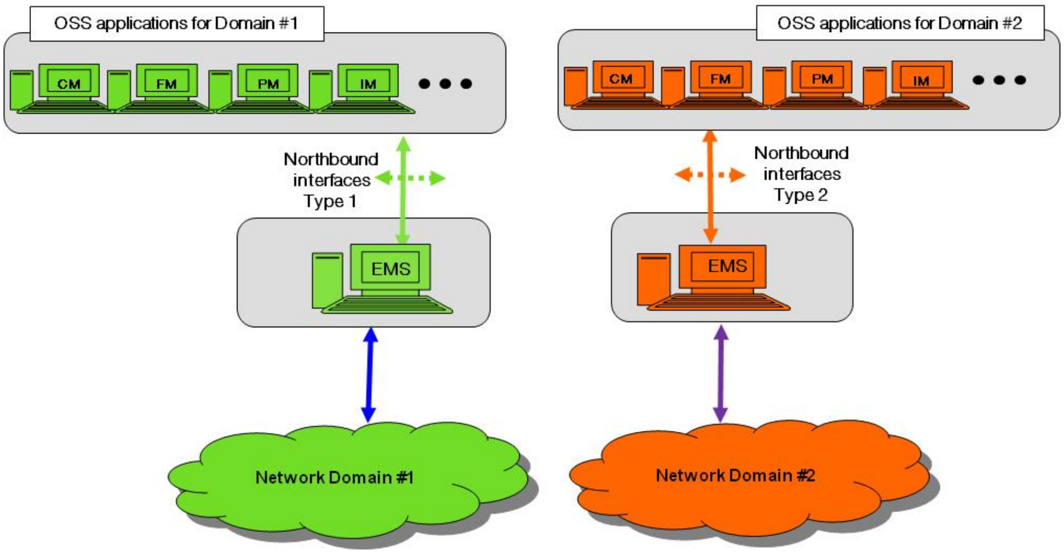


Figure 4-2: Basic Converged Scenario: "No convergence Architecture Scenario" (Current Scenario)

4.3.1.2 Converged Network Management Layer (Intermediate Scenario)

Description

In this scenario:

1. Element Management Systems are dedicated to network technologies/ domains/ regions, e.g. the operator LTE EMS is different from its 3G EMS, or the operator Radio Access Network is different from its IP transport network layer EMS;
2. EMS northbound Interfaces are specific to a given network technology. Typically, they are based on 3GPP IRPs for mobile network domain EMSs or on TMF interface programs for wireline domain EMSs;
3. Convergence has been achieved at the Network Management Layer: the operator has common OSS applications for multiple network technologies/ domains/ regions, for specific OA&M functional areas, e.g.:
    a. One single OSS application for fault management, covering all network domains/ technologies;
    b. One single OSS application for performance management covering all network domains/ technologies;
    c. Etc.

Important:
If the Northbound interface convergence is one aspect of high interest for operators, we need to point out through this scenario that, it is not the only one. CAPEX and OPEX savings are expected from NMS convergence and this is a requirement to OSS vendors and IT integrators.
In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

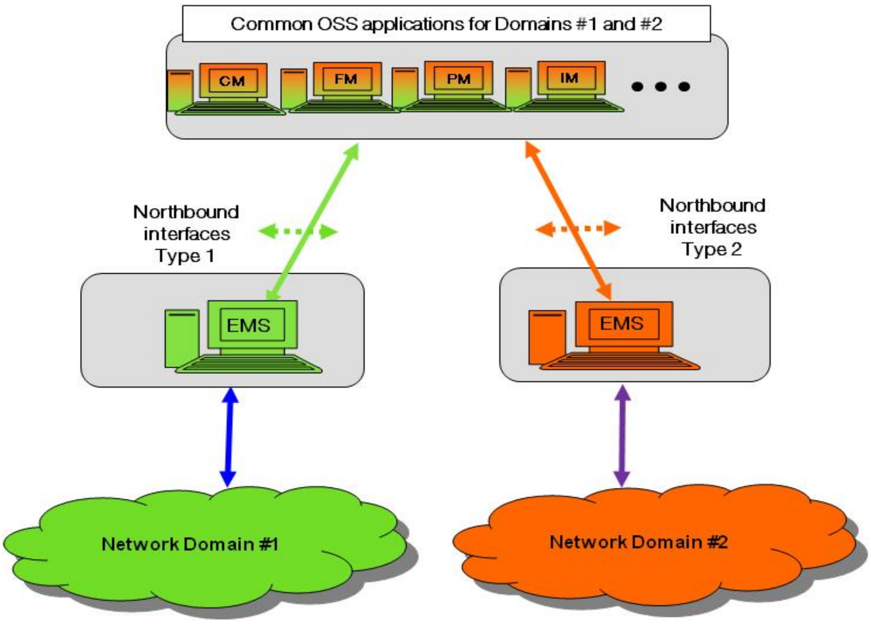


Figure 4-3: Basic architecture scenario "Converged Network Management Layer" (Intermediate Scenario)

4.3.1.3 Converged Element Management Layer (Intermediate Scenario)

Description

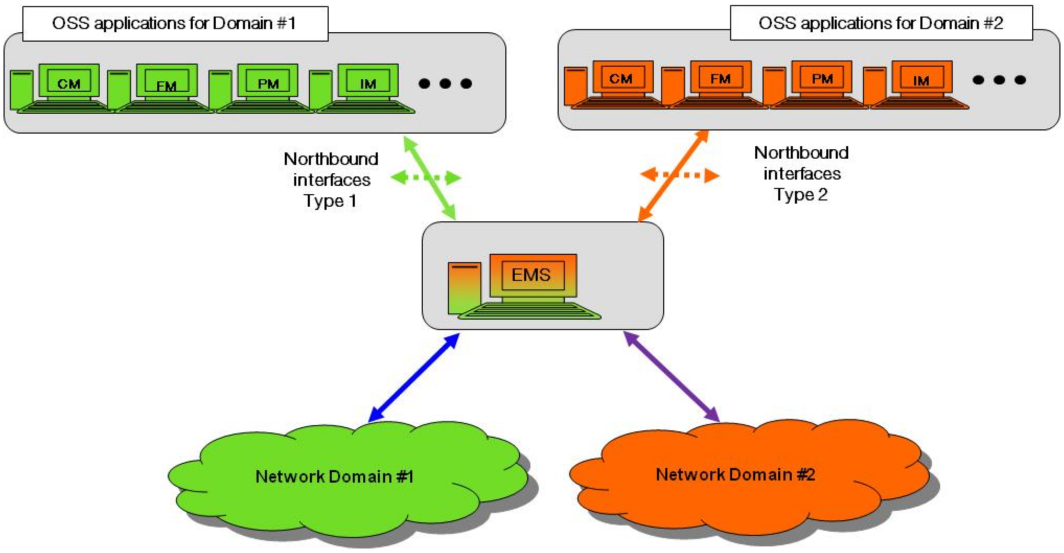


Figure 4-4: Basic architecture scenario "converged element management layer"(Intermediate Scenario)

This scenario is characterized by:

1. Operators get from a given network equipment provider a single Element Management System common to multiple network domains/ technologies/ regions, e.g. vendor X EMS is the same for 2G/ 3G/ LTE Circuit-Switched Core Network/ Packet-Switched Core network/ IMS/ Application Servers, etc.;

2. Vendors' EMSs support various kinds of northbound interfaces, e.g. one set for mobile networks (based on 3GPP IRPs), another set for wireline networks (based on TMF interface programs), meaning that no convergence is achieved at the EMS northbound interface;
3. Operators' OSS network management applications are dedicated to specific network domains/ technologies/ regions and OA&M functional areas, i.e. no convergence at the network management layer.

Important: It shall be noted that using the term "Converged Element Management Layer" in the present document does not necessarily mean having a single EMS platform instance for managing the whole operator network (e.g. for fixed and mobile). Though this might be the case in some environments where the number of managed network elements is limited, reliability/ availability of the EMS is not critical, etc., the architecture scenario depicted above also addresses the case where a network operator manages various network technologies/ domains/ regions using a single EMS product line (not a single EMS instance) for managing network elements of the same vendor.

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

If the Northbound interface convergence is one aspect of high interest for operators, we need to point out through this scenario, that it is not the only one. CAPEX and OPEX savings are expected from EMS convergence and this is a requirement to Network Equipment vendors.

This scenario will involve vendors' product line, therefore, in order to make it happen, a negotiation in a pragmatic way, must be undertaken as early as possible between the two parties operators and vendors.

4.3.1.4 Converged EMS northbound interface (Intermediate Scenario)

This scenario requiring standardized interfaces shall be studied prior to those requiring EMS / NMS convergence. The operators are asking for standards in this section 4.3.1.

Description

In this scenario,

- Vendors offer multiple Element Management Systems on a per network domain/ technology basis;
- Vendors' EMS(s) support one single converged northbound interface:
  - Based on a federated network information model, for both wireless and wireline network domains,
  - Based on an harmonized functional interface per functional area, e.g. one single harmonized functional interface for fault management, for both wireless and wireline network domains, one other single harmonized functional interface for configuration management, etc.;
- Operator has multiple OSS applications for specific network domains/ technologies and OA&M functional area, e.g.:
  - Fault management
  - Performance management, etc.

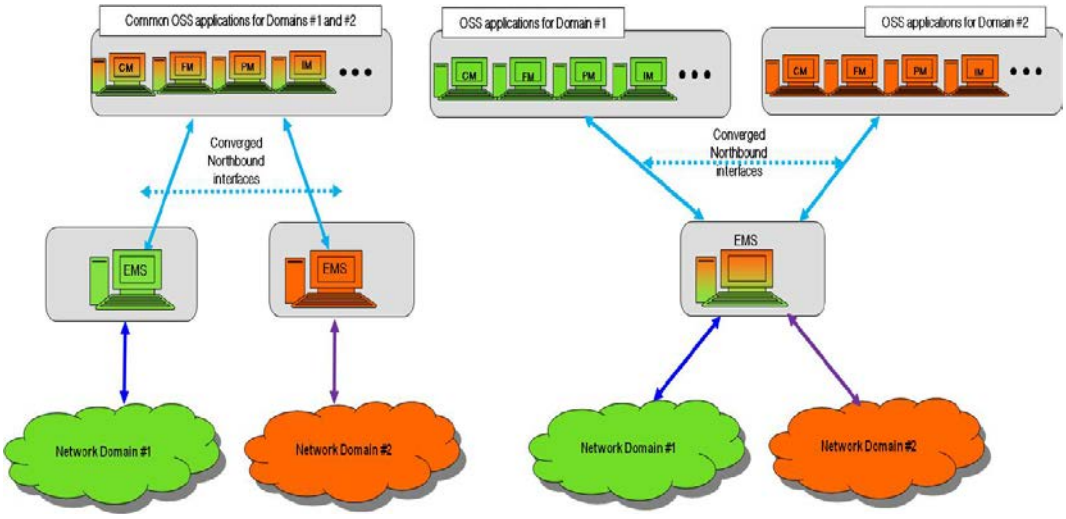


Figure 4-5: Basic Scenario: "Converged EMS northbound interface(s)" (Intermediate Scenario)

It shall be noted that the scenario “converged EMS northbound interface” may apply to the previously described architecture scenarios, as depicted by Figure 4-5.

Important: It shall be noted that one single EMS northbound interface for the management of any kinds of network domains / technologies and for all functional areas is not envisaged here. The converged northbound interface shall be based on federated information and operations models. Please see section “REQUIREMENTS FOR NGCOR MODELLING AND TOOLING” for detailed information about the federated models.

4.3.2 Combined Architecture Scenarios

This Combined Architecture Scenarios family is broken down into 2 types of scenarios from methodology point of view:

- ***Intermediate Architecture Scenarios*** paving the way to the Target Architecture Scenario
- ***Target Architecture Scenario*** as ultimate goal of the migration process

In this section, we defined these "Intermediate" and "Target" Scenarios as possible combinations of basic converged operations architecture scenarios described in Section 4.3.1 within an operator’s environment:

C1: Converged Element Management Layer together with converged EMS northbound interface (Intermediate Scenario)

C2: Converged Network Management Layer together with converged EMS northbound interface (Intermediate Scenario)

C3: Converged Element Management Layer together with converged EMS northbound interface and converged Network Management Layer (Target Scenario)

In this family, the Current Scenario or starting point is implicit in the sense we assume that the operators have obtained from the SDOs the specification of the "Converged Northbound Interface" as depicted at Figure 4-5. Hence, the three "Combined Architecture Scenarios" C1, C2 and C3 are all "Converged Northbound Interface"-capable.

4.3.2.1 C1 - Converged Element Management Layer Together with Converged EMS Northbound Interface (Intermediate Scenario)

This combined architecture scenario combines the basic architecture scenarios described in Section 4.3.1.3 and Section 4.3.1.4.

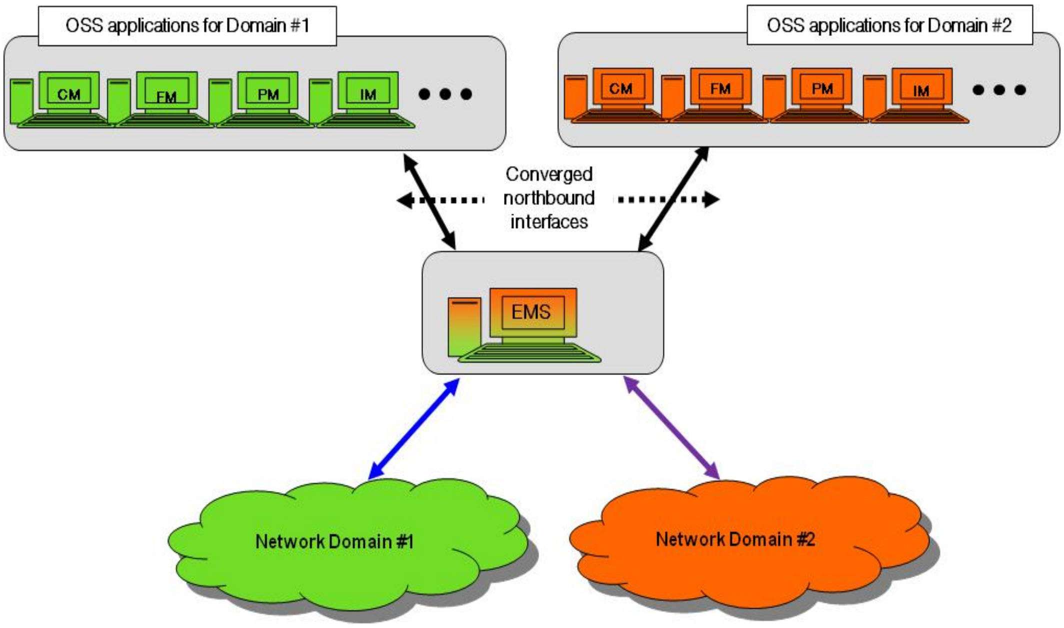


Figure 4-6: Combined architecture scenario "converged EMS and converged NBI" (Intermediate Scenario)

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

This scenario is considered as an "Intermediate Scenario" within the migration path hence paving the way to the target scenario depicted by Figure 4-8. The motivation behind is linked to the need of saving CAPEX and OPEX as highlighted in sub-section 4.3.1.4 beyond the benefit expected by the convergence of the Northbound interface. This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and vendors.

4.3.2.2 C2 - Converged Network Management Layer Together with Converged EMS Northbound Interface (Intermediate Scenario)

This combined architecture scenario combines the basic architecture scenarios described in Section 4.3.1.2 and Section 4.3.1.4. This scenario is considered as an "Intermediate Scenario" within the migration path hence paving the way to the target scenario depicted by Figure 4-8.

The motivation behind is linked to the need of saving CAPEX and OPEX as highlighted in sub-section 4.3.1.3 beyond the benefit expected by the convergence of the Northbound interface.

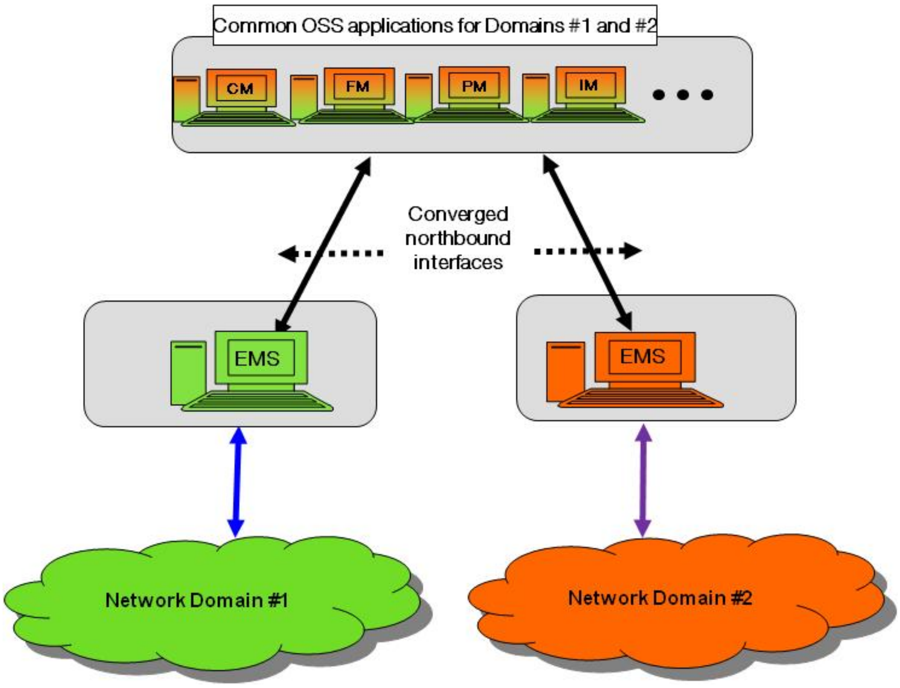


Figure 4-7: Combined architecture scenario "converged network management layer and EMS NBI" (Intermediate Scenario)

In order to make this scenario happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

4.3.2.3 C3 - Converged Element Management Layer Together with Converged EMS Northbound Interface and Converged Network Management Layer (Target Scenario)

The combined converged operations architecture scenario shown in Figure 4-8: Combined architecture scenario "converged northbound interface, EMS & NMS" (Target Scenario) combines the basic converged operations architecture scenarios described in Sections 4.3.1.2., 4.3.1.3 and 4.3.1.4.

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the operators and vendors, in one hand, and between operators and OSS vendors and IT integrators, in the other hand.

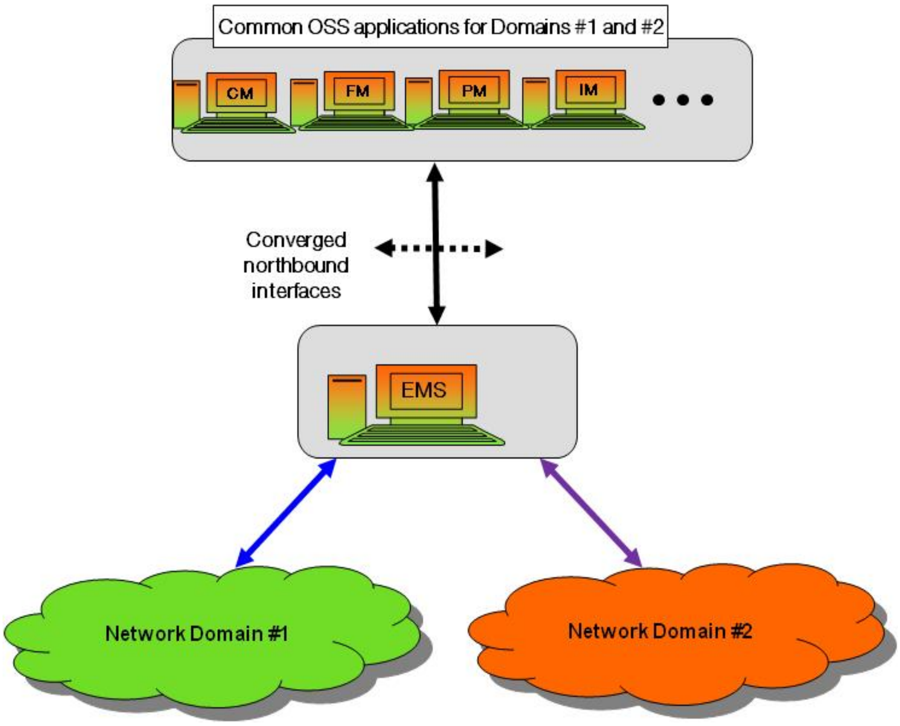


Figure 4-8: Combined architecture scenario "converged northbound interface, EMS & NMS" (Target Scenario)

4.4 Business Scenarios and Requirements wrt. Converged Operations

In this section, we have identified a family of Business Scenarios (as real use cases) of high interest to operators. The list could be extended within the NGCOR scope. In order to demonstrate the benefit from the converged operations perspective, we map them on either Basic or Combined Operations Architecture Scenarios we described in Sections 3.3.1 and 3.3.2.

The whole methodology we adopted in this section is the following:

- Related Use Case description based on ITU-T framework (Goal, Actors & Roles, Assumption, Pr-conditions, Post-conditions…);
- Instantiation and relevance to Basic and / or Combined Operations Architectures Scenarios;
- High-level requirements description;
- Expected benefits (at very high level view, no figures)

4.4.1 Converged Operations Business Scenarios within a Single Operator Environment

4.4.1.1 Business Scenario 1: EMS Shared between Operators' Affiliates

Several affiliates of a network operator share an EMS (mono-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by having one single EMS platform for managing networks belonging to several affiliates of a large service provider deployed over multiple neighbour countries.	
Actors and roles (*)	Several affiliates of a large service provider A near-shore network operation centre, in charge of operating several network domains from affiliates of a single large service provider.	
Telecom resources	Network resources in various countries, all from the same vendor, all from the same network domain, e.g. IMS. A single EMS in a near-shore network operation centre.	
Assumptions	Large service providers have footprints in many countries. Though, in some of these countries, they are incumbent, it also happens that, in some other countries, they are challengers, have limited footprints and have to lower their CAPEX and OPEX to be competitive. In some cases, they deploy a relatively limited number of network elements in each country and put in place a unique organization responsible for operating these domestic networks. The resulting 24/7 shared **Network Operation Centre** (NOC) uses a single EMS for all the nation-wide networks it is in charge of. NOC staff is responsible of daily operation of the various networks.	
Pre-conditions	Each affiliate has deployed its network elements in the country it is responsible for. These network elements are connected to the near-shore shared EMS. All managed network elements and the shared EMS are from a unique vendor.	
Begins when	In some countries, local staff, thanks to their local network operations capabilities, keeps limited capabilities for managing their network.	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		
NOTE – Fields marked with "*" are mandatory for all use case specifications. Other fields are only mandatory when relevant for the specific use case.		

Figure 4-9 depicts this real use case.

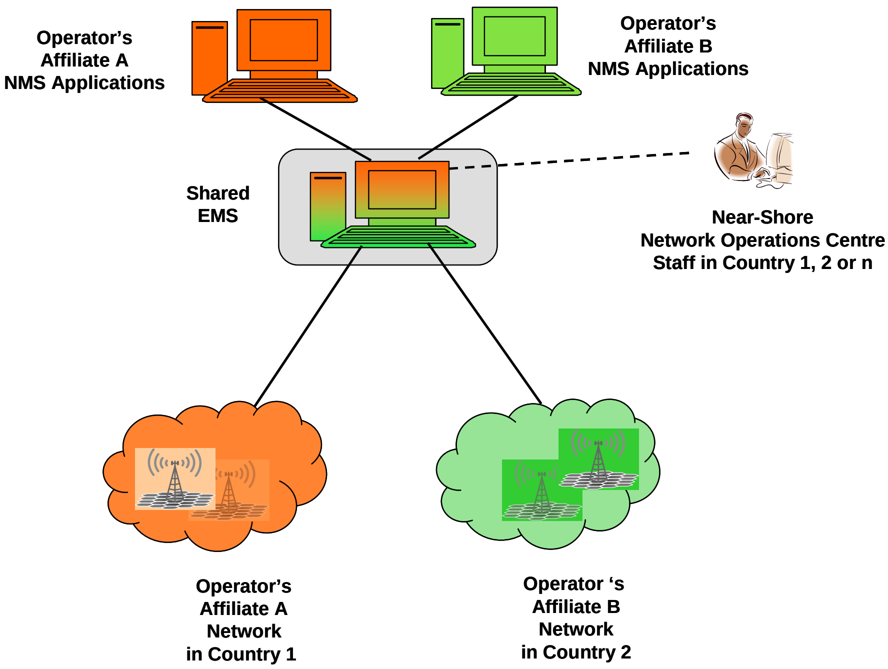


Figure 4-9: Business scenario 1: Single EMS platform managing multiple affiliates' networks in various countries

Instantiation and relevance

This use case makes use of the basic architecture scenario described in Section 4.3.1.3 (Converged Element Management Layer (Intermediate Scenario)).

We do not require having one single EMS instance for the whole network. We require having one single EMS product line for e.g. a given domain (2G/3G/LTE Radio Access Network) or, better, multiple domains (mobile + fixed). Besides, our requirement is for NEs coming all from a given vendor. The multi-vendor aspect is left to the NMSs.

This scenario will involve vendors' product line assuming that converged Northbound Interface is already implemented by vendors. In order to make it happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the operators and vendors,

High-level requirements

REQ-CON (1) Vendors' EMS shall be able to manage network elements belonging to several network operator affiliates. In a minimal configuration, it shall be able to manage multiple network domains / technologies, e.g. it shall be able to cover not only multiple radio access technologies but shall also enable network operators to manage their wireless and wire line network domains in a unified way.

REQ-CON (2) Alarms coming from operator affiliates' domestic network elements up to the shared EMS are handled by shared NOC staff. The shared EMS shall be able to filter such alarms and forward them to the relevant operator affiliate OSS FM application, either for information only or for action (acknowledge, clear, etc.). All alarm-related information exchanges between the shared EMS and the affiliates' OSS FM applications shall comply with standardized specifications.

REQ-CON (3) Operator affiliates shall be able to configure their own network elements from their own OSS CM application(s). The shared EMS shall ensure isolation of configuration action requests coming from the affiliates' OSS CM applications. All configuration management related information exchanges between the shared EMS and the affiliates OSS CM applications shall comply with standardized specifications.

REQ-CON (4) Operator affiliates shall be able to collect performance management counters/ KPIs related to their own network elements. They shall be able to trigger, from their own OSS PM application, performance measurement jobs for their own purpose, and collect related PM measurements within their OSS PM application. All performance management related information exchanges between the shared EMS and the affiliates' OSS PM Applications shall comply with standardized specifications.

REQ-CON (5) Operator affiliates shall be able to inventory resources related to their own network elements. They shall be able to retrieve, from their own OSS InvM application, all available inventory data. All inventory management related information exchanges between the shared EMS and the affiliates' OSS InvM applications shall comply with standardized specifications.

Expected benefits:

CAPEX savings:

- One EMS hardware platform instead of N (N being the number of affiliates);
- In case of highly available (HA) EMS platform, only one is needed instead of N

OPEX savings:

- One team for network operations instead of N
- EMS validation test phase (unitary + end-to-end) to be performed once instead of N times
- Common processes for N affiliates instead of 1 per affiliate, for e.g. backup and restore, software and hardware upgrade management, license management, etc.

4.4.1.2 Business scenario 2: Network Management Level Applications Shared Between Operators' Affiliates

Several affiliates of a network operator share NMS applications (multi-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by having one single set of NMS applications for managing networks belonging to several affiliates of a large service provider deployed over multiple neighbour countries. Large network operators have their networks deployed in several countries. Instead of developing a dedicated OSS application in each country for e.g. fault management, it is common that they develop a single OSS application for multiple countries and/ or multiple domains and/ or multiple technologies. Such operator-wide OSS applications are based on a kernel and possible adaptations due to local and/ or domain-specific and/ or technology-specific requirements.	
Actors and roles (*)	Several affiliates of a large service provider A near-shore Network Operation Centre, in charge of operating several network domains from affiliates of a single large service provider	

Several affiliates of a network operator share NMS applications (multi-vendor environment)

Use case stage	Evolution/Specification	<<Uses>> Related use
Telecom resources	Network resources in various countries, from various vendors, all from the same domain, e.g. IMS. One EMS per country. A single set of NMS applications in a near-shore Network Operation Centre.	
Assumptions	Large service providers have footprints in many countries. Though, in some of these countries, they are incumbent, it also happens that, in some other countries, they are challengers, have limited footprints and have to lower their CAPEX and OPEX to be competitive. In some cases, they deploy a relatively limited number of network elements in each country and put in place a unique organization responsible for operating these domestic networks. The resulting 24/ 7 shared Network Operation Centre (NOC) uses a single set of NMS applications for all the nation-wide networks it is in charge of. NOC staff is responsible of daily operation of the various networks.	
Pre-conditions	Each affiliate has deployed its network elements in the country it is responsible for. These network elements are connected to their local EMS. All EMSs are connected to near-shore NMS applications. Each affiliate may have its own policy with regard to the vendor of their managed network elements and corresponding EMS.	
Begins when	In some countries, local staff, thanks to their local network operations capabilities, keeps some capabilities for managing their network.	
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		

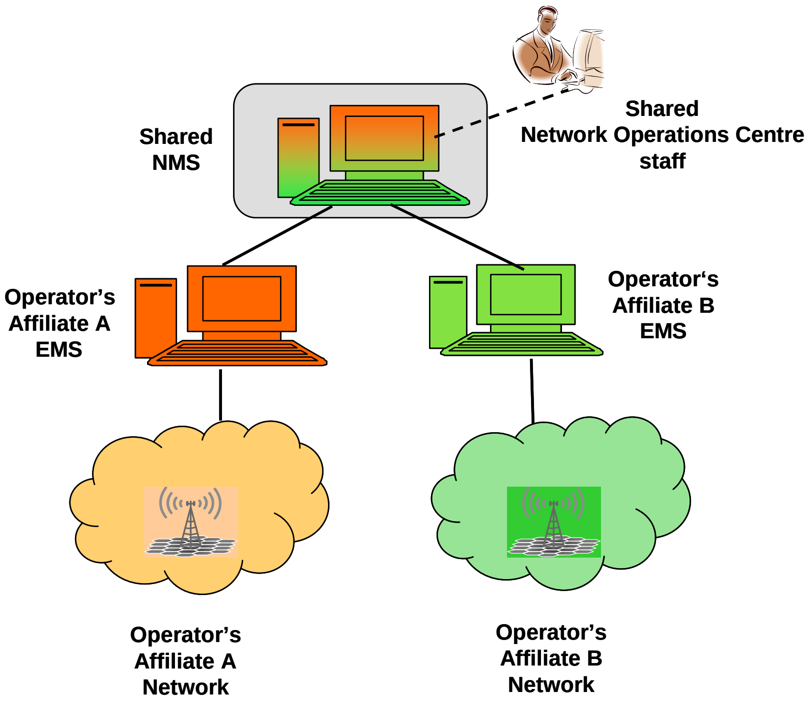


Figure 4-10: Business scenario 2: Common NMS applications for multiple affiliates

Instantiation and relevance

This use case makes use of the basic architecture scenario described in Section 4.3.1.2 (Converged Network Management Layer).

In order to make this scenario happen, a negotiation, in a pragmatic way, must be undertaken as early as possible between the two parties: operators and OSS vendors and IT integrators.

High-level requirements

REQ-CON (6) Network management applications shall be, up to the maximum, common to multiple network domains / technologies. They shall be based on a kernel, common to multiple network domains / technologies, and possibly technology-specific management capabilities.

REQ-CON (7) In order to lower the costs of integration of the various EMSs to the single set of NMS applications, it is required that all EMSs offer the same set of northbound interface(s), based on a standardized federated model (cf. Sub-Task Modelling & Tooling)

Expected benefits

3. CAPEX savings:
    - One set of NMS hardware platforms per application instead of N (N being the number of affiliates);
    - In case of highly available (HA) NMS platform, only one is needed instead of N

4. OPEX savings:
    - NMS applications release management is done centrally instead of locally

4.4.1.3 Business scenario 3: Converged Service Management Applications

Instantiation and relevance

End-to-end service configuration and activation from a unique OSS application is key for service providers. In the future, when a new fixed and mobile IMS VoIP subscriber is to be provisioned, the following list of NEs will have to be provisioned:

- Home Gateway
- IMS HSS
- HLR
- EPC HSS
- SPR/PCRF
- Possibly FemtoCell.

In order to enable end-to-end provisioning in a timely manner and error-freely, having a single service configuration and activation application capable of orchestrating provisioning requests to various underlying domain specific provisioning applications will help in reducing OPEX and improve customer satisfaction.

High-level requirement

REQ-CON (8) Operators expect common service management applications for the following functional processes, belonging to service operation and management:

- Service configuration and activation
- Service problem management
- Service quality management

Expected benefits

OPEX savings:

- o Due to simpler way to manage subscribers from a single point (provisioning, monitoring, tracing, etc.)

4.4.2 Converged Operations Business Scenarios within Multi-Operator Environment

4.4.2.1 Business Scenario 4: RAN Sharing with EMS shared amongst Operators

RAN Sharing

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal (*)	The objective is to lower CAPEX and OPEX by sharing Radio Access Network elements between multiple operators in a given country.	
Actors and roles (*)	Several network operators sharing their RAN. Regulator A "Master Operator", in charge of operating the shared network elements.	
Telecom resources	Radio Access Network resources shared between several operators in a single country, all from the same vendor. One single EMS under the responsibility of the Master Operator. Sharing Operators, having their own set of NMS applications.	

RAN Sharing

Use case stage	Evolution/Specification	<<Uses>> Related use
Assumptions	Shared Network Elements have an OA&M connection to the common EMS. Sharing Operators have no direct OA&M connection to the shared network elements. The EMS is under the full responsibility of the Master Operator. The EMS has interfaces to Sharing Operators' NMS applications.	
Pre-conditions		
Begins when		
Step 1 (*) (M|O)		
Step n (M|O)		
Ends when (*)		
Exceptions		
Post-conditions		
Traceability (*)		

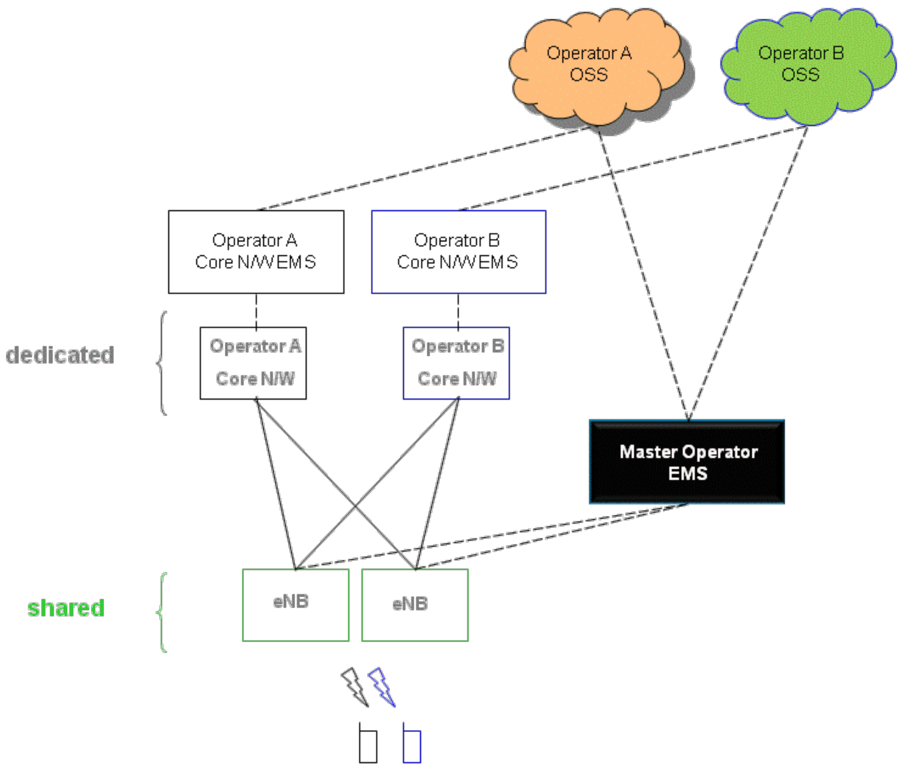


Figure 4-11: Business Scenario 4: RAN Sharing

Instantiation and relevance

This use case is an instantiation or an implementable scenario of generic operations use case depicted in Figure 4-6 which requires a converged EMS and Converged Northbound interface.

High-level requirements

REQ-CON (9) It shall be possible that the "Master Operator" EMS and "Sharing Operators" NMS applications communicate with each others through a standardized northbound interface. This interface shall be "online", i.e. not only based on offline file exchange. These exchanges shall be secured to ensure privacy of information. The Master Operator EMS shall be able to filter information exchanged with Sharing Operators' NMSs based on unique identifiers (PLMN Id, etc.). Standardized northbound interfaces shall enable such a use case.

Expected benefits

- CAPEX savings:
  - One single EMS platform to be deployed (HW + SW), instead of N (N being the number of Sharing Operators)
- OPEX savings:
  - Daily operations of the shared network are common. Sharing Operators can rely on the Master Operator for resource management and operations (only selected types of alarms, KPIs, etc. can be forwarded to each Sharing Operator, based on contract agreements).

4.4.3 General Requirements

4.4.3.1 Harmonized EMS Northbound Interfaces

High-level requirements

REQ-CON (10) Vendors' EMS shall offer a unique set of management capabilities at its northbound interfaces. It is expected that EMS northbound interfaces are implemented according to the following rules:

- Network resource models for various network domains are built on a standardized federated network resource model, i.e. network resource model for wire line network domains shall not be 100% different from network resource models for wireless network domains.
- Functional interfaces for wire line and wireless networks shall be similar for at least configuration management, fault management, performance management, inventory management, software management. EMS northbound Interface shall offer common management capabilities to the operator, regardless of the network domain.
- It is of primary importance that EMS northbound interface fully implements:
  - standardized northbound interfaces firstly and
  - clearly identifiable, vendor-specific extensions to capture vendors' own set of parameters and/or value added management capabilities. Vendor's specific capabilities shall be implemented as extensions
- EMS northbound interface shall be based on Web Services.

Expected benefits:

CAPEX savings:

- Integration of a new EMS in the Operator's environment is simpler, faster and thus cheaper

OPEX savings:

- Evolutions of already deployed EMSs northbound interfaces in the Operator's environment are handled more simply, fast, cheaply

4.4.4 To Which Players the Requirements are addressed

As indicated earlier, the requirements formulated in Section 3.1 are addressed to three types of players in order to be translated into standards **and** implementations, so as to meet operators' needs in terms of CAPEX and OPEX reduction:

- SDOs and Organisations
- OSS vendors / integrators
- Telecom equipment manufacturers.

Table 4-1: Converged Operations Requirements - Whom these requirements are addressed to summarizes this classification.

CON	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CON (1)	X	X	
REQ-CON (2)	X	X	
REQ-CON (3)	X	X	
REQ-CON (4)	X	X	
REQ-CON (5)	X	X	
REQ-CON (6)			X
REQ-CON (7)	X		
REQ-CON (8)			X
REQ-CON (9)	X		
REC-CON (10)	X		

Table 4-1: Converged Operations Requirements - Whom these requirements are addressed to

Comments

From the discussion with the partners, a clarification wrt requirements vs deployment scenarios, implementation was requested.. Indeed, the high level requirements listed in this table are implementation neutral. The reason why, each operator can implement, and map them with regard to his own needs and organisation.
Here after, we try to make illustrations for Business Scenario 2.

Illustration 1
We can imagine a centralized structure that could perform the management of the Affiliates' EMSs and the shared NMS.In this case, the SW of EMSs and NMS can be located in this centralized structure.
The staff in charge of the networks management in the affiliates can remotely access to the EMSs and NMS to retrieve their own data.

Illustration 2

The network management can be provided as a service “SaS”. In this case, a third party can provide SW and HW for the management purpose as well as hosting facilities. The operator staff in their OMCs can access remotely and selectively (through filtering process) to these SW functions ass well as to results processed. The third party can also collect and retrieve data from the operator’s equipment. This “Full” SaaS mode looks like to outsourcing Business Scenario the NGCOR as identified.

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

STREAM "FAULT MANAGEMENT"

by NGMN Alliance

Version:	**1.4**
Date:	**2013-08-13**

Version:	**1.4**
Date:	**2013-08-13**
Document Type:	**Final**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Klaus Martiny, Deutsche Telekom**
Contributors:	**T. Benmeriem, Orange** **A. Buschmann, Vodafone D2 GmbH** **J.M. Cornily, Orange** **M. Geipl, Deutsche Telekom** **M. Mackert, Deutsche Telekom** **K. Martiny, Deutsche Telekom** **P. Olli, Telia Sonera** **B. Zeuner, Deutsche Telekom**
Approved by / Date:	**NGMN Board / 7th November 2013**

Abstract: Short introduction and purpose of document

Consolidated document from all requirement documents by the sub tasks GEN; FM; InvM; CON and MT

Document History

Date	Version	Author	Changes
2011/07/18	**V 0.92**	Klaus Martiny, Deutsche Telekom Axel Heck, Deutsche Telekom	1st Distribution to partners
2011/07/29	V 0.93	Andreas Buschman, Vodafone D2 GmbH	Some small changes in the FM section
2011/11/24	V 0.94	Yvonne Doernhofer et al	First compilation of updated sections: - Chapter 1 Introduction K. Martiny / M.Mackert DT - Chapter 2 - GENERIC REQUIREMENTS (GEN) A.Buschmann Vodafone D2 - Chapter 3 - HL REQUIREMENTS for CONVERGED OPERATIONS (CON) T. Benmeriem Orange - Chapter 4 - REQUIREMENT MODELING AND TOOLING (MT) B.Zeuner DT - Chapter 5 - REQUIREMENT FAULT MANAGEMENT INTERFACE A.Buschmann Vodafone D2 - Chapter 6 - REQUIREMENTS FOR INVENTORY MANAGEMENT P.Olli Telia, M.Geipl DT, M.Mackert DT - Chapters 7 & 8 – REFERENCES & APPENDIX
2011/11/26	V 0.95	Yvonne Doernhofer, Deutsche Telekom	Editorial Changes
2011/11/27	V 0.959	Manfred Mackert, Deutsche Telekom	Editorial Changes and distribution for review
2011/11/28	V 0.96	Manfred Mackert, Deutsche Telekom	Editorial Changes
2011/11/30	V 0.961	Manfred Mackert, Deutsche Telekom	Update with changes and comments from: • T. Benmeriem for chapter 3 (28.11.2011 and 30.11.2011) • M. Cornily for whole document (28.11.2011) • P. Olli for chapter 6 (30.11.2011)
2011/12/02	**V 0.97**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Editorial Changes in chapter 6 & Internal Review & Distribution to partners
2012/01/22	V 0.98	Yvonne Doernhofer, Deutsche Telekom	Changes FM (2.02) ,GEN part (1.02), InvM part (1.21), FM use cases, Glossary
2012/01/26	V 0.99	Manfred Mackert, Deutsche Telekom	Updates: Introduction, CON, InvM part (1.25); New: chapters 8.1. & 8.2.; editorial cons.: chapter 7 and complete document; Distributed for Final Review
2012/01/31	**V 1.0**	Klaus Martiny, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Updates from Final Review & Distribution to NGMN TAC for final approval
2012/02/28	**V 1.1**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update: Introduction with parts of MT Req abstract, FM chapter 5.5.2, Added comment in CON chapter 3
2012/02/28	**V 1.2**	Yvonne Doernhofer, Deutsche Telekom Manfred Mackert, Deutsche Telekom	Update chapter 1 and 5
2012/04/16	**V 1.3**	Yvonne Doernhofer, Deutsche Telekom	Update REQ-MT (6), REQ-MT (8), REQ-MT (34); Add Editor's note for INVM requirements

2013/08/13	**V 1.4**	Thomas Kulik	Fault Management (FM) related content moved from the original PH1 documentation (V1.4) to this separate document; numeration of chapters, figures and tables changed; minor correction

5 Requirements for Fault Management Interface (FM)

5.1 Introduction

Today's Fault Management interfaces between Element Management Systems (EMS) and Network Management Systems (NMS) are based on a large variety of different technologies and standards. Each EMS which has been delivered to Service Providers (SP) in the past uses his own specific interface type and implements element-specific extensions and behaviour, which evolve over time, leading to a continuous need for upgrades on EMS side and to related adaptations/ upgrades on NMS side. SPs estimate of one major upgrade project per EMS per two to three years. The cost and effort for the EMS upgrades are often covered by the budgets for the related network element upgrades. But there are additional costs and effort for the related upgrade adapters/access-modules in the NMS-FM system, although the main requirements on such an interface are almost the same for the last ~ 15 years.

So SPs are driven by vendors to start interface upgrade projects, perform complex and time consuming type acceptance to ensure the needed quality, train administrators and project managers, etc. to get at least no additional value.

The authors of the FM section strongly believe, that there is potentially huge business benefit in using a common officially standardized technical approach, enabling the re-use of the same interface for different EMSs, enabling the planned exchange/ upgrade of the NMS-FM system and enabling us to stop vendor driven upgrades of interfaces which deliver no or small additional value.

So, the FM interface “plug & play” concept, described in the FM section, will be used as a goal for next generation service assurance.

In today's market, service providers aim to ever decrease the time-to-market of new and enhanced services in a cost-conscious manner. As a consequence, the need arises for existing OSS/ BSS infrastructure applications to adapt in an ever increasing pace. This affects OSS applications themselves and also increasingly their integration. Furthermore, there is a growing demand for automation of business processes at service providers, especially in the area of network/service operations to improve operational efficiency. This leads to the need for improved integration of OSS as a common demand from service providers. An integration strategy using SOA concepts, commonly adopted interface standards and NGOSS concepts like eTOM and SID might have the potential to deliver the needed technical basis for real life, standardized OSS integrations.

In the past, Service Providers often over-specified the tenders for FM interfaces and, on the other hand, opened to many degrees of freedom for the implementation of the interface. So they missed the opportunity to describe a simple, useable, maintainable interface, with a clear responsibility assignment between EMS and NMS.

Most of the existing integrations between Element Management systems and Network Management systems are based on proprietary point-to-point interfaces although vendors offer “standard” interfaces such as SNMP, CORBA, etc., which are adapted to their applications. In a real integration scenario these interfaces need a lot of customization to fulfil the business requirements and to allow the communication between different proprietary OSSs because each of these applications follow its own business process, internal logic and semantic. Usually application needs to know a part of the business logic of system B (and vice versa) to be able to implement the interface. This situation ends with the implementation of very specific interfaces with dependencies on the integrated OSS.

This means, re-use of interfaces or dedicated parts of the interfaces in other integration scenarios is not possible. So, there is a need for a standardized interface, which delivers the semantic connectivity and not only the underlying transport mechanisms, which helps to provide out-of-the-box interoperability and more flexible integration.

See also chapter 8.1 “Abstract” from NGMN Top OPE Requirements Version 1.0:

> “Although it is not the intention of the current document to specify implementation details, the operators expect the industry to jointly develop and use common standards, which deliver the semantic connectivity and not only the underlying transport mechanisms. The goal is to achieve out-of-the-box interoperability and more flexible integration, as well as the re-use of the same interfaces between OSS/BSS and the Network or EMS. Based on existing frameworks, provided by the standardization bodies, solutions should be implemented that support plug & play behaviour of network and OSS/BSS infrastructure. This will lead to more open interfaces to allow for 3rd party software integration. Amongst others this implies usage of common data models, e.g. based on SID, interface standards, such as SNMP and XML (if appropriate), and state-of-the-art technologies as SOA, web services, etc. As those standards are evolving over time, the operators resign from specifying exact software versions and implementation details. Our aim is to ensure upwards and downwards compatibility to ease integration of multi-vendor, multi-technology systems for all management areas.”

5.2 Scope

The main scope is the specification of the business requirements and related semantics, which describes the interaction of element management systems to network management (umbrella Fault Management) systems to exchange event/alarm information. The interface requirements support converged networks, that means that wireless and wireline networks are in scope.

In addition to this, there are specific requirements for the Element Management Systems and the Network Management Systems to use the capabilities of the specification in order to support the business requirements.
Please consider that different application topologies have to be supported by the interface:

- Several NMSs can be connected to the EMSs, e.g. operational NMS and test NMS
- An NMS can serve as an EMS (e.g. a technology domain specific NMS, which acts like an EMS to upper level NMS

5.3 Objective

The objective of the FM section is to deliver the specification of the major requirements for a unified, re-useable Fault Management Interface for the alarm interface between EMS → NMS. The FM section will serve as an input for standardization activities which address the FM interface standard.

The FM interface requirements are generic for FMC. They are completely independent from the network/service type which will be monitored by the EMS. So the FM interface requirements are valid for wireless and wireline networks, as well as for IT systems or service platforms.

Please consider that the FM section contains only mandatory requirements to deliver a basic, simple and cost efficient FM Interface. Additional requirements might be added later on as “optional”. (All requirements are “mandatory”, as long as they are not explicitly marked as “optional”). These requirements may not harm the business goals of the basic, mandatory requirements to achieve a simple, cost efficient and easy to integrate FM interface. It must be possible to implement an interface, which contains functionalities in line with the optional requirements, in a mixed mode with the simple/basic interfaces, which contain the mandatory requirements in this section, without any change for simple/basic interface (e.g. the EMS delivers just the mandatory interface functionality and the NMS delivers also the optional part of the interface. In that case, the interface will use only the mandatory functionality, without any change on the EMS or NMS interface functionality).

Benefit and Drivers

The main benefit is achieved, as soon as the specification can be re-used to implement similar interfaces for different integration scenarios, to connect different EMS to NMS applications without creating a complete new implementation of the interface. The goal is to improve efficiency (in terms of cost and effort) for the integration of new EMS and to reduce cost and effort to maintain each single interface in a different way. Another benefit comes from the fact, that a real decoupled approach will reduce the effort to adapt both communication partners, in case there is a need to upgrade just one of the partners.

Saving potential:

- The support for a better level of standardization of the itf-N will reduce the integration effort between EMS and NMS (OSS) during the implementation and the life cycle of network technologies and related EMS.

Possible issues for guidance:

- “Plug & Play” integration of EMS into the OSS domain (no additional cost and effort during the implementation and the life cycle of network technologies and related EMS)
- De-coupling of EMS – OSS domains (changes on EMS or on NE may not lead to changes on OSS domain)
- Re-use of OSS clients of the interfaces

5.4 Methodology

It's the intention to describe the interface capabilities from business point of view, without technology specific requirements. That means, that these requirements reside on the semantically layer and not on protocol specifications. Nevertheless, there are some assumptions which might have an impact on the selected technology, e.g. the de-coupling of the interface specification (which is a basic requirement to support re-usability, exchange of SW versions, etc.) might have an impact on the technology. Furthermore the requirements have to be independent from the tool selection, so that they may not depend on specific tool capabilities.

Explanation of Prioritisation

Essential	→	The standard must fulfil this requirement. It is absolutely necessary and indispensable.
Major	→	The standard should fulfil this requirement. This is an important requirement. The value of the standard is reduced, if it cannot be fulfilled.
Minor:	→	The standard can fulfil this requirement (but must not). This is an optional requirement.

5.5 Requirements

5.5.1 Non-Functional Requirements for Fault Management Interface

The following topics describe some core business driven requirements for the EMS → *"alarm"* → NMS interface, independent from functional requirements. These requirements are not specific for the FM Use Cases and can be used as core "non-functional" requirements for other types of interfaces as well.

Note: The detailed descriptions of these "non-functional requirements" have been shifted into the Generic-Next-Generation-Converged-Operational-Requirements (GEN) section, because they are valid for most types of OSS interfaces.

The following list describes the prioritization of requirements from the GEN section especially for the FM Interface section:

REQ-GEN	Name	Priority
1	**Plug & Play**	**Major**
2	**Useful**	**Major**
3	**Re-Usable / Generic**	**Essential**
4	**Simple**	**Essential**
5	**Flexible / Extensible**	**Major**
6	**Fine grained (as far as needed)**	**Major**
7	**Standardized / Open**	**Essential**
8	**Mature / Stable**	**Major**
9	**De-coupled**	**Essential**
10	**Evolutionary**	**Major**
11	**Independent**	**Essential**
12	**Certifiable**	**Major**
13	**Compatible**	**Essential**
14	**Interoperable**	**Major**
15	**Scalable**	**Essential**
16	**Secure**	**Minor**
17	**Reliable**	**Essential**
18	**Interface robustness**	**Essential**
19	**Simple trace and logging**	**Essential**
20	**1:1 Relation between Event MO Instances and Inventory MO Instances**	**Major**
21	**"MO Instance" Attribute Information Structure for EMS ←→ NMS Event Interface**	**Major**
22	**M : N Connectivity**	**Major**

5.5.2 Functional Requirements for Fault Management Interface

The functional requirements for the FM interface describe the mandatory and some optional requirements for the Fault Management interface between EMS and NMS from an FM business point of view. The optional requirements are not intended to be complete, but mention some of the most likely needed optional features for **the** interface. It does not define the functional capabilities needed on EMS or the NMS itself, although there are some requirements in this areas mentioned to serve as a "basic" information to understand the needed capabilities on system level (they can be used for EMS/NMS vendor selection processes).

Please consider: Several functional requirements have been shifted into the Generic-Next-Generation-Converged-Operational-Requirements (GEN) section, because they are valid for most types of OSS interfaces.

Examples listed here are:

- Trace and Logging
- "Managed Object Instance" Attribute Information Structure
- M : N Connectivity
- 1:1 Relation between Event Managed Object Instances and Inventory Managed Object Instances

REQ-FM (1) X.733 Event/Alarm Attributes

The event/alarm must contain structured information according to the X.733 specification

<u>Description:</u>

- The attributes of the event/alarm object shall follow the X.733 standard definition (for details see X.733 specification – see References)

<u>Short overview of attributes:</u>

- The yellow marked attributes are <u>mandatory</u> for the interface. So they have to contain a useable value (this can be empty, if this is a useable value). The other attributes are optional in this specification. The interface and the connected systems must work in a proper way, if the optional attributes do not contain any value. Additional explanation: The meaning of "useable" used in this context is that the content should deliver a real information for operations, not just something like an unreadable system message without any meaning for the operator. Furthermore, attributes like Event Time may not be empty. They must contain a date.
- Please consider:
    - That the allowable values for the Managed Object Class should be based on classes defined in the Federated Model (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**)
    - That the value for the Managed Object Instance should enable to identify an object instance to which an alarm refers to via a configuration management interface.
    - That the standardization should eliminate (or minimize) the need of using vendor specific problem identification. The standardization should leverage the Federated Model (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**) to provide the library of problems per classes of object which may be defined for different network domains, but should not be vendor specific.

Parameter name	Req/Ind	Rsp/Conf
Invoke identifier	P	P
Mode	P	---
Managed object class	P	P
Managed object instance	P	P
Event type	M	C(--)
Event time	P	---
Event information		---
Probable cause	M	---
Specific problems	U	---
Perceived severity	C	---
Backed-up status	U	---
Backu-up object	C	---
Trend indication	U	---
Threshold information	C	---
Notification identifier	U	---
Correlated notifications	U	---
State change definition	U	---
Monitored attributes	U	---
Proposed repair actions	U	---
Additional text	U	---
Additional information	U	---
Current time	---	P
Event reply	---	---
Errors	---	P

→ The content of the Eventtype and the Probablecause should follow the recommendation in ITU-T M3703 Annex A Table A.1 and Annex B Table B.1 and B.2. to enhance the operational value of these attributes.

→ The Notification ID must be unambiguous to resolve the clear-problem and the synchronization problem (see specific requirements later on)

→ Additional information from Service Quality Management (SQM) oriented data sources (e.g. KPI, DATASOURCE, STIME, etc. …) will be part of the „Additional Text" attribute.

Table 5-1: Event/Alarm Attributes

Special remarks:

* The event/alarm has to be encoded in ASCII

* DateAndTime Format: "yyyyMMddhhmmss.s[Z|{+|-}HHMm]"

where:

yyyy	"0000".."9999"	year
MM	"01".."12"	month
dd	"01".."31"	day
hh	"00".."23"	hour
mm	"00".."59"	minute
ss	"00".."59"	second
s	".0"..".9"	tenth of second (set to ".0" if EMS or ME cannot support this granularity)
Z	"Z"	indicates UTC (rather than local time)
{+|-}	"+" or "-"	delta from UTC
HH	"00".."23"	time zone difference in hours
Mm	"00".."59"	time zone difference in minutes.

* Event type is very useful for operators to locate the alarms and decide which professional team to do trouble shooting. Thus more event type should be added according to network operation requirement. Refer to ITU-T M.3703, event subtype are defined as following table.

Event Types	Explanation
Communications Alarm	An alarm of this type is associated with the procedure and/or process required conveying information from one point to another (ITU-T Recommendation X.733).
Communications_Signalling and IP Alarm	An alarm of this type is associated with signalling and IP failure, e.g.SS7 protocol error. It is a subtype of Communications Alarm.
Communications_ Interface Alarm	An alarm of this type is associated with interface error, e.g.physical interface of communication error. It is a subtype of Communications Alarm.
Processing Error Alarm	An alarm of this type is associated with a software or processing fault (ITU-T Recommendation X.733).
Environmental Alarm	An alarm of this type is associated with a condition related to an enclosure in which the equipment resides (ITU-T Recommendation X.733).
Quality of Service Alarm	An alarm of this type is associated with degradation in the quality of a service (ITU-T Recommendation X.733).
Quality of Service_Equipment Performance Alarm	An alarm of this type is associated with degradation of equipment performance. e.g. system resources overload. It is a subtype of Quality of Service Alarm.
Quality of Service_ Traffic Performance Alarm	An alarm of this type is associated with degradation of traffic performance. e.g. excessive retransmission rate. It is a subtype of Quality of Service Alarm.
Equipment Alarm	An alarm of this type is associated with an equipment fault (ITU-T Recommendation X.733).
Equipment_Traffic Equipment Alarm	An alarm of this type is associated with traffic related equipment fault, e.g. antenna, receiver, transmitter, and switch fault etc. It is a subtype of Equipment Alarm.
Equipment_ Charging System Alarm	An alarm of this type is associated with charging system fault, e.g.billing file error etc. It is a subtype of Equipment Alarm.
Equipment_External I/O Equipment Alarm	An alarm of this type is associated with an external I/O equipment failure, e.g. disk problem. It is a subtype of Equipment Alarm.
Equipment_Relay and Transmission Alarm	An alarm of this type is associated with relay and transmission failure, e.g. printer un-reachable. It is a subtype of Equipment Alarm.
Equipment_Equipment Power Alarm	An alarm of this type is associated with equipment power problem, e.g. power supply failure. It is a subtype of Equipment Alarm.
Integrity Violation	An indication that information may have been illegally modified, inserted or deleted.
Integrity Violation_ Data Configuration	An alarm of this type is associated with data configuration failure. e.g. switch data configuration error. It is a subtype of Integrity Violation.
Integrity Violation_ Database System	An alarm of this type is associated with database system failure. e.g. database out of service. It is a subtype of Integrity Violation.
Operational Violation	An indication that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service.
Physical Violation	An indication that a physical resource has been violated in a way that suggests a security attack.
Security Service or Mechanism Violation	An indication that a security attack has been detected by a security service or mechanism.
Time Domain Violation	An indication that an event has occurred at an unexpected or prohibited time.
Unknown	Event type that cannot be supported by the above definitions.

Table 5: Event Types

Rationale:

- X.733 is widely used as a standard for the specification of a generic event/alarm. The attributes, as well as the state model and the behaviour of the model are quite stable since more than 15 years now. So that this seems to be a commonly accepted definition for the FM interface, which can be adopted to create an “implementation-ready” standardized interface..

The abbreviations and conventions used here are part of the CCITT Rec. X.733 specification. See document: T-REC-X[1].733-199202-I!!PDF-E.pdf , quoted here:

Chapter 4 Abbreviations
Conf Confirm
Ind Indication
Req Request
Rsp Response
…

Chapter 5 Conventions
This Recommendation | International Standard defines services following the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values
M the parameter is mandatory
(=) the value of the parameter is equal to the value of the parameter in the column to the left
U the use of the parameter is a service-user option.
– the parameter is not present in the interaction described by the primitive concerned.
C the parameter is conditional. The condition(s) are defined by the text which describes the parameter.
P subject to the constraints imposed on the parameter by CCITT Rec. X.710 | ISO/IEC 9595.
…

Priority: Essential

REQ-FM (2) Event/Alarm Transport

It must be possible to send (Server) [and receive/listen to (Client) event/alarms]
(see also REQ-FM (9))

Description:
- EMSs (FM servers) can distribute (send) event/alarms according to X.733 event/alarm structure specification to NMS (OSS)
- [NMSs (FM clients) can receive/listen to event/alarms according to X.733 event/alarm structure specification. ("NMS send" is not required. Please consider that these requirements focus on the EMS→ NMS interface only!)]

Rationale:
- This is a basic and generic requirement for an FM interface.

(Remark: the NMS can also query for alarms, beside "Send" and "Receive". This requirement is covered under REQ-FM (5))

Priority: Essential

REQ-FM (3) Clear – Event/Alarm Transport

It must be possible to send [and receive/listen to] "clear" - event/alarm events

Description:
- The interface specification has to support "clear" events, according to the X.733 specification. Element Management Systems (servers) should be able to deliver "clear-event/alarm" events, which can be

unambiguously mapped on related event/alarm events. (See “clear correlation” requirement later on [part of requirement “Unambiguous Notification ID”]). The Network Management System (client) must be able to handle the clear-event/alarms. The interface specification has to support this capability. The EMS must support “clear” - event/alarm handling. (But the NMS must be able to handle situations, if there are missing clear-events/alarms.)

Rationale:

- Support for “clear” – event/alarms improve the ability of network operators to understand the actual status of NEs -> do they deliver the NE service, or are there still open faults in the NE which might impact the NE service and eventually other subsequent end user services. “Clear” - event/alarms reduce the costs for operational processes, because they reduce the effort to identify the status of NEs. Without “clear” - event/alarms, the operator has to perform additional tests to verify the actual NE status.

Priority: Essential

REQ-FM (4) Unambiguous ID

It must be possible to correlate between clear–event/alarm and the original event/alarm, by using an unambiguous ID.

Description:

- A unique and unambiguous ID is a prerequisite to enable the NMS to correlate between “clear” – event/alarms and original event/alarms. It is not allowed to use a combination of different attributes to create unambiguousness.
- The EMS will send a “clear” – event/alarm, as soon as the incident, which caused the original event/alarm, does not exist any more. The NMS needs to be able to correlate between the “clear” - event/alarm and the original event/alarm. So the Element Management System must be able to deliver “clear” - event/alarm events, which can be unambiguously mapped on related event/alarm events. The interface specification has to support this capability. Although this is a general requirement for Element Management Systems and out of scope for this requirement specification for the interface itself, there must be an interface specification which describes the usage of the event/alarm attributes, so that the relation between event/alarm and “clear” - event/alarm can be uniquely identified.
- Remark: the requirement is different to the correlation mechanism described in the document “ITU-T X.733 Correction”.

Rationale:

- The actual X.733 mechanisms used to correlate between “clear” - event/alarms and the original event/alarms are inefficient and complex. They lead to complex and expensive implementations of FM interfaces, especially to be able to deliver NMS support for **Event/Alarm Correlation (Clearing) and Re-Synchronization**.

Priority: Essential

REQ-FM (5) Event/Alarm Query

It must be possible for the client (NMS) to query all active event/alarms.

Description:

- The interface has to support the “Synchronization” functionality of the Network Management System. That means, the Network Management System can use a “query” functionality of the interface to get all event/alarms, which are known by the Element Management System (during the time of the “query” command) and which do not have the perceived severity = “cleared”.

Remark: this capability requires the “unambiguous Notification ID” (see related requirement “REQ-FM(4) Unambiguous Notification ID”

Rationale:

- This functionality allows the implementation of a synchronization mechanism in the Network Management – System. In case of an undefined state of the event/alarm data in the NMS (e.g. caused by a restore of the NMS database), the Network Management System can send a query to the EMS to synchronize between EMS event/alarm data and NMS event/alarm data.

Priority: Essential

REQ-FM (6) Heartbeat

The interface has to support a heartbeat capability which allows EMS to send heartbeats (configurable) and NMS to receive/listen to heartbeats.

Description:

- The interface has to support EMS heartbeat signals to the NMS. This functionality allows to indicate that the EMS and also the connection between EMS and NMS is up and running.

Rationale:

- The heartbeat functionality ensures that the NMS is able to inform the operator about a connection loss between EMS and NMS (alarming of connection-loss and clearing if connection is back).

Priority: Essential

REQ-FM (7) Supplementary Information contained within alarm

The interface has to provide all information required for correlation

Description:

- All information required for the correct analysis of the fault context must be provided. All supplementary information from the EMS or NE explaining the alarm context shall be embedded / encoded into one alarm parameter in a regular expression. This should include ID’s, topological information. The field must be structure in a regular manner, so that automatical processing by a post processing function is possible.

Rationale:

- It shall not be required to consult the Element Manager or other tools to analyse the fault context.

Priority: Essential

REQ-FM (8) Co-operative alarm acknowledgement (OPTIONAL)

The interface shall support a co-operative alarm-acknowledgement function as described in 3GPP TS 32.111-1 (Optional feature)

Description:

- Acknowledgement performed at EM layer is notified at NM layer and vice versa, thus the acknowledgement-related status of this alarm is the same across the whole management hierarchy. The alarm acknowledgement function requires that:
  a) All involved OSSs have the same information about the alarms to be managed (including the current responsibility for alarm handling).
  b) All involved OSSs have the capability to send and to receive acknowledgement messages associated to previous alarm reports.

Rationale:
- The alarm acknowledgement function assures that activities concerning the resolving of the specific problem are indicated.

Priority: Minor

5.5.3 EMS Specific Functional Requirements for Interface Support

REQ-FM (9) Reliable Event/Alarm Communication (supported by EMS)

- EMS buffers event/alarms if they cannot be sent to the NMS
- EMS sends event/alarms immediately as soon as the connectivity to the NMS is up again

Description:
- The main intention of this requirement is to ensure that no event/alarm is lost when NMS goes down (caused by NMS problems or by maintenance work). (For example: X.733 (relates to X.710 for events) requests a logging mechanism for events on the originator site. This enables the NMS to synchronize with its data sources as soon as the NMS is back again) → this is a requirement for the EMS.
  Another problem might occur, when the transport mechanism between EMS and NMS is not available. To ensure that the operator is aware about the malfunction of the interface, which will stop the ability to retrieve and to monitor event/alarms. This situation cannot be handled by the interface itself, but it can be handled either on EMS site (For example: X.733 specifies a confirmation event which has to be delivered by the NMS, as soon as the NMS receives the event/alarm) and/or by the NMS (e.g. via regular queries to the EMS [heartbeat]). → These requirements have to be supported by EMS and NMS. The interface itself has to support the confirmation of "sent – events" and it has to support "queries".

Rationale:
- Ensure that no event/alarm gets lost if the NMS or the interface to the NMS goes down.

Priority: Essential

REQ-FM (10) Configurable EMS Heartbeat Message

EMS will send heartbeats in regular (configurable) intervals to NMS.

Description:
- The EMS will send heartbeat signals to the NMS in regular intervals (configurable intervals) to indicate that the EMS and the connection between EMS and NMS are up and running.

Rationale:

- The heartbeat functionality ensures that the NMS is able to inform the operator about a connection loss between EMS and NMS (event/alarming of connection loss and clearing if connection is back).

Priority: Essential

REQ-FM (11) Alarm Suppression

The EMS - NMS - Fault Management interface should enable the alarm suppression.

Description:
- The EMS interface offers the possibility to suppress the alarm of physical and logical objects when the NMS should not receive any alarms from EMS. After alarm suppression all alarms will be cleared on the NMS and a warning will be generated on the NMS which indicates the alarm suppression. After re-enabling of the alarms all active alarms will be sent from EMS to NMS. This capability has to be configurable (manual / automatically).

Rationale:
- This functionality is very important for maintenance of equipment, hardware / software upgrade, testing etc.

Priority: Major

REQ-FM (12) Summary Alarms

EMS interface summary should provide summary alarm functionality.

Description:
- For minor alarm is sometimes not practicable to send every alarm from EMS to NMS. EMS generates a summary alarm and sends it to NMS when an alarm occurs several times within a certain window-time. This capability should be configurable. E.g. if a alarm occurs and clear more than 50 times per minute, then EMS will send a summary alarm to NMS. If this alarm occurs and clear less than 50 times per minute, then EMS will sent clear alarm to NMS.

Rationale:
- This feature protects the NMS from alarms flood.

Priority: Major

5.5.4 NMS Specific Functional Requirements for Interface Support

REQ-FM (13) Re-Synchronization

The NMS must be able to synchronize the own event/alarm list with the EMS event/alarm lists

Description:
- The NMs will use the query functionality of the FM interface to synchronize the own event/alarm list with all EMs event/alarms with a perceived severity ≠ "cleared". This functionality will be invoked automatically by re-connection of the NMs with the EMs after startup of the NMs or the interface

Rationale:

- This capability has to ensure, that the event/alarm lists of the EMs and the NMs are always synchronized.

Priority: Essential

5.6 Use Cases

Introduction

This document contains "Use Cases" to explain the meaning of the requirements REQUIREMENTS FOR FAULT MANAGEMENT INTERFACE (FM) and GENERIC NEXT GENERATION CONVERGED OPERATIONAL REQUIREMENTS (GEN). Please consider, that not all requirements are related to a specific Use Case in this document, because some of them are business requirements without a concrete technical implementation (e.g. generic requirements, like "Standardized", "Mature", "Useful", etc.)

Event/Alarm Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**It must be possible to send (EMS) and to receive/listen to Event/Alarms (NMS) via the FM Interface** [See REQ-FM (2), REQ-FM (1)and **Fehler! Verweisquelle konnte nicht gefunden werden.**.	
Actor and Roles	1. Element Management – systems (FM Servers) can distribute (send) Event/Alarms according to the alarm structure specified in REQ-FM (1). 2. Network Management– systems (FM Clients) can receive/listen to Event/Alarms according to the alarm structure as specified in REQ-FM (1).	
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected	
Begins when	EMS created an alarm	
Step n	EMS issues an alarm	
Step (n+1)	-	
Ends when	NMS receives the alarm	
Exceptions	-	
Post Conditions	- The Alarm information between EMS and NMS is consistent for this alarm. - The Alarm structure fulfils the requirements from REQ-FM (1). - The "Managed Object Instance" – Attribute for the EMS ← Alarm → NMS Interface fulfils the requirements from **Fehler! Verweisquelle konnte nicht gefunden werden.**. - Mapping of Event Attributes between Event and NMS are aligned - Inventory Source is CMDB	
Traceability	-	

Event/Alarm Update Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**It must be possible to send (EMS) and to receive/listen to an Update of the Event/Alarms (NMS) via the FM Interface** [See Requirement REQ-FM (2) and REQ-FM (1).	
Actor and Roles	1. Element Management – systems (FM Servers) can distribute (send) an Event/Alarms – Update 2. Network Management – systems (FM Clients) can receive/listen to an Event/Alarms Update	See Use Case: “2.1 Event/Alarm Transport”
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected. An EMS Alarm has been send to the NMS already.	
Begins when	EMS updated an alarm attribute	
Step n	EMS issues the updated alarm	
Step (n+1)	-	
Ends when	NMS receives the updated Alarm	
Exceptions	-	
Post Conditions	The Alarm information between EMS and NMS is consistent for this alarm, Existing Alarm will be overwritten , no additional Alarm in Alarm list	
Traceability	-	

Clear – Event/Alarm Transport

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	It must be possible to send [and receive/listen to] “Clear” Event/Alarm events [See Requirement REQ-FM (3) and REQ-FM (4)]	
Actor and Roles	Element Management systems (Servers) should be able to deliver “Clear-Event/Alarm” events, which can be unambiguously mapped on related Event/Alarm events (See “Clear Correlation” requirement later on). The Network Management system (client) must be able to handle the Clear Event/Alarms. The interface specification has to support this capability. The EMS must support Clear - Event/Alarm handling.(But the NMS must be able to handle situations, if there are missing Clear-Events/Alarms)	
Assumptions	EMS and NMS implemented and connected	
Pre conditions	EMS and NMS started and connected. An EMS Alarm has been send to the NMS already.	
Begins when	The Alarm is being cleared.	
Step n	EMS issues an Alarm-Clear notification	
Step (n+1)	-	
Ends when	NMS receives the Alarm-Clear - notification	

Exceptions	-	
Post Conditions	- The Alarm information between EMS and NMS is consistent for this alarm - The Notification ID´s of the original Alarm and the related Clear Alarm update are unambiguously correlated to each other by a combination of the numerical Notification ID and the “Managed Object” [See REQ-FM (4)and REQ-FM (3)]	
Traceability	-	

Event/Alarm Query

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**NMS queries all active Event/Alarms at EMS.** [See REQ-FM (5)]	
Actor and Roles	The interface has to support the “Synchronization” functionality of the Network Management system. That means, the Network Management system can use a “query” functionality of the interface to get all Event/Alarms, which are known by the Element Management system (during the time of the “query” – command) and which do not have the perceived-severity: “cleared” (Comment: This functionality allows the implementation of a synchronization mechanism in the Network Management – system. In case of an undefined state of the Event/Alarm – data in the Network Management system (e.g. caused by a restore of the NMS database), the Network Management system can send a query to the EMS to synchronize between EMS Event/Alarm – data and NMS Event/Alarm – data.)	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	- EMS and NMS are started and connected. - There are active (not cleared) alarms in the Alarm-List of the EMS and the NMS. Both lists are synchronized - EMS and NMS are disconnected - The Alarm-List of the NMS is deleted?? Alarms which are not in NMS will be created, don’t change Alarm status of existing Alarms like Ack ,Operator Note ...	
Begins when	EMS and NMS are connected again	
Step n	The NMS queries for all active Alarms (automatically or manually)	
Step (n+1)	The EMS sends all active Alarms	
Ends when	NMS receives all Alarm events	
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability	-	

Heartbeat

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**EMS sends heartbeat events (configurable) to NMS.** [See REQ-FM (6)]	
Actor and Roles	EMS sends heartbeat signals in regular (configurable) time intervals to the NMS. This functionality allows to indicate, that the EMS and the connection between EMS and NMS and is up and running.	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	EMS and NMS are started and connected. Heartbeat – Interval is configured in EMS and NMS	
Begins when	Time for first Heartbeat-Interval in EMS is arrived	
Step n	EMS issues Heartbeat-Event to NMS in regular Intervals	
Step (n+1)	NMS receives the Heartbeat-Event in regular Intervals	
Step (n+2)	Cut of Network Connectivity between EMS and NMS, or EMS shutdown	
Step (n+3)	NMS detects, that it does not received the Heartbeat – Event in the expected Heartbeat-Interval. NMS will show a “lost-connection” notification (e.g. Alarm), that the connectivity to the EMS does not work any more.	
Step (n+4)	Connect EMS with NMS again	
Step (n+5)	EMS sends all outstanding (buffered) Alarms to the NMS	See also Use Case “Reliable Alarm/Event Communication”
Step (n+6)	EMS sends Heartbeat Event again	
Step (n+7)	NMS clears the “lost-connection” notification.	
Ends when	NMS receives all outstanding Alarms	See also Use Case “Reliable Alarm/Event Communication”
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability	-	

Reliable Event/Alarm Communication (supported by EMS)

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**No lost Alarm/Event, after connection breakdown between EMS and NMS.** [See REQ-FM (9)]	
Actor and Roles	- EMS buffers Event/Alarms if they cannot be send to the NMS - EMS sends Event/Alarms immediately as soon as the connectivity to the NMS is up again It has to be ensured that no Event/Alarm is lost, when NMS goes down	

	(caused by NMS problems or by maintenance work). X.733 (relates to X.710 for Events) requests a logging mechanism for Events on the originator site. This enables the NMS to synchronize with its data sources as soon as the NMS is back again. → this is a requirement for the EMS Another problem might occur, when the transport mechanism between EMS and NMS is not available. To ensure, that the operator is aware about the malfunction of the interface, which will stop the ability to retrieve and to monitor Event/Alarms. This situation cannot be handled by the interface itself, but it can be handled either on EMS site (X.733 specifies a confirmation event which has to be delivered by the NMS, as soon as the NMS receives the Event/Alarm.) and/or by the Network Management system (e.g. via regular queries to the EMS [heartbeat]). → These requirements have to be supported by EMS and NMS. The Interface itself has to support the confirmation of "send – events" and it has to support "queries".	
Assumptions	EMS and NMS are implemented and connected	
Pre conditions	EMS and NMS are started and connected.	
Begins when	Disconnection of the physical connectivity between EMS and NMS	
Step n	EMS creates several new Alarms	
Step (n+1)	Connect EMS with NMS again	
Step (n+2)	EMS sends all outstanding (buffered) Alarms to the NMS	
Ends when	NMS receives all outstanding Alarms	
Exceptions		
Post Conditions	The list of Alarms between EMS and NMS is consistent Connection Lost is alarmed in Alarm list	
Traceability	-	

De-Coupled, Flexible/Extendible and Compatible

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Implementation of a new Version of an Interface on EMS OR NMS** [See **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**]	
Actor and Roles	One of the communication partners implements a new version of the interface, e.g. with additional attributes, while the other communication partners still use an old version of the interface specification. This "mixed versions" of interface implementations can be used without any impact on the communication partners or the interface implementations of the communication partners, so that changes in the application or in the interface implementation at one of the communication partners do not lead to the need for changes in the application or in the interface implementation of the other communication partners. It must be possible to extend the interface capabilities (methods and attributes), without breaking the standard	

Assumptions	EMS and NMS are implemented and connected	
Pre conditions	- EMS and NMS are started and connected. The interface works as expected and the EMS sends Alarms to NMS successfully.	See UseCase “Event/Alarm Transport”
Begins when	A new EMS Interface-Version is ready to implement. The new Interface Version uses one additional optional attribute (for example)	
Step n	Disconnect EMS from NMS.	
Step (n+1)	Activate new EMS Interface Version	
Step (n+2)	Connect EMS to NMS	
Step (n+3)	NMS performs a synchronization (started by a “query for active alarms”) with the EMS	
Step (n+4)	The NMS receives Alarms from the EMS (just don’t use/show the additional attribute).	
Ends when	NMS received all outstanding Alarms without any impact on NMS	
Exceptions	-	
Post Conditions	The list of Alarms between EMS and NMS is consistent	
Traceability		

Certifiable

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Certify the standard compliancy of the interface implementation** Remark: There is no description of the concrete steps for the certification in this Use Case description, because there is no description of the certification mechanism available today. [See REQ-GEN (12)]	
Actor and Roles	The interface implementation on EMS and NMS will be certified (e.g. via tool). This will allow the verification, that the interface implementation is compliant with the standardized interface specification to avoid compatibility problems between interface implementations of different communication partners.	
Assumptions	The FM Interface is implemented on EMS and NMS.	
Pre conditions	-?	
Begins when	-?	
Step n	-?	
Step (n+1)	-?	
Ends when	-?	
Exceptions	- ?	
Post Conditions	The Certification of the FM Interface on EMS and NMS has been passed successfully	
Traceability	-	

Interface Robustness

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Outage of the connection to one of the EMS does not harm the interfaces from other EMS to the NMS.** [See REQ-GEN (18)]	
Actor and Roles	An outage of one or more EMSs (source) may not lead to any impact on the connectivity between NMS and other EMSs	
Assumptions	Several EMS are connected to one NMS	
Pre conditions	All connections between the EMS and the EMS´s are up and running	
Begins when	Disconnect EMS 1	
Step n	The NMS receives Alarms from the other (still connected) EMS´s without any impact caused by the connection breakdown to EMS 1	
Step (n+1)	Connect EMS 1 again	See also 2.10 : "Reliable Event/Alarm Communication (supported by EMS) "
Ends when	NMS receives Alarms from all EMS´s	
Exceptions	-	
Post Conditions	The list of Alarms between all EMS´s and NMS is consistent	
Traceability	-	

Simple Trace and Logging

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Error analysis of the FM Interface by check of the Log on EMS and NMS in case of interface problems** [See REQ-GEN (19)]	
Actor and Roles	The Operator/Administrator of the NMS and the EMS check the logs on "their" systems in case of problems with interface. Examples: - Connection breakdown between EMS and NMS - EMS does not react on "Query"- Command - The EMS does not deliver a mandatory attribute The level of logging details will be configured on EMS and NMS: - Masking of attributes - Masking of attribute- content	
Assumptions	EMS and NMS are implemented and connected. The logging mechanism is working on EMS and NMS.	
Pre conditions	The logs do exist in a human readable format. EMS and NMS are up and running.	
Begins when 1.0	Breakdown of the connection between EMS and NMS	
Step 1.1	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand the problem and to restore	

	the connectivity)	
Step 1.2	Restore the connectivity	
Ends when 1.3	The connectivity is up and running. The log on EMS and NMS shows, that the problem has been resolved.	
Begins when 2.0	Stop EMS database.	
Step 2.1	Start NMS query: "Query all active alarms" manually.	See Use Case "Event/Alarm Query"
Step 2.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand and to solve the problem)	
Step 2.3	Restart EMS database	
Step 2.4	Start NMS query: "Query all active alarms" manually.	See Use Case "Event/Alarm Query"
Ends when 2.5	The NMS Query is successfully. The NMS receives all active alarms from the EMS. The log on EMS and NMS shows, that the problem has been resolved.	
Begins when 3.0	EMS creates a new alarm. The content of the Managed Object attribute is deleted manually.	
Step 3.1	The EMS sends the alarm to the NMS. (The NMS will not be able to handle the alarm correctly in this case)	
Step 3.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the information needed to understand and to solve the problem)	
Step 3.3	The EMS sends further alarms to NMS (this time correctly, with the MO – attribute, as expected)	
Step 3.4	The NMS receives the alarms and can handle it correctly.	
Ends when 3.5	The log on EMS and NMS shows, that the problem has been resolved.	
Begins when 4.0	The Operator/Administrator on EMS and NMS mask attributes in the log.	
Step 4.1	The EMS sends alarms to the NMS.	
Step 4.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all the needed information without the masked attributes)	
Step 4.3	The Operator/Administrator on EMS and NMS de-mask attributes in the log.	
Ends when 4.4	Check Log on EMS and NMS manually. (Verify, that the Log contains all the needed information including the de-masked attributes)	
Begins when 5.0	The Operator/Administrator on EMS and NMS mask attributes-content in the log (e.g. masking of Severity = "Warning")	
Step 4.1	The EMS sends alarms to the NMS. Some of them (not all) must contain Alarm with Severity="Warning"	
Step 4.2	Check Log on EMS and NMS manually. (Verify, that the Log contains all transactions, without "send/receive Alarm" with Severity="Warning")	
Step 4.3	The Operator/Administrator on EMS and NMS de-mask all attributes-content in the log	
Ends when 4.4	Check Log on EMS and NMS manually. (Verify, that the Log contains all transactions, including Alarms with Severity="Warning")	
Exceptions	-	
Post Conditions	The log on EMS and NMS shows, that the problems have been resolved.	
Traceability	-	

M : N Connectivity

Use Case Stage	Evolution / Specification	<<Uses>> Related use
Goal	**Connect several [min. 3] EMS to several [min. 2] NMS.** [See **Fehler! Verweisquelle konnte nicht gefunden werden.**]	
Actor and Roles	Implementation of an N:M scenario	
Assumptions	Several EMS are connected to several NMS	
Pre conditions	All connections between the EMS and the NMS´s are up and running	
Begins when	All EMS´s send alarms to all NMS´s	See Use Case: “2.1 Event/Alarm Transport”
Step n	-	
Ends when	All NMS´s receive all Alarms from all EMS´s	
Exceptions	-	
Post Conditions	The list of Alarms between all EMS´s and all NMS´s are consistent	
Traceability	-	

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

STREAM "CONFIGURATION MANAGEMENT"

by NGMN Alliance

Final Draft

Version: 1.2

Date: 2013-08-13

Publication	**NGMN Confidential with Limited Dissemination**
Project	**NGCOR (Next Generation converged Operations Requirements) Phase 2 Configuration Management Requirements**
Editor in Charge	**Manfred Mackert**
Editing Team	**Frank Lehser, Manfred Mackert, Mario Schulz (Deutsche Telekom)**
Document Status	**Approved for Publication**
Approved by	**NGMN Board / 7th November 2013**

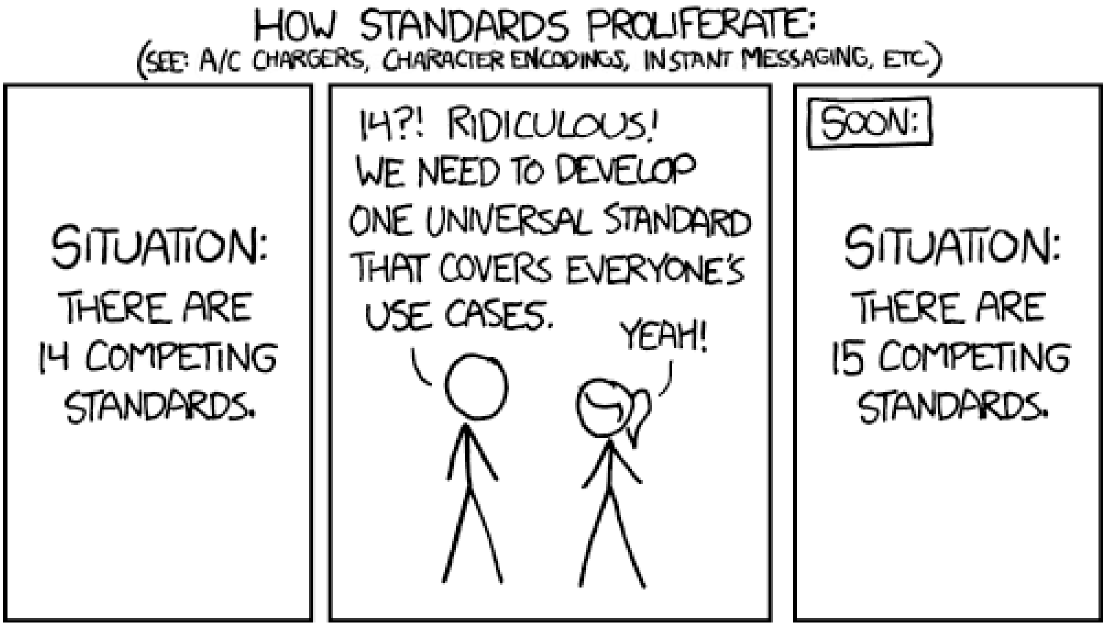
Abstract:
Requirement Specification for Configuration Management in the context of NGCOR

Document History

Date	**Version**	**Author**	**Changes**
30/05/2012	V 0.1	Manfred Mackert	Initial Draft
15/08/2012	V 0.2	Manfred Mackert	extended Draft I
23/11/2012	V 0.3	Manfred Mackert	extended Draft II
01/14/2013	V 0.4	Manfred Mackert	extended Draft III
18/01/2013	V0.5	Manfred Mackert	Editorial Review (Yvonne Doernhofer)
31/01/2013	V0.6	Manfred Mackert	Included Results from Beijing Partner Review
20/03/2013	V0.7	Manfred Mackert	Included Review Results from NGCOR CM Conf Calls (22.2. & 14.3.2013)
8/04/2013	V0.8	Manfred Mackert	Included Review Results from NGCOR CM Conf Call (25.3.2013)
25/04/2013	V0.9	Manfred Mackert	Included: Review Results from NGCOR CM Conf Call (15.4.2013) Feedback Mats Eriksson on Base Template Feedback Edwin Tse on Template Syncronisation
25/05/2013	V0.91	Manfred Mackert	Editorial Review (Yvonne Doernhofer)
15/06/2013	V1.0	Manfred Mackert	Inserted 5.5.2 CM use cases Inserted details on MTOSI and Netconf Added chapter 6.1 Survey template approach
01/07/2013	V1.1	Manfred Mackert	Added details in 6.2 (former 6.1)
13/08/2013	V1.2	Thomas Kulik	numeration of chapters, figures and tables changed; minor corrections

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6 REQUIREMENTS FOR CONFIGURATION MANAGEMENT (CM)



ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.1 SUBTASK GENERAL OVERVIEW

Networks and Services are becoming increasingly complex to manage, resulting in a lot of OPEX consumption, as well as huge CAPEX requirements due to the ever increasing need to purchase and deploy different types of management software/ solutions required to cope with the growing complexity.

The deployment of key emerging network technologies such as IP Transport, Long Term Evolution (LTE)/ Evolved Packet Core (EPC) will increase the amount of equipment in the underlying network architectures for Fixed & Mobile Access - Backhaul. These are all key drivers, demanding the need

- to evolve the underlying network architecture,
- to automate the deployment and change processes from an NMS/OSS perspective.
- to harmonize and standardise the information models,
- to harmonize and standardise the EMS northbound management interfaces

to enable the reduction of the OSS integration tax and the the overall Operating costs of the Deployment/ Configuration and Operations process (OPEX).

Network Operators are thus calling for Unified Service and Network Management solutions and evolution of OSSs. For this reason, and from network deployment and operation perspective, Operators' networks and associated OSS (Management System) must become intelligent, agile, open, secure, flexible and autonomous (i.e. operating with minimum human intervention).

In this context, Operators need the Automation of Network and Service Management processes as well as Self-configuring, Self-diagnosing, Self-healing and Self-optimising network elements/ network. This requires Autonomics and Self-Management solutions that reduce human involvement in Service and Network Management.

This document will develop requirements in these areas from a configuration management perspective in a converged operations scenario. Focus will be on RAN deployment guided by the economy of scale.

This approach heralds the introduction of a "autonomics" paradigm. Indeed, some basic autonomics features should be embedded into the network equipment and the OSS initially for Deployment and Configuration purposes.

For large scale deployment, the Future Network infrastructure should incorporate more and more autonomic features like Self-configuration in order to maintain operational cost control. Autonomic capabilities are introduced in the management architecture thanks to Autonomic Functions (AF) at different layers. The implementation of these AFs in the autonomic network architecture is driven by operator's policy.

We can identify 3 autonomic network architecture schemas (as specified by 3GPP/ SA5 for SON related OA&M 3GPP - TS 32.500 V11.1.0 (2011-12)):

- Distributed: the AFs are embedded in the NE only.
- EM-focused: the AFs are embedded in EMs and NEs.
- NMS-focused: the AFs are embedded in the operators' OSS, the EMS and the NEs.

The same controls should also be applicable during the operational life span of the network. This requires embedding Self-optimisation & Self-Healing features. In the "optimisation & operation" phase, this autonomics paradigm rises the issue of pertaining to "trust & confidence" on these Self-functions, as well as the coordination of interactions of various Autonomic functions running simultaneously to mitigate or prevent unstable behaviour of the network. This issue is tackled by research community (European project such as SOCRATES, SEMAFORE, UNIVERSELF) and the outcome is expected by standardisation community such as ETSI AFI and 3GPP. This issue needs to be solved before undertaking large commercial deployments in the coming years.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

However, the main focus of 3GPP (SA2, SA5) is on the SON functions and related management aspects of RAN features (eNodeBs in LTE for instance) but not on the wire line connections between eNodeBs and the EPC NEs (S1-MME, S1-U, X2-U, X2-C) on IP level aspects.

This combination of SON features designed for the RANs and Autonomics features that could be embedded into Transport part of the Backhaul will shape a broader picture of "Autonomicity and Self-Management" of the Backhaul.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.2 INTRODUCTION TO NGCOR CONFIGURATION MANAGEMENT

Three general life-cycle phases can be described which represent different degrees of stability of a network. Once the first stage is over, the system will cycle between the second and the third phases. This is known as the network life-cycle and includes:

1) The network is installed, configured and put into commercial service;
2) The network reaches certain stability and is only modified (dynamically) to satisfy short-term requirements by (dynamic) re-configuration of resources or parameter modification; this stable state of a network cannot be regarded as the final one - each equipment or SW modification will let the network progress to an unstable state and require optimisation actions again;
3) The network is being adjusted to meet the long-term requirements of the network operator and the customer, e.g. with regard to performance, capacity and customer satisfaction through the enhancement of the network or equipment up-grade.

During all these phases, the operators will require adequate management processes, information models and functions to perform the necessary tasks.

Configuration Management (CM), **as a process** with a dedicated set of actions/ activities and the functions to support their automation, provides the operator with the ability to assure correct and effective operation of a network as it evolves. CM actions/activities have the objective to control and monitor the actual configuration on the Network Elements (NEs) and Network Resources (NRs), and they may be initiated by the operator or by autonomic functions in the Operations Systems (OSS) or in the NEs.

Configuration Management actions/ activities may be requested

- as part of an implementation/ rollout program (e.g. additions, swaps or deletions),
- as part of an optimization program (e.g. modifications),
- to document the current network situation, and
- to maintain the overall Quality of Service (QoS).

The Configuration Management actions/activities are initiated either as single actions on single NEs of the network, or as part of a complex procedure involving actions on many resources/ objects in one or several NEs in one domain (bulk actions).

In today's market, service providers aim to ever decrease the time-to-market of new and enhanced services in a cost-conscious manner. As a consequence, the need arises for existing OSS/BSS infrastructure applications to adapt in an ever increasing pace. This affects OSS applications themselves and also increasingly their integration.

Furthermore, there is a growing demand for automation of business processes at service providers, especially in the area of network/ service operations to improve operational efficiency. This leads to the need for improved integration of OSS as a common demand from service providers. [An integration strategy using ESB concepts, commonly adopted interface standards and NGOSS concepts might have the potential to deliver the needed technical basis for real life, standardized NMS-EMS integrations.]

A **Configuration Management System** (CMS) here is understood as the set of all relevant IT systems to provide and exchange information required by the Planning, Deployment and Operations Processes to set up and monitor a network.

Its kernel consists of capabilities for Activation & Discovery and their integration points with a Planning Database, a Reconciliation Engine, a Resource Inventory, a Configuration Inventory and the Element Management Systems.

Configuration Management interfaces between Element Management Systems (EMS) and Network Management Systems (NMS) as available on the market today are based on a huge variety of different technologies, proprietary information models and sometimes standards. Each EMS implemented in a Service Provider's (SP) environment uses its own specific interface type and implements element-specific extensions and behaviour, which evolves over time, leading to a continuous need for upgrades on EMS side and to related adaptations and upgrades on NMS side.

SPs estimate a need of one major upgrade project per EMS per two to three years. The cost and effort for the EMS upgrades are often covered by the budgets for the related network element upgrades. But there are additional costs and effort for the related upgrade of adapters/ access-modules in the NMS, although the main requirements on such an interface are almost the same for the last ~ 15 years.

SPs are driven by vendors to start interface upgrade projects, perform complex and time consuming type acceptance to ensure the needed quality, train administrators and project managers, etc. but don't get a real additional value.

The authors of the CM section strongly believe, that there is potentially huge business benefit in using a common officially standardized technical approach, enabling the re-use of the same interface for different EMSs, enabling the planned exchange/ upgrade of the NMS and enabling us to stop vendor driven upgrades of interfaces which deliver no or small additional value.

Most of the existing integrations between Element Management systems and Network Management systems today are based on proprietary point-to-point interfaces although vendors offer "standard" interfaces based on SNMP, CORBA and SOAP, which are adapted to their applications. In a real integration scenario these interfaces need a lot of customization to fulfil the business requirements and to allow the communication between different proprietary OSSs because each of these applications follows its own business process, internal logic and semantic.

Obviously there is a need for a standardized interface, which delivers the semantic connectivity in the sense of a harmonized information model and a harmonized operation model and not only the underlying transport mechanisms, which helps to provide out-of-the-box interoperability and more flexible integration.

The huge expenses for OSS integration in a non-harmonized or a non-standardized environment forces operators to start a transformation process for an EMS-NMS Interface requirements definition. The way forward has to be based on Network Operator requirements – these will be developed in this document.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.2.1 Scope & Objectives

Following **objectives** have been identified:

- o Analysis and documentation of the typical deployment process for a SON enabled RAN.
- o Definition of configuration management use cases and related detailed requirements.
- o Elaboration of OSS requirements for highly efficient and flexible & adaptable Configuration Management.
- o Specification of OSS requirements for the northbound Configuration Management Interface and the related information services on the EM layer as Input for standardization bodies and vendors to deliver a standardized/ operational CM interface specification in line with the operational needs of SPs to improve the efficiency (time and costs) of CM interface implementations.

The main **scope** of the subtask Configuration Management is the specification of use cases and the elaboration of the related business requirements with a focus on:

- Working out OSS requirements for highly efficient and flexible & adaptable Configuration Management with:
  - o A Parameter set classification for the Radio part during the elements lifecycle
  - o A focus on the configuration of the essential parameters so that a minimum number of parameter must be set by the operator and all other parameters are managed by the system transparently.
- Scenario description of requirements EMS to NMS northbound Configuration Management Interface & Information services on the EMS northbound CM interface for Radio, Transport (mobile backhaul), etc.
- OSS architecture reference model definition especially concerning relations between Configuration Management and a Configuration Inventory.

However – in this first step – the focus will be on RAN configuration management as here the majority of benefits can be gained.

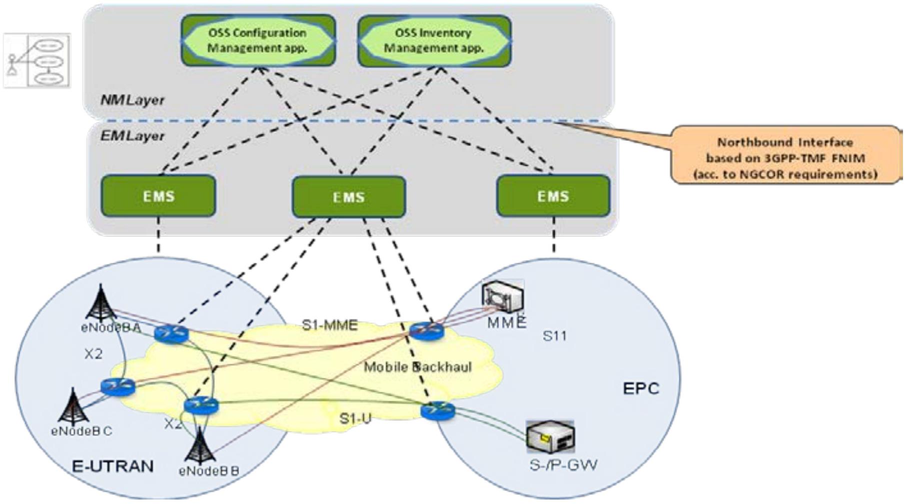


Figure 6.2-1: Operator's OSS with harmonized NBI - end-to-end network multi-domain view

In addition to this, there are specific requirements for the Element Management Systems and the Network Management Systems to use the capabilities of the specification in order to support the business requirements.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Different application topologies have to be supported by the interface:

- Several NMSs can be connected to one EMs, e.g. operational NMS (RAN sharing) and test NMS.
- An NMS can serve as an EMS (e.g. a technology domain specific NMS, which acts like an EMS to upper level NMS).

6.2.2 Benefit and Drivers

One of the most significant changes in software development and procurement practice over the past decade is the greatly increased emphasis being placed on building O&M systems mainly from COTS software in order to keep overall development and maintenance costs as low as possible. Source of COTS software are the equipment vendors and OSS vendors who can supply off-the-shelf or COTS components that can be plugged into a larger software system to provide capabilities that would otherwise have to be custom built.

The rationale for building an operators OSS solution based on harmonized and standardized interfaces and COTS OSS components is that they will involve less development time by taking advantage of existing, market proven, vendor supported products, thereby reducing overall system development costs and time to market for new services.

The main benefit is achieved, as soon as the standard specification can be re-used to implement similar interfaces for different integration scenarios, to connect different EMS to NMS applications without creating a complete new implementation of the interface.

Savings are rapidly growing in a multi domain and multi vendor environment with a significantly reduced number of integration points.

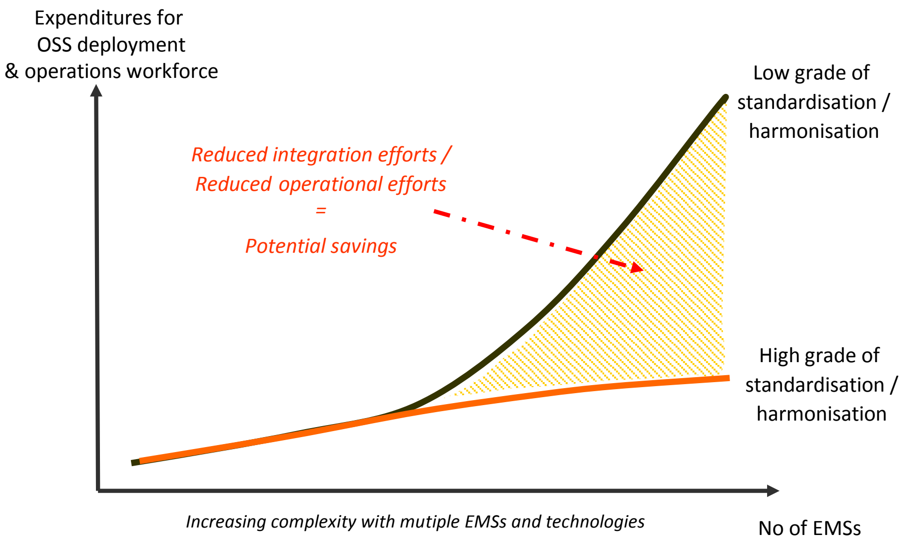


Figure 6.2-2: Savings through Interface standardization and Information Model harmonization

The effort reduction regarding optimized operations processes is estimated to be another 30% with the benefits originating from a Converged Configuration-Management process:

- Shortened time to deploy and thus time to market for new products.

- Reduced OPEX and improved service quality through improved configuration parameter transfer and deployment.
- Reduced Governance efforts for consistency checks of network configuration
- Reduce time & efforts for network diagnosis, extension and swap.
- Avoided and shortened network outage time in case of misaligned configuration.

Saving potential:

- The support of template management - pre-defined parameter sets - via the north bound interface will reduce the operations effort for planning, optimisation and change during the implementation and the life cycle of network technologies and related EMS. It has the capability to avoid or massively reduce the need for vendor specific parameter handling on the NMS layer. Resulting is a less complex information model to be implemented in CM tools with impact on development and maintenance cost.
- The support for a better level of standardization of the north bound interface will reduce the integration effort between EMS and NMS (OSS) during the implementation and the life cycle of network technologies and related EMS.

Possible issues for guidance:

- Plug & Play integration of EMS into the OSS domain (no additional cost and effort during the implementation and the life cycle of network technologies and related EM).
- De-coupling of EMS – OSS Domains (changes on EMS or on NE may not lead to changes on OSS Domain).
- Re-use of OSS clients of the interfaces.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.3 EXISTING STANDARDS FOR CONVERGED CONFIGURATION

6.3.1 3gpp Configuration Management; Concept and high-level requirements (Rel. 10)

3GPP TS 32.600 V10.0.0 states:

The Itf-N (see ref. 3GPP TS 32.102 [4]) is an object oriented interface, i.e. all resources of the PLMN network (functional and physical resources) whose management is standardized by the present document are represented as Managed Object Instances (MOI) of a Network Resource Model (NRM).

The NRM shall be highly simplified for the purpose of the NMs, based on the assumption that all of the detailed CM actions, including fault correction after one or more alarms, are performed by an Element Manager (EM), which knows the vendor-specific NRM and configuration.

The NRM identifies the basic Network Resources (NRs) to the level of detail required by FM and PM at the Network Management (NM) level. In addition to NR identification, the NRM also supports the alarm surveillance part of FM by defining which alarms can be notified by which Information Object Classes (IOCs).

The definition of the Network Resource Model (NRM) for the Itf-N (connecting the NM with a "subordinate entity", which may be an EMS or a NE) is described in 3GPP TS 32.622 [11] and other NRM IRPs listed in the Introduction clause, which define the Generic Network Resource Model and other specific NRMs applicable to PLMN management, such as the UTRAN, EUTRAN and EPC NRM.

This sub clause describes the specific functional requirements related to CM of Network Resources (NRs) on the Itf-N.

There are **two types** of CM functions:

a) ***Passive* CM** (configuration overview), which mainly provides to the NM current information about the current configuration changes by means of notifications, and allows a retrieval and synchronisation of configuration related data on NM request.

   The forwarding of these notifications over the Itf-N is controlled by means of configuring adequate filtering mechanisms within the subordinate entities. The Itf-N also provides the means for storage ("logging") and later retrieval of desired information within the subordinate entities.

b) ***Active* CM**, which offers to the NM operator a real capability to change the current network configuration.

   There are also at least **two approaches** to CM: **Basic CM** and **Bulk CM**.

   1. **Basic CM** is characterised by

      a) The use of singular operations to retrieve (configuration parameters) over *Itf-N* from single NEs, or a collection of NEs. (The passive aspect of Basic CM).

      b) The use of singular operations to activate configuration parameters in EM/NEs over Itf-N. (The active aspect of Basic CM).

   2. **Bulk CM** is characterised by

      a) Bulk (file-oriented) data retrieval (configuration parameters) over Itf-N from single NEs, a collection of NEs or the whole network. (The passive aspect of Bulk CM).

b) Bulk (file-oriented) data download of configuration parameters to EM/ NEs over Itf-N. (An active aspect of Bulk CM).

c) The network-wide activation of those parameters through a single operation. (An active aspect of Bulk CM).

d) The ability to fallback to a previous stable configuration through a single operation. (An active aspect of Bulk CM).

The gap between 3GPP NBI and commercially offered NBI - Missing Topics:

- In 3GPP no HW view is specified (what is a conscious agreement to avoid vendor specific parts) but in real NBI implementations HW view is needed: e.g. existence of HW units is represented by parameters and must be given correctly for proper work of the unit).
- Transport configuration is not touched!

The gap between 3GPP NBI and commercially offered NBI - General observations:

- In 3GPP only a subset of possible parameters is specified: in real NBI implementations number of parameter are seen between 3000 and 7000 parameters!
- 3GPP defines already a system to structure parameters: nevertheless structures are often detail vendor specific and need consideration.
- 3GPP NBI definition cannot grow as fast as real implementation: every new function follows in new parameters mostly not covered by 3GPP model.
- Implementation of NBI follows the needs of quick availability of new features: this is in conflict with a proper version management and logical and minimized parameter structure.
- The config file of an eNodeB reflects directly the SW code to realize certain functionality. The config file can be influenced (not necessarily fully) by NBI.
- Features: Programmer tends to give maybe significant parameters in the config file. The parameter accessible in the config file is the maximum set of parameter accessible in CM or in NBI. This fact leads to the situation that there are many parameters understandable only for experts and being accessed only very seldom. Most of parameters are just default values hardly ever changed.
- To be differentiated between: handling of parameters (read, store, verify) and content (these parameter which can be handled). The today's problem is the content!

6.3.2 3gpp Self-configuration of network elements; Concepts and requirements

The 3GPP concept for Self-configuration of network elements [6] describes Self Configuration as: The process which brings a network element into service requiring minimal human operator intervention or none at all.

Mainly covers SW and radio configuration. All other points unspecified. Especially for self-configuration of new eNodeBs:
- The way to make any information available to eNB is outside the scope of standardization.
- Conflict resolution in case of contradicting information made aware to the eNodeB is outside the scope of standardization.

6.3.3 SDN and its (not yet existing) northbound APIs

Software-Defined Networking (SDN) is currently transforming networking architecture in wireline networks.
SDN is an emerging network architecture where network control is decoupled from data forwarding and is directly programmable. This migration of control, formerly tightly bound in individual network devices, into accessible

computing devices enables the underlying infrastructure to be abstracted for applications and network services, which can treat the network as a logical or virtual entity.

In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications. As a result, enterprises and carriers gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs.

The upcoming Open flow specifications cover the aspect south bound interface (SBI) – the communication and data exchange from the SDN controller layer to the NE. From a telecommunication management architecture view a SDN controller has the role of an Element Manager. The SDN Controller northbound APIs play the role of Itf-N/ NBI as discussed by 3gpp/ TMF.

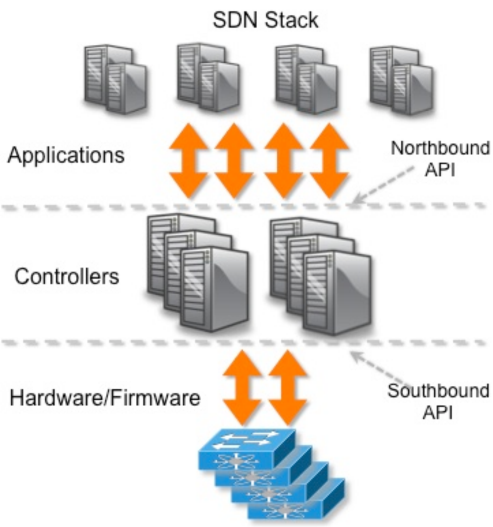


Figure 6.3-1: Software-Defined Network Architecture

[source: Brent Salisbury's Blog on http://networkstatic.net/the-northbound-api-2/]

"SDN has the potential to revolutionize the way networks operate." [Lauri Oksanen, Head of Research, Nokia Siemens Networks]

The Open Networking Foundation in their actual white paper [Software-Defined Networking: The New Norm for Networks, ONF White Paper - April 13, 2012]:

"In addition to abstracting the network, SDN architectures support a set of APIs that make it possible to implement common network services, including routing, multicast, security, access control, bandwidth management, traffic engineering, quality of service, processor and storage optimization, energy usage, and all forms of policy management, custom tailored to meet business objectives.

For example, the SDN architecture makes it easy to define and enforce consistent policies across both wired and wireless connections on a campus. Likewise, SDN makes it possible to manage the entire network through intelligent orchestration and provisioning systems. The Open Networking Foundation is studying open APIs to promote multi-vendor management, which opens the door for on-demand resource allocation, self-service provisioning, truly virtualized networking, and secure cloud services.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Thus, with open APIs between the SDN control and applications layers, business applications can operate on an abstraction of the network, leveraging network services and capabilities without being tied to the details of their implementation. SDN makes the network not so much "application-aware" as "application-customized" and applications not so much "network-aware" as "network-capability-aware". As a result, computing, storage, and network resources can be optimized. "

But the current situation is that SDN Controller northbound APIs are not standardized at all – no interest to do so & possibly political conflicts ONF/ IETF at all.

A very interesting source [14] states:

Current favorite SDN topic: creating and standardizing the Northbound API (NBAPI).

We've seen posts and musings around this from multiple folks (Brent Salisbury, David Lenrow to name just a few) and I've had many more conversations with others in the SDN community. I believe that a compelling Northbound API will not likely emerge from a standards body, or any kind of committee and the best bet for a compelling Northbound API is through competition in the open market.

Where are we at today?

If we look at where we are from an SDN Northbound API standpoint, we do have early implementations today. Take for example, Floodlight's RESTful northbound interface to handle queries and state reporting, and for static rule programming. Unfortunately and perhaps unsurprisingly, dynamic or reactive rules require direct programming within the Java framework. Trema has one to handle resource management in sliceable networks centered around tenant management. And I have no visibility into Nicira's NVP APIs presumably built on ONIX. And finally we have NOX's limited API. Most of these are relatively nascent and there are limited publicly available applications built on top of these NBAPIs.

This standardization is vital for a successful converged operations approach as NGCOR is promoting it.

6.3.4 eTOM Process 1.1.3.1 - RM&O Support & Readiness

RM&O Support & Readiness processes are responsible for managing resource infrastructure to ensure that appropriate application, computing and network resources are available and ready to support the Fulfilment, Assurance and Billing processes in instantiating and managing resource instances, and for monitoring and reporting on the capabilities and costs of the individual FAB processes.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

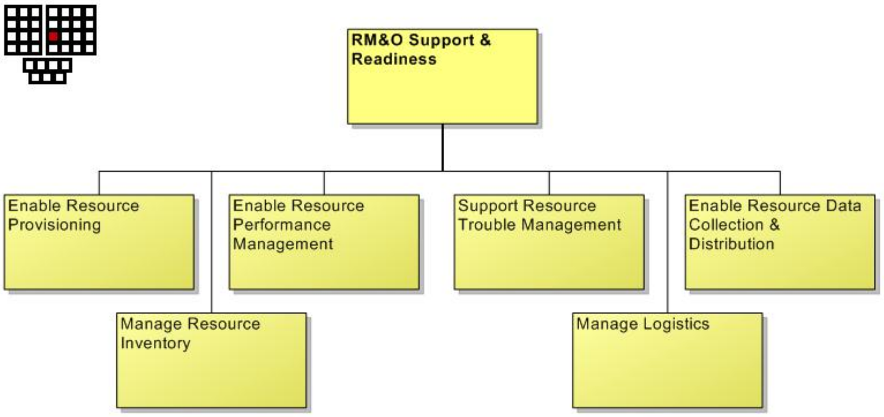


Figure 6.3-2: Process RM&O Support & Readiness

Responsibilities of these processes include but are not limited to:

- Supporting the operational introduction of new and/ or modified resource infrastructure and conducting operations readiness testing and acceptance;
- Managing planned outages;
- Managing and ensuring the ongoing quality of the Resource Inventory;
- Analyzing availability and performance over time on resources or groups of resources, including trend analysis and forecasting;
- Demand balancing in order to maintain resource capacity and performance;
- Performing pro-active maintenance and repair activities;
- Establishing and managing the workforce to support the eTOM processes; and
- Managing spares, repairs, warehousing, transport and distribution of resources and consumable goods.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.3.5 eTOM Process 1.1.3.2 - Resource Provisioning

Resource Provisioning processes encompass allocation, installation, configuration, activation and testing of specific resources to meet the service requirements, or in response to requests from other processes to alleviate specific resource capacity shortfalls, availability concerns or failure conditions.

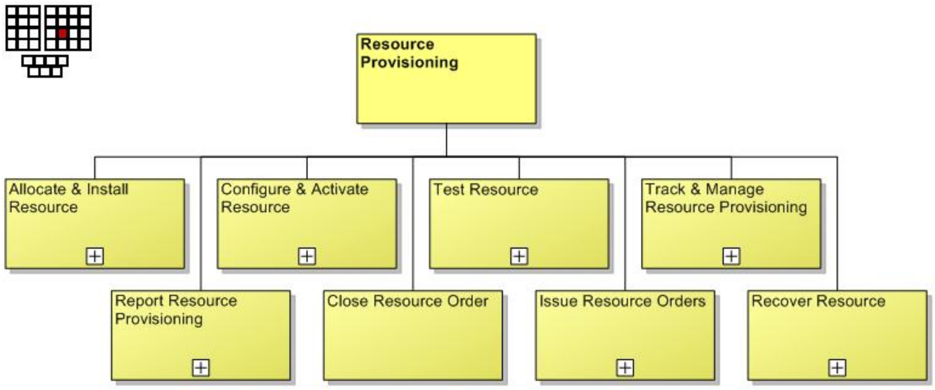


Figure 6.3-3: Process Resource Provisioning

Responsibilities of the Resource Provisioning processes include, but are not limited to:

- Verifying whether appropriate specific resources are available as part of pre-order feasibility checks;
- Allocating the appropriate specific resources to support service orders or requests from other processes;
- Reserving specific resources (if required by the business rules) for a given period of time until the service order is confirmed;
- Possibly initiating delivery of specific resources to the central office, to site or to the customer premise;
- Installation and commissioning of specific resources after delivery;
- Configuring and activating physical and/ or logical specific resources, as appropriate;
- Testing the specific resources to ensure the resource is working correctly;
- Recovery of resources;
- Updating of the Resource Inventory Database to reflect that the specific resource has been allocated to specific services, modified or recovered;
- Assigning and tracking resource provisioning activities;
- Managing resource provisioning jeopardy conditions; and
- Reporting progress on resource orders to other processes.

6.3.6 MTOSI

The goal of TeleManagement Forum's (TMF) Multi-Technology Operations Systems (MTOSI) - see [16] - is to provide open and standardized interfaces between OSSs (e.g., Service Activation systems, Inventory systems, Network Management Systems, Element Management Systems, etc.).

Multi-Technology Operations Systems Interface (MTOSI) is an XML-based OSS-to-OSS interface suite. The Network Management System to Element Management System communications is a special case and is defined by the Multi-Technology Network Management (MTNM) standards.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

MTNM provides CORBA-based Element Management Layer (EML) to Network Management Layer (NML) interfaces for the management of "multi-technology" networks (SONET, SDH, PDH, ATM, Frame Relay, DSL, connectionless networks such as Ethernet, etc.). Management areas are: connection management, NE and EMS configuration, network inventory discovery, euqipment inventory management, performance monitoring, alarm surveillance and event reporting, etc.

MTOSI has gradually taken sets of MTNM interfaces, generalized the operations systems to operations systems interactions and created XML, SOAP Web services based interfaces - recasting and extending MTNM. Like MTNM, it provides a single interface for the management of many technologies. Moreover, MTOSI has had the goal to make XML interfaces independent of the underlying transport (HTTP, JMS, etc.)

MTOSI has been part of TM Forum Interface Program (TIP) since April 2008. Multi Technology OSS Program (mTOP) coordinates advances in the SOAP and XML based MTOSI interface standard, as well as the CORBA/IDL based MTNM standard. MTOSI service classifications are based on the eTOM model, while the information model is based on SID and MTNM data models.

MTOSI uses a single interface infrastructure and applies the same patterns across multiple technologies. For example, the same basic termination point and connection models are applied across all connection-oriented technologies ranging from DWDM to ATM. A similar statement can be made about the MTOSI connectionless model.

Configuration operations provided are described in TMF's DDPs.

6.3.7 Netconf

NETCONF is an IETF configuration management protocol and YANG is its data modeling language in response to SNMP/SMI shortcomings for managing configuration e.g. lack of support for simple things like backup-and-restore of element configuration, no concept of transactions (single- or multibox), many inherent limitations in SMI (e.g. label length) – see [17].

NETCONF is designed to support management of configuration, including:

- Distinction between configuration and state data
- Multiple configuration data stores (candidate, running, startup)
- Configuration change validations
- Configuration change transactions
- Selective data retrieval with filtering
- Streaming and playback of event notifications
- Extensible remote procedure call mechanism

YANG is a data modeling language designed to write data models for the NETCONF protocol. It provides the following features:

- Human readable, and easy to learn representation
- Hierarchical configuration data models
- Reusable types and groupings (structured types)
- Extensibility through augmentation mechanisms
- Supports definition of operations (RPCs)
- Formal constraints for configuration validation
- Data modularity through modules and sub-modules

- Well defined versioning rules

Basic NETCONF Operations are

- Get configuration <get-config>
    - Retrieve all or part of a specified configuration from a named data store
- Get all information <get>
    - Retrieve running configuration and device state information
- Edit configuration <edit-config>
    - Loads all or part of a specified configuration to the specified target configuration
- Copy configuration <copy-config>
    - Create or replace an entire configuration datastore with the contents of another complete configuration datastore.
- Delete configuration <delete-config>
    - Delete a configuration datastore (not applicable to running)
- Lock and unlock <lock>, <unlock>
    - Short-lived lock and unlock of the configuration system of a device
- Close and kill session <close-session>, <kill-session>
    - Graceful (close) or forced (kill) termination of a NETCONF session

There are quite similar goals but different approaches that should be harmonized.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.4 PROCESSES & USE CASES

Autonomous functions in telecommunications management architectures - like SON functions - have different requirements on reaction speed, decision complexity (number of parameters to drive a decision) and size of databases (e.g. how much history of configuration data to take into account).

Having in mind a future solution for end-2-end Configuration Management that includes SON features requires a common understanding and agreement on:

- The autonomous functions, especially here the SON features and their impact on processes, responsibilities and tools to drive the automation approach.
- Deriving functional capability requirements for Configuration Management solutions - distributed in the NM and EM layers - as well as their cooperation from process descriptions.
- In an all-IP network with its dynamic relations an up-to-date Configuration Management Database is even more important for proper change and assurance management than in 2G/ 3G networks. This requires automatically retrieving most of the information (HW inventory, configuration and topology) from all devices and storing it in a central Resource and Configuration Inventory.

Based on the aim to improve the degree of automation of the configuration management process including the benefits of SON functionalities we can identify the following groups of requirements related to SON functional blocks:

- Plug & Play eNodeB deployment to enable automatic configuration/commissioning of eNodeB
    - Harmonised data modelling in all involved tools (Planning DB, Inventory, Configuration Tool).
    - Interfaces and capabilities / FB in all involved tools.
    - Capabilities / FB for the maintenance of configuration data with templates for:
        - Operator defined generic radio parameters,
        - Standard cell parameters,
        - Operator defined transport parameters and
        - Vendor specific parameters.

- Plug & Play configuration to enable automatic configuration of AR (inclusive DHCP) and Sec-GW
    - Interfaces and capabilities / FB in a provisioning tools for AR and DHCP as well as Sec-GW

- Plug & Play PKI configuration to enable automatic configuration of PKI
    - Interfaces and capabilities / FB in a provisioning tool for PKI

- Automatic Neighbor Relations to enable B&W List handling and configuration
    - Data modeling of B&W List in the Tool chain
    - Capabilities for B&W List handling + history of NBR in Planning DB, Inventory, Configuration Tool
    - Interfaces and capabilities / FB in the Tool chain

- Automatic Inventory to enable upload & reconciliation
    - Resource Inventory and Configuration Inventory exchange and Inventory reconciliation. Distinguish between configuration data and resource data.

6.4.1 Business Process Analysis - SON featured LTE deployment

6.4.1.1 Overview

In the following section a typical RAN deployment process flow is presented from a high level perspective.

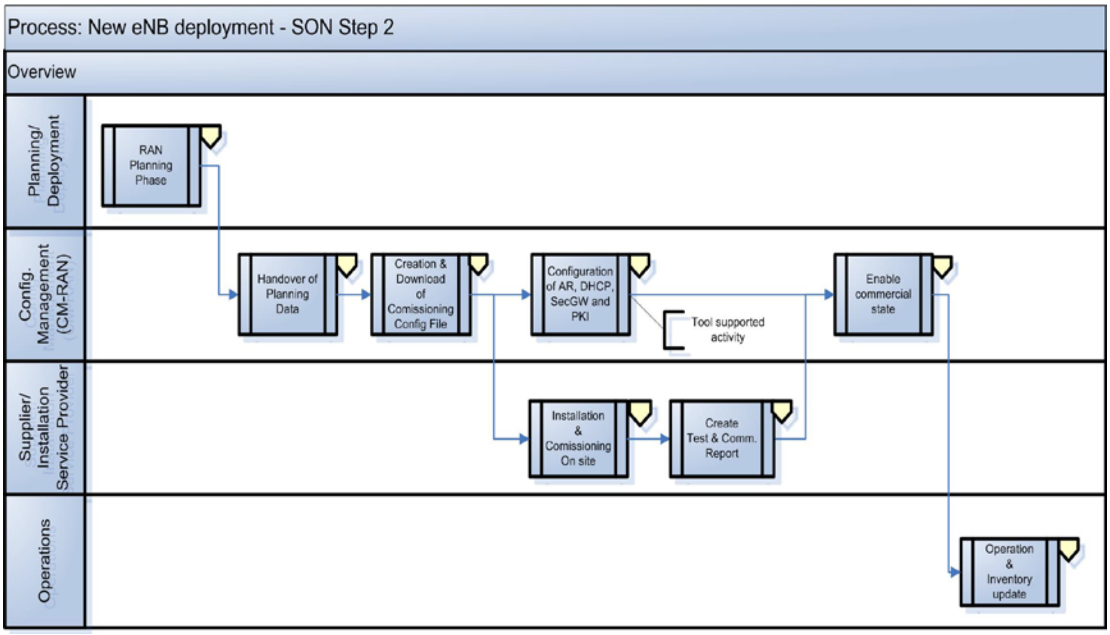


Figure 6.4-1: LTE deployment process – overview

The different high level process steps shown in this figure are broken down to more detailed process steps with higher granularity in the next sub chapters. From there those use cases covering new requirements from increased degree of automation and from including autonomic functionality in the network are depicted.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.4.1.2 Details - SON featured LTE deployment process

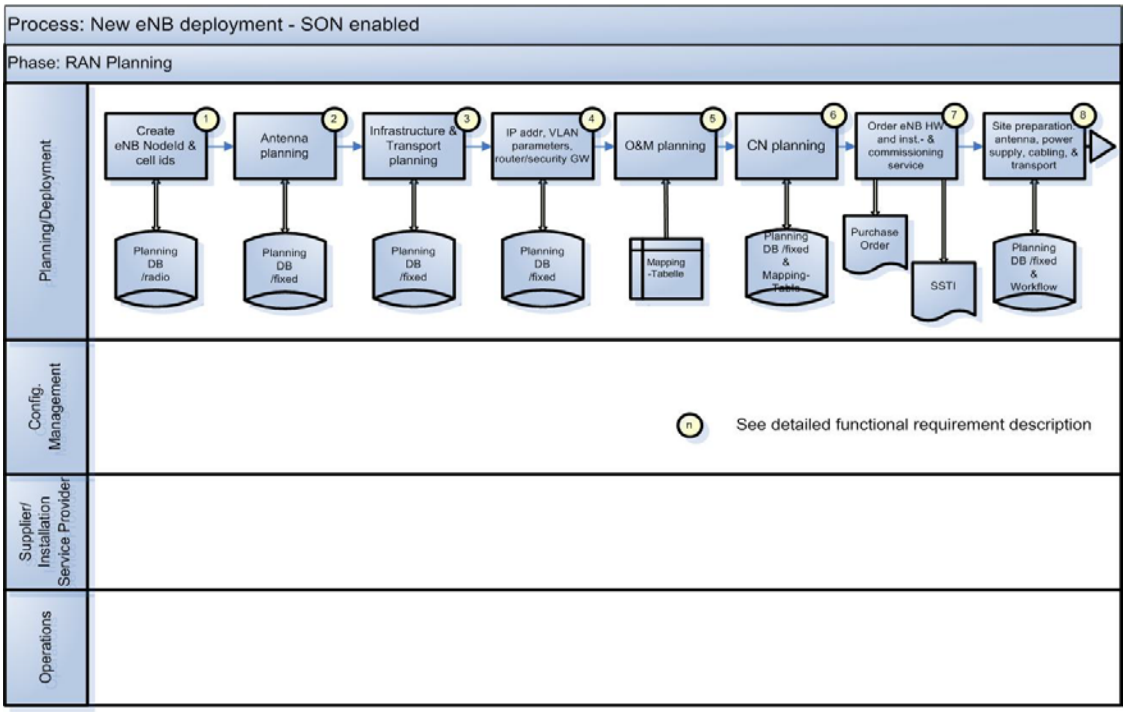


Figure 6.4-2: LTE deployment process – phase: RAN Planning

5.	The eNodeB is planned from the radio point of view: a unique eNodeB identifier and cell identifiers are assigned. After the planning of the basic coverage and following parameters like sector direction further planning activities are given.
6.	Antenna planning is done: consideration of existing antennas, planning of new antennas, cable planning.
7.	Site planning is done: antenna related things, transport related things … (cooling & power are covered in dedicated process steps).
8.	Transport & infrastructure planning is done: HW types, IP addresses, VLAN parameters, router/ security GW configuration.
9.	O&M planning is done: planning of dedicated EMS, planning of IP addresses of EMS (general planning); EMS IP address associated to eNodeB is configured statically in the DHCP configuration depending on the location of the AR.
10.	CN planning is done: planning of dedicated MME, IP address(es) and port(s) of MME to be used; Note: Type Acceptance (TAC) has to be planed by optimization. We assume a similar approach like in 3G, means for LTE rollout that an eNodeB will be tested with a default TAC configuration. The individual TAC will be set with the MileStone commercial.
11.	eNodeB HW and service for installation and commissioning is ordered. eNodeB identifier is given to the

	installation service provider as part of the installation and commissioning order.
12.	Site is prepared: antenna, power supply, cabling, and transport.

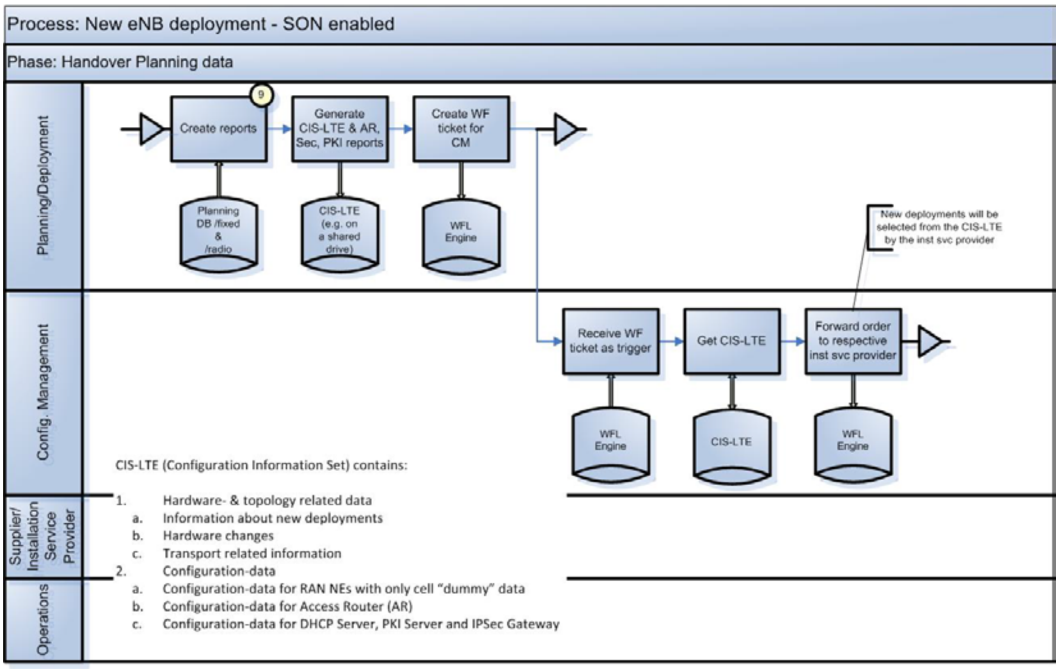


Figure 6.4-3: LTE deployment process – phase: Handover Planning data

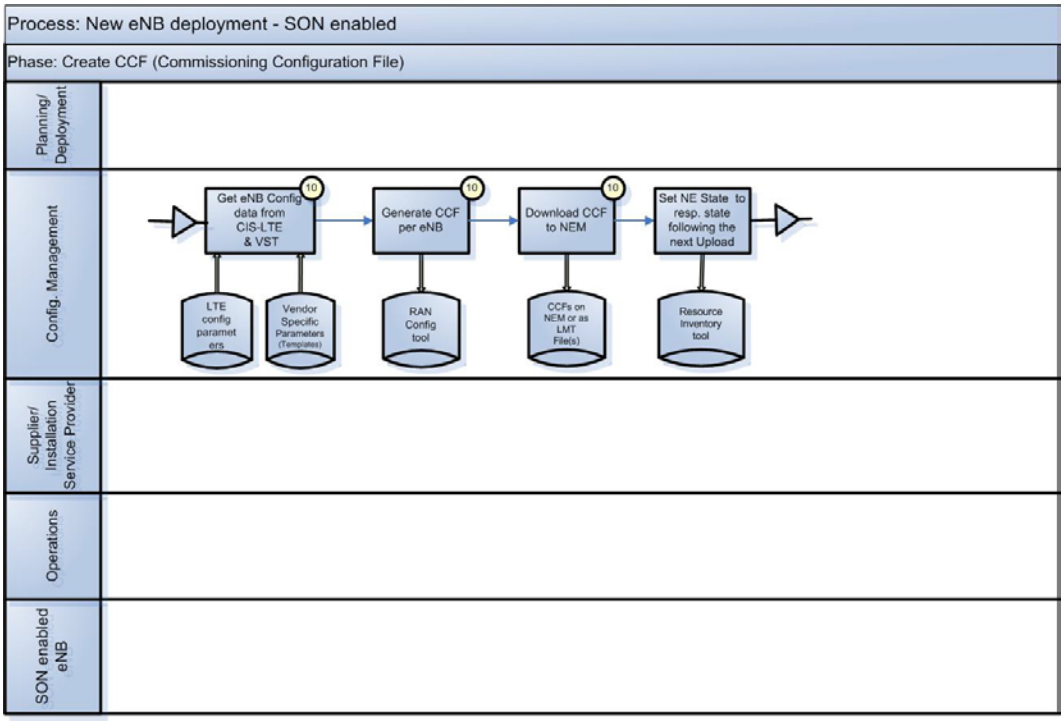


Figure 6.4-4: LTE deployment process – phase: Create CCF

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

13.	The RAN configuration team (CM-RAN) gets planning input forwarded from planning departments in form of DB reports. CM-RAN is triggered via workflow event. Vendor or installation service provider will get an order from Deployment and is able to select the information for “new deployments”.)
14.	Relevant data are read/ extracted from the Planning DB and other sources (templates). After that a Commissioning Configuration file (CCF) is created automatically and transferred & stored in the EM. The vendor or installation service provider is allowed to access the EMS for storing these configuration files. The setting of operator specific defaults should already be included in this step via template usage. To avoid tool adaptations with every new release vendor-specific, release dependant attributes & values to be introduced into eNodeB commissioning configuration file via automatism like base templates in the EM. Additional Process Step needed: provide vendor specific template agreed during the acceptance of the appropriate release to operational persons responsible for CCF (Commissioning Configuration File – see: 6.5.5.1 Configuration parameters and their use during commissioning and optimization) creation.

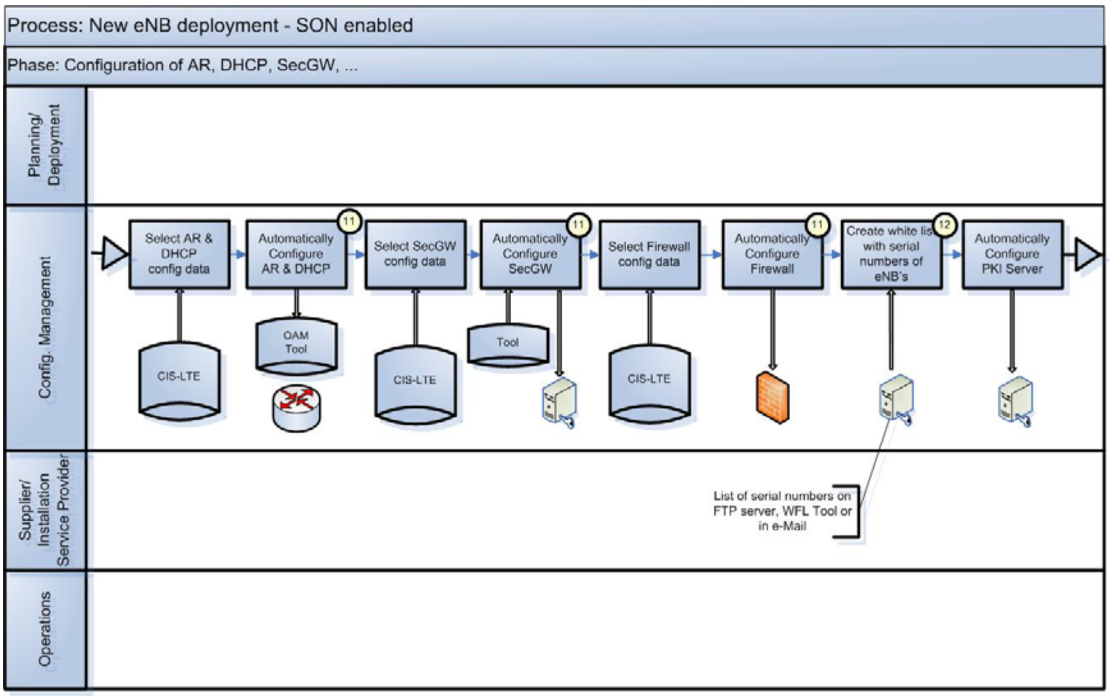


Figure 6.4-5: LTE deployment process – phase: configuration of transport and security etc.

15.	All transport nodes are configured based on the transport planning for eNodeB specific transport parameters: i. Access router (AR) (Note: Internal DHCP is configured generally in all access routers in a static way – not needed to be updated in eNodeB specific way) (Note: Ensure that DHCP related configuration is within standard AR router configuration.) ii. Security GW iii. Others Note: Firewalls are configured in a generic way: no eNodeB specific rules are expected!!!

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

	AR to be configured automatically: • Tool extracts data from Planning Data Set and produces & transfers configuration data file to a router manager. • Router Manager configures AR automatically. Sec-GW to be configured automatically: • Tool extracts data from Planning Data Set and produces & transfers configuration data file to a SECGW manager. • SECGW manager configures Sec-GW automatically.
16.	White list with serial numbers of eNodeBs to be deployed has to been given into PKI server. (From vendor -> planning -> operation) **Note**: maybe this step is done earlier. The serial number of an eNodeB must at latest be configured in PKI before rollout of the dedicated eNodeB.

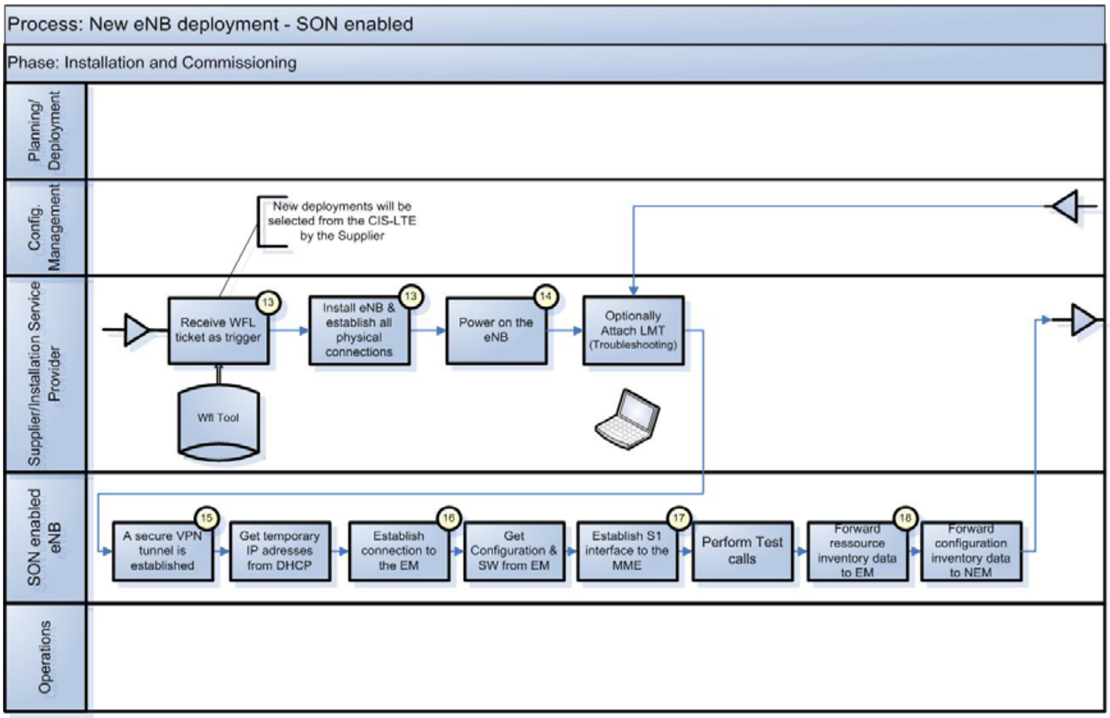


Figure 6.4-6: LTE deployment process – phase: Installation and commissioning

17.	Vendor or Installation Service Provider takes over the responsibility to deliver (install and commission) the eNodeBs and to ensure going onto air in good quality. Vendor or Installation Service Provider gets an order from Operators Deployment Team and is able to select the information for “new deployments”. The Commissioning Config file already delivered to the EMS (see step 11) is converted and enhanced with release specific attribute values and it is stored in the EM. The vendor is allowed by the Operators operation Team to access the EMS for storing these configuration files. The eNodeB is then in the state “visible at NEM”. eNodeB is physically installed and all physical connections are established.

	Option for control: Local Maintenance Terminal (LMT) is plugged in to follow plug'n play process.
18.	eNodeB will be Powered on.
19.	eNodeB runs through P'P process and gets configuration file and SW. A secure tunnel is established between eNodeB and the Security GW. The PKI server is involved in the process to transfer the Operators certificates to the eNodeB. A DHCP server in Operators' network ensures the configuration of temporary IP addresses to setup a configuration tunnel. Prerequisite: The access router is configured in a way such that Plug'n Play is supported.
20.	A connection between the eNodeB and the EMS will be established and the Plug and Play Process continues. The eNodeB gets its final planned parameters by the EM, resets and comes up again with the planned configuration. Exceptional case: if step 15 fails a special procedure should ensure that the rollout process is as efficient as possible. Installation people use LMT to analyse problem issue under assistance of operator at EM. Target is to solve the problem directly when installation people are at the site. To be discussed: if something fails and contact to EMS is already established an alarm shall be raised on NEM. Send a SMS with appropriate indicators on problem to service personal to indicate problem.
21.	The S1 interface between eNodeB and MME is established based on the settings in the configuration file.
22.	Following a successful Test call the eNodeB forwards its physical and logical configuration information to the EM.

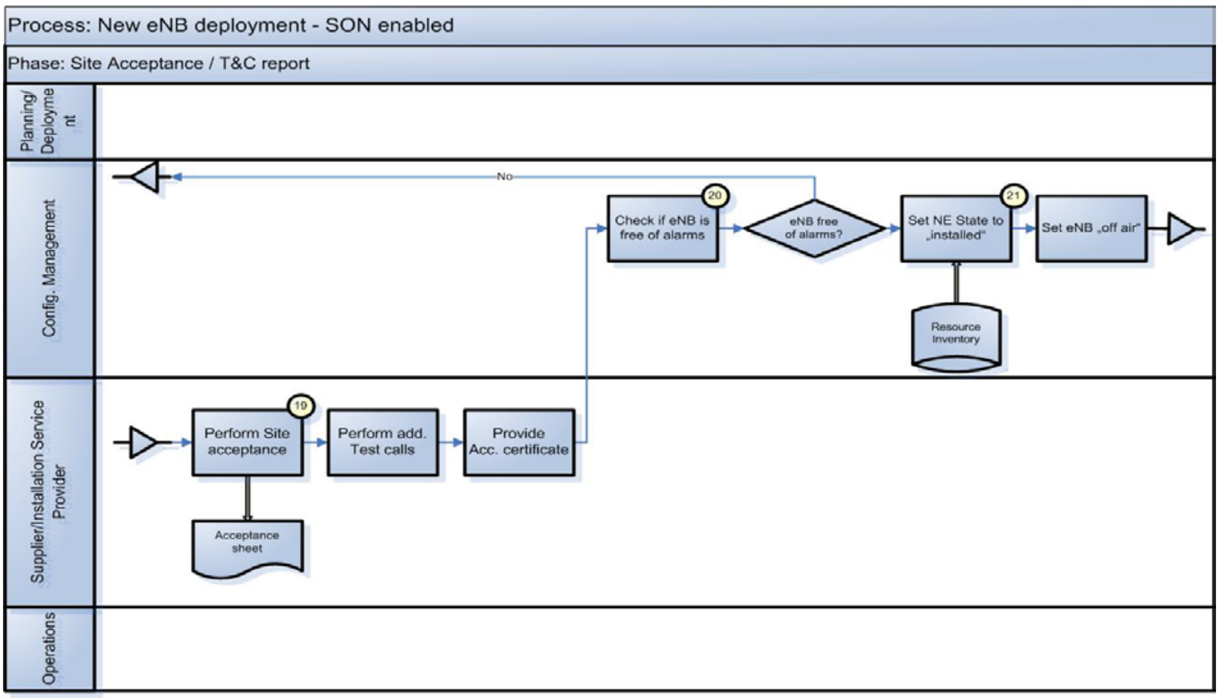


Figure 6.4-7: LTE deployment process – phase: Site acceptance

23.	Site acceptance is executed by the Vendor or ISP. Test calls are successfully performed. Plug and Play Process is finished. Inst Service provider (supplier) gives certificate on successful installation and commission. Test calls (in form of drive test) are done optionally to proof quality.
24.	RAN Configuration Team checks alarm states of eNodeB and cooperates with resp. involves the vendor and the planning department if troubleshooting is needed.
25.	RAN configuration team checks alarm states of eNodeB. In case of absence of alarms the eNodeB state is changed to “installed” (=RFT) but it is not on air. Responsibility handover from deployment team to operation team only if eNodeB is free of alarms.

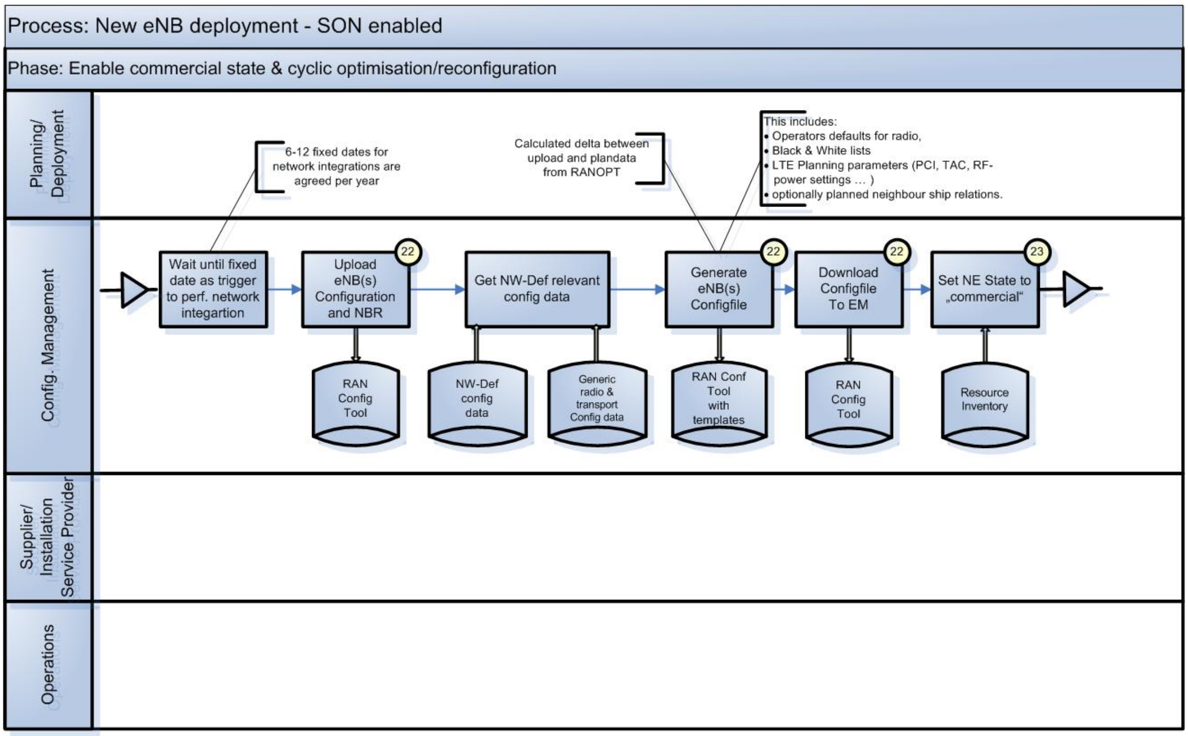


Figure 6.4-8: LTE deployment process – phase: Transition into commercial state

26.	Integration of Network Integration File to be done. (Means preparation and downloading of final configuration files for relevant eNodeBs with all current parameters as described in 2b, 3 of chapter 6.5.5.1.2). This includes: • Operator defaults for radio, • LTE cell specific planning parameters • Black & White lists and • Optionally planned neighbour ship relations. Upload of Neighbour Relationships (NBR) as set in the eNodeBs.
27.	Operator at OMC changes eNodeB status into “commercial” after successfully “final initial configuration”. The appropriate eNodeB is on air. The integration of the “final initial configuration” is normally done for a complete

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

	cluster.

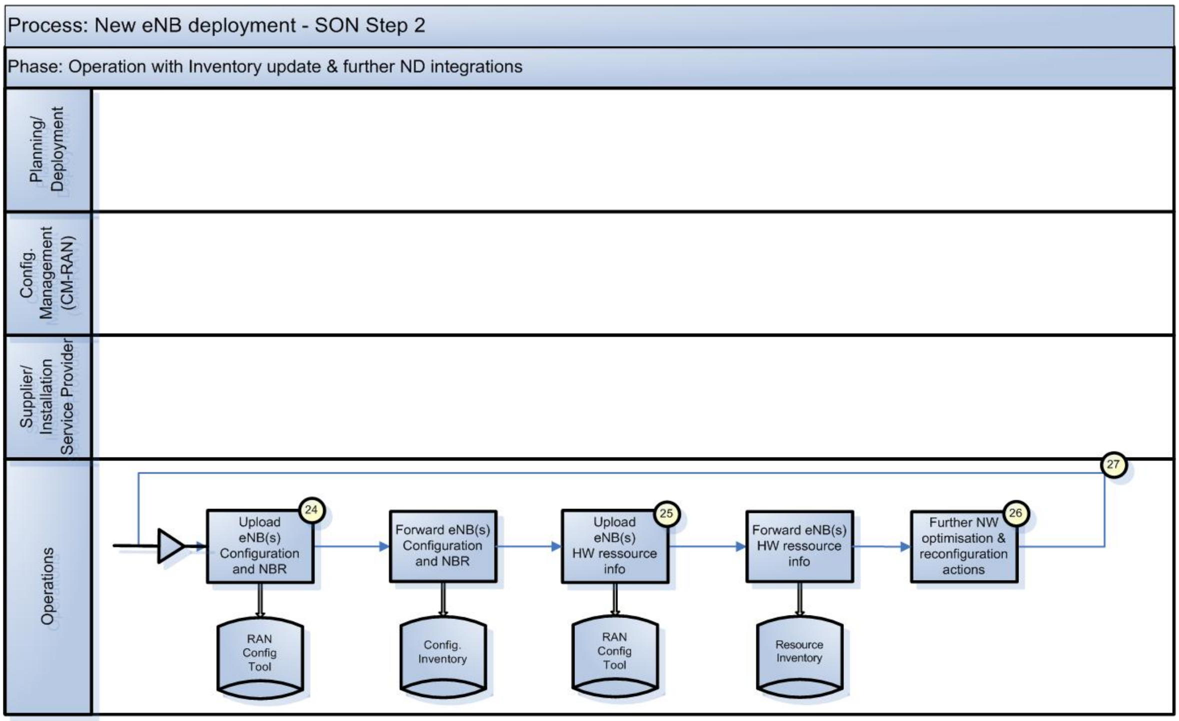


Figure 6.4-9: LTE deployment process – phase: Operation with Auto Inventory update

28.	The complete eNodeB resource inventory data (HW status) is stored in a resource inventory system based on EMS status and manual updated HW lists. The EMS gives an automatic update of HW status via its northbound interface.
29.	The complete eNodeB configuration data as in the network is stored in in a configuration inventory system. The EMS gives an automatic update of the configuration status via its northbound interface (pull preferred as of today? – to be decided!!!) SON AI. Forward of actual configuration data into planning tools – to be defined.
30.	Neighbour planning, configuration and optimisation will be done with support of SON ANR. • Black & White lists and • (optionally planned neighbour ship relations). Upload of NBR as built up by SON ANR in the eNodeBs.
31.	Further periodic changes of the configuration - on a monthly or other base - and their integration as result of optimisation activities (performed by RAN-Optimisation Team). This includes: • Operator defaults for radio • Cell specific parameter (e.g. based on re-planning activities)

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.4.2 Use Cases

6.4.2.1 … Radio, Site & Transmission planning processes

Identifier: Basic eNodeB parameters for P&P	**Use Case Id: RP - 1**
Originating Process : Radio, Site & Transmission Planning	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB is in its early planning phase and not yet physically installed.	
Scenario description: During the installation and commissioning phase each eNodeB has to be provided with a set of configuration data in a so called "commissioning configuration file". These configuration data consist of the elements shown in Figure 6.5-14: eNodeB configuration parameter sets and their relation to CCF and NIF: • Site specific eNodeB parameters; • dummy cell parameter; • standard cell spec. parameters having a generic, net wide nature and underlying a change from time to time; • Operator specific transport parameters having a generic, net wide nature; • Vendor specific parameters that are not touched by the Operator but needed by vendors. All these parameters have to be carefully and consistently planned.	
The resulting requirements: a. The Planning tool shall allow a consistent planning of all these parameter values, maintain them in its database and provide an interface to the CMS for parameter transfer. b. The CMS shall allow maintaining and presenting the above mentioned set of dedicated parameters including ANR specific values for each planned eNodeB (normally prepared by the planning processes). c. The CMS shall provide an interface to the Planning Tools for parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)).	
Justification (Business benefits/ Impact if not Implemented): Basic parameters have to be provided as a pre-deployment activity. This allows to minimize detailed manual planning of neighbour relations, frequencies etc.	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Black & White lists	**Use Case Id: RP – 2**
Originating Process : Radio Planning	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB is in its early planning phase and not yet physically installed **or** the eNodeB is physically installed and should be enabled to enter the NE-state commercial **or** the eNodeB is in the NE-state commercial.	
Scenario description: The list of NR is built up by the ANR functionality. As soon as an UE is moving to the edge of its serving eNodeB it reports possible neighbours (target eNodeB) by their global CI to the serving eNodeB. The serving eNodeB requests the IP address of the target eNodeB from the MME to set up an X2 link. The serving eNodeB will add the target eNodeB into its list of neighbours. In certain cases this mechanism has to be controlled. This can be achieved based on the ANR feature black/ white list. Black & White lists are used to control the built-up of the neighbour relationship list.	
The resulting requirements: a. The Planning tool shall allow a consistent planning of these black/ white lists, maintain them in its database	

and provide an interface to the CMS for parameter transfer. b. The CMS shall provide an interface to the Planning Tools for black/ white list transfer (Initial black/ white list is defined by the planning tool). c. The CMS shall allow maintaining and presenting a black list and a white list for each cell.
Justification (Business benefits/ Impact if not Implemented): This saves manual planning and configuration of neighbour relations. Without Black & White lists the SON configuration activities cannot be controlled.
Miscellaneous Comments/ Useful hints: ANR is seen as standard cell functionality and can be enabled or disabled by default setting during initial setup of cells. ANR can be enabled or disabled on a per cell level. There are standardised parameters (data) to impact ANR behaviour: White and Black List.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
1	NGMN NGCOR/ mm

6.4.2.2 … Radio Deployment process

It is important to notice that the requirements listed in the chapters 4.2.1 and 4.2.2 with the Use Case Ids RP-x and RD-x has to seen as a cluster of dependant requirements that all need to be fulfilled as otherwise a Plug&Play eNodeB installation will not be viable.

Identifier: Initial eNodeB connection (temporary IP addresses) – Plug&Play	**Use Case Id: RD – 1**
Originating Process : Radio Deployment	**Actor role:** Radio Deployer
Precondition(s) and Dependencies: The eNodeB is physically installed and all physical connectors are plugged in. A unique eNodeB identifier has been given to the supplier with the order. It has no IP Address assigned. There shall be no need to pre-configure the eNodeB by the vendor or T-Mobile. Local Maintenance Terminal is not needed.	
Scenario description: The eNodeB issues a request for an IP address to a DHCP server. This DHCP solution integrated with the AR will provide a temporary IP address and the subnet and default G/W addresses for the eNodeB from a pool of IP addresses. Additionally the network element manager IP address, the security gateways IP address and the PKI Server IP address are provided by the DHCP server to the eNodeB during deployment.	
The resulting requirements: The DHCP Server has to be set up with a pool of temporary IP addresses. The CMS shall allow to a) maintain and present a central IP Address pool for temporary and final addresses; b) maintain and present a list of associations eNodeB identifier <-> IP Address, subnet, default GW; c) maintain and present Information about resources that is allocated from a "resource pool"; in terms of a maximumnumber of resources available, number of resources in use, reserved and vacant.	
Justification (Business benefits/ Impact if not Implemented): This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB. It is assumed that IP address and address range planning is internationally coordinated.	
Miscellaneous Comments/ Useful hints: The initial assignment of EMS address and x-GW addresses for a dedicated eNodeB Is assumed to be a planning activity. Initial Data will be set up in the Planning Tools.	
Required timeline (link to roadmap)/ Priority: Step 2	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Identifier: eNodeB authentication via IPSec	**Use Case Id: RD - 2**
Originating Process : Radio Deployment	**Actor role:** Radio Deployer
Precondition(s) and Dependencies: The eNodeB is physically installed and all physical connectors are plugged in. It has an IP Address assigned, knows the EMS and SGW IP addresses and can access the SGW via TCP/IP. The configuration of SecGW and PKI Server has been successfully accomplished.	
Scenario description: The eNodeB has necessary information to get access to a Security Gateway. Based on information delivered by the DHCP solution the eNodeB gets permission to access the inner network and nodes like the network element manager and other management nodes.	
The resulting requirements: See SecGW and PKI configuration in Use Case Ids: **SID - 1** and **SID - 2**	
Justification (Business benefits/Impact if not Implemented): Follow the company security rules.	
Required timeline (link to roadmap) / Priority: Step 2	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR / mm

Identifier: Setup secure tunnel to O&M and access gateways to retrieve the CCF	**Use Case Id: RD – 3**
Originating Process : Radio Deployment	**Actor role:** Radio Deployer
Precondition(s) and Dependencies: The eNodeB is physically installed and all physical connectors are plugged in. The configuration of SecGW and PKI Server has been successfully accomplished. The eNodeB has a temporary IP Address assigned (DHCP) and is able to connect to the security servers to retrieve a certificate and establish a secure end-to-end connection to the network element manager.	
Scenario description: Based on information delivered by the DHCP server and the PKI server/IPSec GW the eNodeB starts to establish a bidirectional, stable and secure end-to-end connection. The network element manager looks up its internal DB for a planned object with the same characteristics as the requesting eNodeB (eNodeB Identifier) and retrieves a CCF dedicated to the requesting eNodeB. This CCF - an aggregated commissioning configuration file - consists of a parameter set with dedicated radio- and IP-parameters (eNodeB UP IP, eNodeB CP IP, MME IP, Port info, Route info, VLAN info, etc.) plus a set of default parameters. This file is delivered back to the requesting eNodeB.	
The resulting requirements: The CMS shall allow a. to maintain and present a set of dedicated radio- and IP-parameters for each planned eNodeB (normally prepared by the planning processes) b. to maintain and present a set of default parameter sets for eNodeBs	
Justification (Business benefits/Impact if not Implemented): This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB.	
Miscellaneous Comments / Useful hints: Default parameter sets – today kept in several template types – see Figure 6.5-14: eNodeB configuration parameter sets and their relation to CCF and NIF.	
Required timeline (link to roadmap) / Priority: Step 2	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Retrieve CCF – Plug&Play	**Use Case Id: RD – 4**
Originating Process : Radio Deployment	**Actor role:** Radio Deployer

Precondition(s) and Dependencies:
The eNodeB is physically installed and all physical connectors are plugged in. A unique eNodeB identifier has been transferred into the eNodeB by appropriate medium latest during the onsite installation phase. It has a temporary IP Address assigned and has established secure end-to-end connections to the security servers and the network element manager.
There shall be no need to pre-configure the eNodeB by the vendor or operator. A CCF has been placed onto the EMS by a operator tool. Local Maintenance Terminal is not needed.

Scenario description:
Based on information delivered by the DHCP server/Configuration Server the eNodeB starts to establish a bidirectional, stable and secure end-to-end connection during its plug & play deployment phase.
The eNodeB requests the CCF from its NEM, the network element manager looks up its internal DB for a planned object with the same characteristics as the requesting eNodeB (unique eNodeB identifier is used to bind a configuration file with the actual eNodeB HW) and retrieves a parameter set dedicated to the requesting eNodeB. This parameter set, consisting of dedicated radio- and IP-parameters plus a set of default parameters has been aggregated into a commissioning configuration file (CCF) based on policy or other selection criteria. This file is delivered back to the requesting eNodeB.
The eNodeB reconfigures itself and comes up with its final IP addresses and a radio configuration as provided in the CCF.

The resulting requirements:
The CMS shall provide an interface to the Planning database for bidirectional parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)) – from **RP - 1**

The CMS shall provide the capability
a) to generate the commissioning configuration file (CCF) out of the respective data sources
b) to transfer this CCF (with the "basic" parameter set) to the EMS in accordance with the northbound interface specification of the EMS for later SON enabled Plug & Play configuration of the eNodeB

Justification (Business benefits/Impact if not Implemented):
This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB.
This saves commissioning cost charged by the supplier to the Operator.

Miscellaneous Comments / Useful hints:
The initial assignment of EMS address and x-GW addresses for a dedicated eNodeB Is assumed to be a planning activity. Initial Data will be set up in the Planning Tools.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
Step 2	NGMN NGCOR/ mm

Identifier: Self Test & Automatic Inventory	**Use Case Id: RD – 5**
Originating Process : Radio Deployment	**Actor role:** Radio Deployer

Precondition(s) and Dependencies:
The eNodeB is physically installed and all physical connectors are plugged in. It has an IP Address assigned and has retrieved its configuration data / parameter set via an end-to-end connections to the network element manager.

Scenario description:
Following the final self test the eNodeB delivers

- a state change notification
- details on its resource configuration

to the network element manager. The element manger can forward this to a CM Tool.

The resulting requirements:
a. The CMS shall allow to upload (from EM), reconcile (between planned data and uploaded data) and forward (to the inventory DBs)

1. the resource inventory information for each installed eNodeB 2. the configuration information for each installed eNodeB in real-time respectively at dedicated intervals (<= 24h). b. The CMS shall have access to these parameter sets on the network element manager on request (in accordance with the northbound interface specification of the network element manager). c. The inventory information is exchanged via NBI/Itf-N using XML file transfer. d. An Automatic Inventory function shall synchronise in real time with the Ordering Party's inventory systems.	
Justification (Business benefits/ Impact if not Implemented): This saves specialized personnel from visiting the installation site and performing a manual report of the eNodeB characteristics.	
Required timeline (link to roadmap)/ Priority: Step 2	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR / mm

6.4.2.3 … Core Network Deployment processes

Left blank intentionally

6.4.2.4 … RAN Transmission (Backhaul) Deployment process

Identifier: Configuration of Access Router and DHCP Server	**Use Case Id: TD – 1**
Originating Process: Configuration management	**Actor role:** Deployer
Precondition(s) and Dependencies: The eNodeB is planed and ordered. Vendor has delivered the respective key(s). The eNodeB is/ will be installed and intends to start the plug & play deployment phase. A Router Management System shall be used to configure the AR automatically from received configuration files.	
Scenario description: The Access routers have to be configured with Inner eNodeB user plane IP address, Inner eNodeB control plane IP address, Inner eNodeB management plane IP address, eNodeB transport IP subnet range, eNodeB transport IP subnet mask, eNodeB transport gateway IP address, Temporary VLAN ID and Permanent VLAN ID. This shall be implemented as automated configuration step.	
The resulting requirements: The CMS shall allow the Configuration of the Access routers. This needs functionality to extract transport configuration data from the planning database and to generate & transfer the respective configuration file(s) to a (possibly integrated) Management Node that configures the AR automatically based on these received configuration files.	
Justification (Business benefits/ Impact if not Implemented): Time and quality enhancement compared with today's manual process based on field developed tools.	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

6.4.2.5 … Security Infrastructure Deployment processes

Identifier: Security Management - Configuration of PKI Server	**Use Case Id: SID - 1**
Originating Process : Configuration Management	**Actor role:** Deployer
Precondition(s) and Dependencies: eNodeB is planed and ordered. Vendor has delivered the respective key(s). eNodeB is / will be installed and intends to start the plug & play deployment phase.	
Scenario description: The capability to manage all required security access data centrally (e.g. IPSec keys), to enable future international consolidation. This is related to SON requirement 2.3 Auto-establishment of secure connection. A white list with serial numbers of eNodeBs to be deployed has to be configured into the PKI server before the commissioning via plug & play of the dedicated eNodeB can start. Keys are forwarded from vendor -> planning -> operation.	
The resulting requirements: a. The CMS has to provide new functionalities (like Scripts) to fetch the keys from a FTP Server and copy them into the PKI Server. b. A FTP Server has to be provided (Cost ownership).	
Justification (Business benefits/ Impact if not Implemented): Manual labour with additional FTE consumption.	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Security Management - Configuration of IPSec Gateway	**Use Case Id: SID - 2**
Originating Process : Configuration Management	**Actor role:** xxx
Precondition(s) and Dependencies: eNodeB is planed and ordered. Vendor has delivered the respective key(s). eNodeB is/ will be installed and intends to start the plug & play deployment phase.	
Scenario description: The capability is needed to manage all required security access data centrally (e.g. IPSec keys), to enable future international consolidation. This is related to SON requirement 2.3 Auto-establishment of secure connection.	
The resulting requirements: Data required for managing access to Operator's services must be centrally stored and managed in the Configuration Inventory as a part of the CMS. The CMS has to provide new functionalities to extracts data from the Planning database and produces & transfers configuration file to a Management Node or Capability that will be used to configure the Sec-GW automatically. The location of the data must not be a constraint. It must be integrated with relationships to all other relevant data e.g. 1. Services 2. Resources Incidents, Changes, Problems… The capability to correlate this data with workflow tickets for IM, CM, ChM, PM and Planning/Deployment must be provided.	
Justification (Business benefits/Impact if not Implemented): The business must be in full control, and be able to give full information about access to our services, and the security of data managed by our services (incl. voice) at all times. Security information must be able to be managed centrally, to enable future international consolidation.	

It must be possible to provide an audit trail about the above at all times. This is a legal requirement in most countries, and is required by the data privacy division.
Miscellaneous Comments/ Useful hints: 1. CMS is fully IP enabled and the master data for all IP planning systems Controls IPSec tunnel etc. 2. All configurable and no configurable parameters at the IP layer, such as IP address, DNS, MAC address, Classes of Service, Traffic Scenario description Parameters, VPN parameters, VPN, IP- Sec, etc. will exist on CMS. 3. CMS for 4G will be the master for other IP planning respectively configuration tools, like tools for planning and configuration of IP routers / switches, DNS - servers, DHCP servers, etc. Basis to Plan, Deploy and Operate 4G network. Requirements vary per Operator.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner / Date (MM-DD-YYYY):**
1	NGMN NGCOR/ mm

6.4.2.6 … RAN Optimization process

Identifier: Black & White lists handling	**Use Case Id: OPT – 1**
Originating Process : Radio Optimization	**Actor role:** Radio Optimizer
Precondition(s) and Dependencies: The eNodeB is up, connection to EMS and MME (via S1) established. No or some NR existing but this leads to suboptimal HO behaviour.	
Scenario description: The list of NR is built up by the ANR functionality. As soon as an UE is moving to the edge of its serving eNodeB it reports possible neighbours (target eNodeB) by their global CI to the serving eNodeB. The serving eNodeB requests the IP address of the target eNodeB from the MME to set up an X2 link. The serving eNodeB will add the target eNodeB into its list of neighbours. In certain cases this mechanism has to be controlled. This can be achieved based on the ANR feature black/ white list. Black & White lists are used to control the setup of neighbour ship lists. Black & white list is defined and refined by the planning tool (see RP – 2).	
The resulting requirements: 1. The CMS shall allow maintaining and presenting a black list and a white list for each cell. 2. The CMS shall allow ANR to be switched on or off. This should be in accordance with the northbound interface specification of the respective network element manager. **3.** The CMS shall provide access to these black lists and white lists for the network element manager on request or populate the network element manager with these lists (in accordance with the northbound interface specification of the network element manager).	
Justification (Business benefits/ Impact if not Implemented): No manual planning and configuration of neighbour relations. Minimum optimisation effort.	
Miscellaneous Comments/ Useful hints: ANR is seen as standard cell functionality and can be enabled / disabled by default setting during initial setup of cells. ANR can be enabled or disabled on a per cell level. There are standardised parameters (data) to impact ANR behaviour: White and Black List.	
Required timeline (link to roadmap)/ Priority: Step 2	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Neighbour relationship lists	**Use Case Id: OPT – 2**
Originating Process : Radio Optimisation	**Actor role:** Radio Optimiser
Precondition(s) and Dependencies:	

The eNodeB is up, connection to EMS and MME (via S1) established. No or some neighbours existing as no pre-configuration is in place but eNodeB might have built up NR based on ANR functionalities.
Scenario description: The list of NR is built up by the ANR functionality. As soon as an UE is moving to the edge of its serving eNodeB it reports visible neighbours (target eNodeB) by their global CI to the serving eNodeB. The serving eNodeB requests the IP address of the target eNodeB from the MME to set up an X2 link. The serving eNodeB will add the target eNodeB into its list of neighbours. As no pre-configuration had happened before, the current topology is not known in the CMS and thus not known to the rest of the OSS tools.
The resulting requirements: o The CMS shall provide an upload functionality of Neighbour relationship lists from the network element manager on request (change notification from eNodeB -> EMS -> CMS) in real-time or o The CMS shall provide a bulk upload for these lists from the network element manager (in accordance with the northbound interface specification of the network element manager). o The CMS shall provide reconciliation functionality for these Neighbour relationship lists.
Justification (Business benefits/ Impact if not Implemented): No manual planning and configuration of neighbour relations. Minimum optimisation effort.
Miscellaneous Comments / Useful hints: For 2G/ 3G this functionality is provided today by CoRan – this could be provided by an upgrade.

Required timeline (link to roadmap)/ Priority: Step 2	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: NE configuration update	**Use Case Id: OPT - 3**
Originating Process : Radio Optimisation	**Actor role:** Change Manager/ Radio Optimiser
Precondition(s) and Dependencies: The eNodeB is up, connection to EMS and MME (via S1) established. No or some neighbours existing as no pre-configuration is in place but eNodeB might have built up NR based on ANR functionalities.	
Scenario description: The operational cell specific parameter set and the generic cell parameter sets designed to model the characteristic of different types of cells (maintained by the Operator in several different templates) are aggregated in the network integration file (NIF) and are downloaded to the eNodeB.	
The resulting requirements: The CMS shall allow to • access and retrieve these parameter sets (ND) from the planning database • upload the current configuration from the network element manager on request (in accordance with the northbound interface specification of the network element manager), • generate the delta between current and planned configuration and • download the delta configuration information onto the EMS in accordance with the northbound interface specification of the NEM for each installed eNodeB in real-time respectively at dedicated intervals (<= 24h).	
Justification (Business benefits/ Impact if not Implemented):	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Configuration History	**Use Case Id: OPT - 4**
Originating Process : Radio Optimisation	**Actor role:** Radio Optimiser

Precondition(s) and Dependencies:	
Scenario description: The RAN optimisation activities – seen as preparatory work for configuration tasks – need fast and uncomplicated access to the eNodeBs historical configuration data and functionalities to analyse and check the data (e.g. consistency, changes, dimensioning rules…). As the reliability of SON activities (introducing changes to the network automatically) is estimated to be in a range between 85% and 95% and thus far beyond 100% the frequency of providing configuration data back from the network into a CMS will be less than once a day – two to three hours should be sufficient.	
The resulting requirements: o The CMS shall provide the complete history of configuration data for eNodeBs for a timeframe of not less than 15 months. The relevant data details have to be identified and agreed. o The CMS shall provide actual network configuration data not later than 3 hours after a change of a configuration has happened. o Enhanced analysis functions have to be provided, for manual and automated, scheduled analysis.	
Justification (Business benefits/ Impact if not Implemented): Reduce optimisation effort.	
Miscellaneous Comments/ Useful hints: Today for 2G/3G a time consuming searching is performed to select historical configurations needed in the optimisation process: Some – but not enough - data are retrievable from Planning Database, others have to be searched for in activation tools – but this search is to complex.	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

6.4.2.7 … Change management & Provisioning and Activation processes

Identifier: NE Transitioning into commercial service	**Use Case Id: ChM – 1**
Originating Process : Change management	**Actor role:** Change Manager
Precondition(s) and Dependencies: The eNodeB is deployed, configured and has been set to NE-state installed.	
Scenario description: The operational cell specific parameter set and the generic cell parameter sets designed to model the characteristic of different types of cells (maintained by the Operator in several different templates) are aggregated in the network integration file (NIF) and are downloaded to the eNodeB.	
The resulting requirements: The CMS shall allow to • access and retrieve these parameter sets (ND) from the planning database • upload the current configuration from the network element manager on request (in accordance with the northbound interface specification of the network element manager), • generate the delta between current and planned configuration and • download the delta configuration information onto the EMS in accordance with the northbound interface specification of the NEM for each installed eNodeB in real-time respectively at dedicated intervals (<= 24h).	
Justification (Business benefits/ Impact if not Implemented):	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Identifier: Rollback	**Use Case Id: ChM – 2**
Originating Process : Change Management	**Actor role:** Change agent
Precondition(s) and Dependencies: Major incidents or disaster has happened	
Scenario description: The capability to roll back configuration data, documenting the network configuration to a certain point in time (E.g. before last Friday 20:00) to restore services after to a certain point in time. Audit trails building Configuration baseline, directly linked to RFCs (Change Management process) performed must be linked into the Inventory solutions especially for Service, Resource, configuration and Policy Inventory. This should enable a rollback of the data to a certain point in time, thus enabling a speedy recovery of the service.	
The resulting requirements: The CMS shall model and provide actual configuration information history.	
Justification (Business benefits/ Impact if not Implemented): After Major incidents or disasters it must be possible to roll back the affected network Configuration to a certain point in time as fast as possible to restore the required service levels, and ensure revenue.	
Miscellaneous Comments/ Useful hints:	
Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Discovery of changes in the networks	**Use Case Id: ChM – 3**
Originating Process : Change management	**Actor role:** Change manager
Precondition(s) and Dependencies: The eNodeB is in commercial use.	
Scenario description: Actual configuration information history is needed to ensure the service quality.	
The resulting requirements: The CMS shall model and provide actual configuration information history. a. The CMS shall discover changes in the networks that are monitored by the Network Element Mgmt Services. b. The CMS shall discover changes in resource details, topology and configuration made to a network element. c. The discovery features shall be configurable in respect to: 1. what type of information that the discovery feature shall cover 2. how often the discovery feature shall interact with the Network Element Mgmt services and the network elements	
Justification (Business benefits/ Impact if not Implemented):	
Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Identifier: Reconciliation in general	**Use Case Id: ChM – 4**
Originating Process : Change management	**Actor role:** xxx
Precondition(s) and Dependencies: The eNodeB is in commercial use.	
Scenario description: Avoidance of discrepancies between the inventory/ planning data and the real network	
The resulting requirements: The CMS shall support reconciliation of discrepancies between information in inventory and network element mgmt services: 1. manually 2. automatically • The CMS shall support to apply rules and a set of criteria to decide if the information shall be I) manually or automatically reconciled and II) the appropriate behaviour when detecting discrepancies: 1. automatically reconciliation; user defines the source that is master 2. manual reconciliation; user defines which users to notify about the required manual reconciliation • The CMS shall notify the user(s) if discrepancies between inventory and network are detected, according to a pre-defined distribution list. • The CMS shall notify user(s) about the outcome of the reconciliation, i.e., after inconsistent data are reconciled.	
Justification (Business benefits/ Impact if not Implemented): This complements the SON feature *Automatic inventory* up onto the data management in the OSS layer. Degree of automation will dramatically decrease if not implemented.	
Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

6.4.2.8 … Configuration Management & Common Data Management processes

Identifier: Configuration Management System	**Item Number: CM - 1**
Originating Process : Configuration Management	**Actor role:** Process Manager
Precondition(s) and Dependencies: Cross functional agreement of the principles of a Configuration Management Process and System	
Description: 1. Information required is to be stored as Configuration Items in a Configuration Management system (CMS). The CMS must link all relevant data sources consolidated into a Common Functional Architecture with an agreed common data model. The categorization of information stored should be split into: Service Inventory, Resource Inventory, Configuration Inventory and policy Inventory. It is to be agreed by all relevant stakeholders in the organisation. 2. The information stored must be labelled with which lifecycle state it is describing e.g. Planned, Active or Removed. 3. Standard interfaces for presenting information to Engineering/Design systems, Planning and Deployment systems and Operations Event management and workflow systems must be provided. RN, CN, PD All engineering, design and testing processes must have access to integrated information to perform the required tasks.	

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

OP The core operations processes: Incident Management (IM), Change Management (ChM), and Problem Management (PM) must have access to integrated information to perform the required tasks. For Incident and Problem diagnosis, and Change Task planning it must be possible to access all required information, linked together from the eNodeB up to the Customer Facing Service (e.g. Internet access) and vice versa. The tasks managed by Change Management of configurations (parameters etc.) supported by Configuration Inventory, and automation (SON) supported by Policy Inventory must be able to be performed across the TMO 5 performed irrespective of the location of the employee, the location of the information stored or the object being managed. SM It must be possible to create consolidated service management reports with integrated information.
Justification (Business benefits/ Impact if not Implemented): All relevant Technology functions must have access to full and relevant information to perform their work across the organisation. This information must be integrated to enable tasks to be performed irrespective of the location of the employee, the location of the information stored or the object being managed.
Miscellaneous Comments/ Useful hints: The CMS has to be multi vendor with a generic layer for the operator. The 4G CMS system has the ability to communicate via standardized interface, like xml or web service Interface, with different systems, such as performance management system, fault management systems, trouble ticket , GIS etc. We suggest using ESB or EAI Bus as communication platform between CMS and other systems. There is a need to keep the planning systems in sync with the actual live configurations within the network. This requirement is essential as with the introduction of the SON features the network will carry out certain configuration changes automatically. If they are not uploaded and made available to the planning systems then further planning might be based on an inaccurate view of the network.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
1	NGMN NGCOR/ mm

Identifier: Configuration Inventory	**Use Case Id: CM – 2**
Originating Process : Configuration Management	**Actor role:** Process Manager
Precondition(s) and Dependencies: Adoption of NGCOR Architecture proposal	
Scenario description: Resource-, Configuration- and Service-Inventory must be centrally stored and managed as a part of the CMS – the Common data management. It must be integrated with relationships to all other relevant data e.g. ▪ Services ▪ Resources ▪ Incidents, Changes, Problems Configuration Inventory is e.g. ▪ Downloadable Operating systems ▪ Software ▪ Licenses ▪ Security data ▪ IP Addresses and address ranges ▪ DNS Names (master) ▪ Cell basic parameter sets and B&W lists	
The resulting requirements: The CMS shall deliver:	

1. The capability to manage all required configuration data centrally. The location of the data must not be a constraint. 2. The capability to report on what configurations where used when and where at a given point in time. 3. The capability to correlate this data with workflow tickets for IM, CM, ChM, PM and Planning/Deployment must be provided.
Justification (Business benefits/ Impact if not Implemented): Configuration Inventory must be able to be managed centrally, to enable future international consolidation. Without this we will lose control of our services and will endanger revenues, and will be inefficient.
Miscellaneous Comments/ Useful hints: Only Configuration Inventory required by Self x required in Phase 0. Central IP address planning is a key requirement to assure consistency for IP address planning.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
Step 2	NGMN NGCOR/ mm

Identifier: Configuration Identification	**Item Number: CM - 3**
Originating Process : Configuration Management	**Actor role:** Process Manager
Precondition(s) and Dependencies:	
Description: The creation, modification, removal evaluation and acceptance of templates, and sources of Master Data for CIs into the Configuration Management System. Support by the CMS and workflow solutions for Configuration Identification from the initial requirements specification, through planning and design, to operation, and eventual removal of configuration data templates and Master Data. This is what generally is known as data modelling. The CMS should have abilities to create and store templates for all resources and network elements that are represented in the system. These templates (specifications) shall define information and configuration details in addition to the default capabilities available for the resource/ network element. The CMS should provide functionality for creating and storing specialisations of an existing design template. These specialisations shall be available to a particular user or user group. For each design template the CMS shall allow users to define resource and network element specific: a) parameters b) allowed parameter values or range of values. Auto-generation of values: Design templates stored in the CMS shall have support for parameters that automatically are given a value from a number series. The CMS should provide functionality for modifying and deleting design templates that are in the CMS: a) copy and rename design template b) delete design template c) add, change and delete parameters and parameter values to the design template. The CMS should separate between design templates in production and those that are drafts and thus only available to a particular user group.	
Justification (Business benefits/ Impact if not Implemented): **<u>Configuration Management Process</u>** **<u>Configuration Identification</u>** To achieve the NGMN requires information held in the Configuration Management System (CMS) to be correct, up to date and of high integrity at all times. This is to be achieved with the Configuration Management Process. 1. Efficiency gains through European organizational consolidation supported by NGMN will not be possible	

2. NGMN Automation will not be possible e.g. 2.2 Automatic inventory 2.3 Auto establishment of secure connections 2.4 Automatic SW/FW management 2.5 Initial configuration 3.1 Automatic neighbourhood relations 4.6 Auto correlation for Fault Management
Miscellaneous Comments/ Useful hints: **Recommendation** Integration of the process workflow of configuration identification into the workflow systems, from request to delivery using the agreed lifecycle states (planned, active, removed)

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
1	NGMN NGCOR/ mm

Identifier: Configuration Control	**Item Number: CM - 4**
Originating Process : Configuration Management	**Actor role:** Process Manager

Precondition(s) and Dependencies:
Description: 1. Ensure that only authorized and identifiable CI s are accepted and recorded, from receipt to disposal. It ensures that no CI is created, modified, or removed without appropriate controlling documentation. 2. All NGMN requirements for automatic inventory (SON Feature 2.2) must be addressed with this requirement. Automatic updates of inventory must be performed in controlled way in the responsibility of the Data Owner. 3. Support by the CMS and workflow solutions for Configuration control from the initial creation of CIs (LC state Planned), through operational implementation (LC state Planned), and removal (LC state removed). 4. Support from the standard workflow solution for the interface between Configuration Management and Change Management. 5. The CMS solution must support auto-discovery for reconciliation between the documented state of the CIs in question and real life status of Network elements to enable the automatic update of CIs in the CMS. 6. The CMS solution must support the SON functionality Automatic inventory by enabling an audit trail of changes, confirmation of automatic updates by the data owners, and correlation of automatic updates with Changes performed with Change Management. 7. The automatic update solution must support the manual confirmation of the data owners that the update can be performed.
Justification (Business benefits/ Impact if not Implemented): To achieve the NGMN requires information held in the Configuration Management System (CMS) to be correct, up to date and of high integrity at all times. This is to be achieved with the Configuration Management Process. 1. Efficiency gains through European organizational consolidation supported by NGMN will not be possible. 2. NGMN Automation will not be possible e.g. Automatic Inventory.
Miscellaneous Comments/ Useful hints: Support this with the common workflow system Periodical upload of live configuration of Huawei Core network elements (MME und SGW) onto Configuration Management system (CMS) to ensure data accuracy in the CMS. This feature is also required because the current change management process doesn't include the formal documentation of the changed configuration after finishing a change. Similar to functionality already provided for Huawei SGSN/GGSN (out of M2000). The uploaded live configurations are used for (manual) delta analysis between planned and live configuration of these network elements. Integrated auto-discovery in CMS for IP NE. Includes eNodeB Router. Essential not possible as manual process

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

The auto-discovery features offer the possibility to detect the new IP node (e.g. eNodeB) and its configuration. There must be various ways to start this function: as a periodical polling mechanism, triggered from OMC or by next download of live configuration. If CMS offers the polling mechanism as an option then the pooling interval should be configurable. Basis to Plan, Deploy and Operate 4G network. Basic IP discovery is already available in TMD. Must have elsewhere.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner/ Date (MM-DD-YYYY):**
Phase 0 RFA	NGMN NGCOR/ mm

Identifier: Status Accounting and Reporting	**Use Case Id: CM – 5**
Originating Process : Configuration Management	**Actor role:** Process Manager

Precondition(s) and Dependencies:

Scenario description:

The reporting of all current and historical data concerned with each CI throughout its life cycle.

The resulting requirements:

1. This enables modifications to CI s and their records to be traceable.
2. Support from the CMS solution to provide a unique CI-ID across the whole organisation to enable reporting of all current and historical data concerned with each CI throughout its life cycle.
3. Requests for Reporting capabilities must be supported by the Workflow solution.
4. The reporting of metrics to contribute to Key Performance Indicators for the process must be supported by the CMS and Workflow solutions.
5. The capability for correlation of information between the audit trail of RFCs (from Change Management, Incidents and Problems from the Operations workflow system(s)), and the audit trail in the inventory systems must be possible.

Justification (Business benefits/ Impact if not Implemented):

To achieve the NGMN requires information held in the Configuration Management System to be correct, up to date and of high integrity at all times. This is to be achieved with the Configuration Management Process.

1. Efficiency gains through European organizational consolidation supported by NGMN will not be possible.
2. Automation will not be possible e.g.

    2.2 Automatic inventory
    2.3 auto establishment of secure connections
    2.4 automatic SW/FW management
    2.5 Initial configuration
    3.1 automatic neighbourhood relations
    4.6 Auto correlation for fault management

Miscellaneous Comments/ Useful hints:

An SQL front end reporting engine must be provided to enable reports to be created by end users. SQL Queries which could lock databases must be rejected by the GUI E.g. Problem Managers, Change Managers. Access to this capability must be controlled through user profiles assigned centrally by an access management function.

Required timeline (link to roadmap)/ Priority:	**Requirement Owner / Date (MM-DD-YYYY):**
2	NGMN NGCOR/ mm

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Identifier: Verification and Audit	**Use Case Id: CM – 6**
Originating Process : Configuration Management	**Actor role:** Process Manager
Precondition(s) and Dependencies:	
Scenario description: **REQ-CON (11)** Capability for logical audits betweens the CMS and real life configurations. **REQ-CON (12)** Capability to tag CIs with a last audit date for physical (live looking physically at the equipment) or logical audits (discovery) betweens the CMS and real life configurations.	
The resulting requirements:	
Justification (Business benefits/ Impact if not Implemented): To achieve the NGMN requires information held in the Configuration Inventory DB to be correct, up to date and of high integrity at all times. This is to be achieved with the Configuration Management Process. Efficiency gains through European organizational consolidation supported by NGMN will not be possible NGMN Automation will not be possible.	
Miscellaneous Comments/ Useful hints:	
Required timeline (link to roadmap)/ Priority: 2	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Compliance Reporting	**Item Number: CM - 7**
Originating Process : Compliance	**Actor role:** *Technology Compliance Manager*
Precondition(s) and Dependencies: The Compliance controls and roles are integrated into the Configuration Management process	
Description: The Guidelines from the Compliance division require proof that a complete and auditable documentation of changes of the Infrastructure is available. The capability to prove that changes to the network are documented and are auditable must be guaranteed with the introduction of the SON features. The requirement from Compliance division is proof that the documentation of the change has been performed, not the documentation itself. (i.e. that the compliance control is working). The level of automation resulting from the implementation of Plug and Play, ANR and the EPC Infrastructure has to be reflected in the automation of this proof. The specific requirement is: 1. All changes resulting from SELF-x are tracked automatically, are auditable, and reportable at all times. 2. The compliance control to ensure this is established in the processes managing Change and Configuration Management.	
Justification (Business benefits/Impact if not Implemented): *As a Technology Compliance Manager* *I want to* have met the Compliance criteria for S-OX404, BiLMoG and ICFR in regard to CM. *So that* any new CM system and/or CM process is checked against requirements from Telekom Compliance. *Acceptance Criteria* 1. Understand if CM impacts one of the listed compliance guidelines. 2. If there is any, make sure that processes and controls are owned, documented and managed aligned with the guidelines. 3. Agree the way forward with the local Technology Compliance Managers and drive pre-testing with external (PwC) or internal auditors.	
Miscellaneous Comments/ Useful hints: Recommendations:	

1. All changes resulting from SELF-x trigger standard change RFCs to be documented in the Workflow systems as change tickets, supporting the Operations Change Management process, and can be reported on from a data warehousing facility. 2. The Compliance controls and roles are to be integrated into the Configuration Management process.	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner/ Date (MM-DD-YYYY):** NGMN NGCOR/ mm

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.5 CONFIGURATION MANAGEMENT REQUIREMENTS

6.5.1 Definitions

For the purposes of the present document, the following terms and definitions - imported from 3GPP TS 32.601 V10.0.0 (2011-03) - apply.

Data: is any information or set of information required to give software or equipment or combinations thereof a specific state of functionality.

Element Manager (EM): provides a package of end-user functions for management of a set of closely related types of Network Elements (NEs). These functions can be divided into two main categories:

- *Element Management Functions* for management of NEs on an individual basis. These are basically the same functions as supported by the corresponding local terminals.
- *Sub-Network Management Functions* that are related to a network model for a set of NEs constituting a clearly defined sub-network, which may include relations between the NEs. This model enables additional functions on the sub-network level (typically in the areas of network topology presentation, alarm correlation, service impact analysis and circuit provisioning).

Information Object Class (IOC): Describes the information that can be passed/used in management interfaces and is modeled using the stereotype "Class" in an UML meta-model.

Managed Element (ME): an ME communicates with a manager (directly or indirectly) over one or more interfaces for the purpose of being monitored and/or controlled. MEs may or may not additionally perform element management functionality. An ME contains equipment that may or may not be geographically distributed.

An ME is often referred to as a "Network Element".

Managed Object (MO): an abstract entity, which may be accessed through an open interface between two or more systems, and representing a Network Resource (NR) for the purpose of management. The Managed Object (MO) is an instance of a Managed Object Class (MOC) as defined in a Management Information Model (MIM). The MIM does not define how the MO or NR is implemented; only what can be seen in the interface.

Managed Object Class (MOC): a description of all the common characteristics for a number of MOs, such as their attributes, operations, notifications and behavior.

Managed Object Instance (MOI): an instance of a MOC, which is the same as a MO as described above.

Management Information Base (MIB): the set of existing managed objects in a management domain, together with their attributes, constitutes that management domain's MIB. The MIB may be distributed over several OS/NEs.

Management Information Model (MIM): also referred to as NRM – see the definition below. There is a slight difference between the meaning of MIM and NRM – the term MIM is generic and can be used to denote any type of management model, while NRM denotes the model of the actual managed telecommunications Network Resources (NRs).

Network Element (NE): is a discrete telecommunications entity, which can be managed over a specific interface e.g. the RNC.

Network Manager (NM): provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EM(s) but it may also involve direct access to the NEs. All communication with the network is based on open and well-standardized interfaces supporting management of multi-vendor and multi-technology NEs.

Network Resource (NR): is a component of a NE, which can be identified as a discrete separate entity and is in an object oriented environment for the purpose of management represented by an abstract entity called Managed Object (MO).

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Network Resource Model (NRM): a model representing the actual managed telecommunications Network Resources (NRs) that a System is providing through the subject IRP. An NRM describes Managed Object Classes (MOC), their associations, attributes and operations. The NRM is also referred to as "MIM" (see above) which originates from the ITU-T TMN.

North Bound Interface (NBI): In network management, usually Southbound Interface refers to the interface exposed to lower layers and the northbound interface refers to the interface exposed to the higher layers. For an EM, lower layer is NE and upper layer is NM. Northbound interface here describes the interface between Element Management -> Network Management Layer.

Operations System (OS): indicates a generic management system, independent of its location level within the management hierarchy.

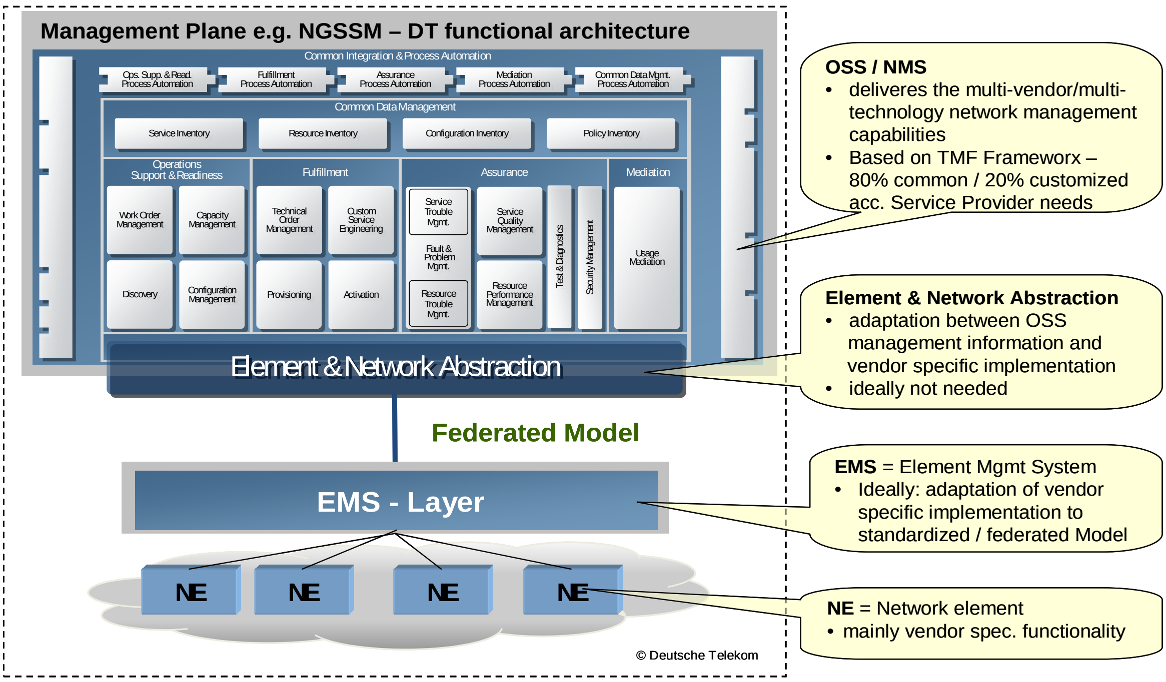


Figure 6.5-1: Agreed NGCOR OSS Architecture: 80% based on Frameworx, 20% operator specific

6.5.2 Requirements on the EMS and its Interfaces from a CM perspective

Configuration management covers the aspects of configuring NEs, software, inventory and path (routing) management.

6.5.2.1 General

REQ-CM (1)

Identifier: REQ-CM (1)	**Rel. Use case id :**	**Priority:**
Title:		
Description: Network control has to be decoupled from data forwarding – this requires a SDN architecture in line with IETF/ITU TMN also for wireline domain where SDN behaves		
Rationale:		

REQ-CM (2)

Identifier: REQ-CM (2)	Rel. Use case id :	Priority:
Title:		
Description: SDN North bound interfaces have to be defined and standardized with respect to currently ongoing wireless/ wireline harmonisation activities performed by 3GPP and TMF.		
Rationale:		

REQ-CM (3)

Identifier: REQ-CM (3)	Rel. Use case id :	Priority:
Title:		
Description: All CM change activities have to be documented in a CM log file or a capability to filter all CM activities from a general log file.		
Rationale:		

REQ-CM (4)

Identifier: REQ-CM (4)	Rel. Use case id :	Priority:
Title:		
Description: Effective and efficient execution of every CM function has to be supported by a well structured dialog window and through the Northbound Interface of the EMS.		
Rationale:		

REQ-CM (5)

Identifier: REQ-CM (5)	Rel. Use case id :	Priority:
Title:		
Description: On implementing CM, the functions described by ITU-T recommendation M.3400 have to be considered and applied accordingly.		
Rationale:		

REQ-CM (6)

Identifier: REQ-CM (6)	Rel. Use case id :	Priority:
Title:		
Description: The configuration data in the CM application on the EMS shall always reflect all real parameter settings on Radio Network Element regardless of the way the parameter has been set.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (7)

Identifier: REQ-CM (7)	Rel. Use case id :	Priority:
Title:		
Description: Inventory data related to NEs like available cards (including information on serial number, hardware version, software version, etc.) available ports (including information on features of ports) have to be provided by the EM.		
Rationale:		

REQ-CM (8)

Identifier: REQ-CM (8)	Rel. Use case id :	Priority:
Title:		
Description: Available as well as reserved resources have to be displayed by a well structured dialog window on the EMS. The same shall also be provided as inventory data through the Northbound Interface of the EMS.		
Rationale:		

REQ-CM (9)

Identifier: REQ-CM (9)	Rel. Use case id :	Priority:
Title:		
Description: The EMS offers via the NBI the capability to a NMS to create, read, update and delete instances of IOCs/ MOCs and update Parameter values per ME type on request.		
Rationale:		

REQ-CM (10)

Identifier: REQ-CM (10)	Rel. Use case id :	Priority:
Title:		
Description: The current configuration (all instances and their attribute values) of the network managed by the EMS has to be accessible by the NMS via a standardized Northbound Interface.		
Rationale:		

REQ-CM (11)

Identifier: REQ-CM (11)	Rel. Use case id :	Priority:
Title:		
Description: Parameter values that characterise a connection, like network access port, type of protection, configuration name, etc. have to be storable and readable and updateable by the NMS via a standardized Northbound Interface / by a well structured dialog window on the EMS in accordance with their properties (e.g. if isWritable = false it can't be updated).		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.5.2.2 Configuration of Network Elements

REQ-CM (12)

Identifier: REQ-CM (12)	Rel. Use case id :	Priority:
Title:		
Description: All parameters of the NE have to be configurable via an EMS standardized northbound interface in accordance with their properties.		
Rationale:		

REQ-CM (13)

Identifier: REQ-CM (13)	Rel. Use case id :	Priority:
Title:		
Description: The setting of a default configuration on the NE by the EMS or the NE itself or the NE with the EMS in cooperation is a vital required feature.		
Rationale:		

REQ-CM (14)

Identifier: REQ-CM (14)	Rel. Use case id :	Priority:
Title:		
Description: The EMS provides the capability to automatically register new NEs if these NEs support automatic registration or plug&play.		
Rationale:		

REQ-CM (15)

Identifier: REQ-CM (15)	Rel. Use case id :	Priority:
Title:		
Description: All so far existing records of the NE and components have to be stored in the EMS database after the operator has approved this action.		
Rationale:		

REQ-CM (16)

Identifier: REQ-CM (16)	Rel. Use case id :	Priority:
Title:		
Description: To simplify respectively to accelerate the configuration, predefined configuration records (templates), allowing the setting of network typical configurations, have to be hold available and offered.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (17)

Identifier: REQ-CM (17)	Rel. Use case id :	Priority:
Title:		
Description: It has to be possible to give a name to a NE or a component, where the name can consist of more than 40 ASCII-characters.		
Rationale:		

REQ-CM (18)

Identifier: REQ-CM (18)	Rel. Use case id :	Priority:
Title:		
Description: Data fields for realising a specific naming concept for NE and connections have to be provided and to be coordinated between the equipment provider and the Ordering Party.		
Rationale:		

REQ-CM (19)

Identifier: REQ-CM (19)	Rel. Use case id :	Priority:
Title:		
Description: A modification of a NE or component name has to be possible.		
Rationale:		

REQ-CM (20)

Identifier: REQ-CM (20)	Rel. Use case id :	Priority:
Title:		
Description: Reconfigurations of NEs have not to cause a need for restart of the NE or of the connections that start, end or pass through the NE.		
Rationale:		

REQ-CM (21)

Identifier: REQ-CM (21)	Rel. Use case id :	Priority:
Title:		
Description: Reconfigurations have not to cause outages on connections on/via this NE.		
Rationale:		

REQ-CM (22)

Identifier: REQ-CM (22)	Rel. Use case id :	Priority:
Title:		
Description: It has to be supported by the GUI of the EMS, that a selected port can be locked or unlocked to enable or disable the reactivation of the selected port.		
Rationale:		

REQ-CM (23)

Identifier: REQ-CM (23)	Rel. Use case id :	Priority:
Title:		
Description: Further on the port types (like UNI, NNI) have to be configurable via the GUI.		
Rationale:		

REQ-CM (24)

Identifier: REQ-CM (24)	Rel. Use case id :	Priority:
Title:		
Description: The entire MIB managed by an EM, has to be collectable and is to be provided by this EM as a data file to the operator via standardized Northbound Interface on request.		
Rationale:		

REQ-CM (25)

Identifier: REQ-CM (25)	Rel. Use case id :	Priority:
Title:		
Description: The collection of the database from the NE by an EMS shall be initiated either by manual interaction or automatically on predefined times.		
Rationale:		

REQ-CM (26)

Identifier: REQ-CM (26)	Rel. Use case id :	Priority:
Title:		
Description: Collection-orders have to be periodically executable within predefined times (daily, weekly, monthly, quarterly intervals).		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (27)

Identifier: REQ-CM (27)	Rel. Use case id :	Priority:
Title:		
Description: An entire collection of data as well as a partial collection (a user defined sub-set of data) has to be supported.		
Rationale:		

REQ-CM (28)

Identifier: REQ-CM (28)	Rel. Use case id :	Priority:
Title:		
Description: The EMS has to be able to collect the data from multiple NEs in parallel.		
Rationale:		

REQ-CM (29)

Identifier: REQ-CM (29)	Rel. Use case id :	Priority:
Title:		
Description: As the period of time needed to collect the data from all NEs (even in parallel) is depending on the number of NEs attached to the EM, it is required to propose system configurations such that the entire collection of data can be done within 1 hour.		
Rationale:		

REQ-CM (30)

Identifier: REQ-CM (30)	Rel. Use case id :	Priority:
Title:		
Description: Data collection by the EMS has not to cause any interference on the call handling by the NEs.		
Rationale:		

REQ-CM (31)

Identifier: REQ-CM (31)	Rel. Use case id :	Priority:
Title:		
Description: Data collection by the EMS is allowed to interfere or to limit maintenance functions only in a limited way. This means, that the maintenance function can be temporarily disabled, but only for the area in which the data collection is actually running.		
Rationale:		

REQ-CM (32)

Identifier: REQ-CM (32)	Rel. Use case id :	Priority:
Title:		
Description: Time intervals for data export have to be configurable (EMS will work in push mode).		
Rationale:		

REQ-CM (33)

Identifier: REQ-CM (33)	Rel. Use case id :	Priority:
Title:		
Description: The structure and content of the files has to be documented completely (see 6.5.3. Interface Information and Documentation Requirements).		
Rationale:		

REQ-CM (34)

Identifier: REQ-CM (34)	Rel. Use case id :	Priority:
Title:		
Description: The EMS comes with a node migration feature, which includes reparenting features: Keep all of the configuration parameters when moving an eNodeB from one MME (/MME Pool) or S-GW (/S-GW Pool) to another one. This includes cell and carrier related parameters, transmission parameters, and neighbouring relations.		
Rationale:		

REQ-CM (35)

Identifier: REQ-CM (35)	Rel. Use case id :	Priority:
Title:		
Description: The EMS comes with a node migration feature, which includes reparenting features: Keep all of the configuration parameters when moving a base station (BTS/NodeB/eNodeB) from one EMS to another one. This includes cell and carrier related parameters, transmission parameters, and neighbouring relations.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.5.2.3 Discovery, backup and restore management

REQ-CM (36)

Identifier: REQ-CM (36)	Rel. Use case id :	Priority:
Title:		
Description: Backup processes – saving all or selected configuration data - can be started both manually and automatically.		
Rationale:		

REQ-CM (37)

Identifier: REQ-CM (37)	Rel. Use case id :	Priority:
Title:		
Description: It must be possible to initiate backup processes after a preset time with freely selectable intervals (e.g., daily, weekly, monthly).		
Rationale:		

REQ-CM (38)

Identifier: REQ-CM (38)	Rel. Use case id :	Priority:
Title:		
Description: Backup files can be transferred to a central location on a suitable storage medium.		
Rationale:		

REQ-CM (39)

Identifier: REQ-CM (39)	Rel. Use case id :	Priority:
Title:		
Description: In addition, it must be possible to transfer backup files to a central backup server.		
Rationale:		

REQ-CM (40)

Identifier: REQ-CM (40)	Rel. Use case id :	Priority:
Title:		
Description: It must be possible to transfer backup files from a central backup server back to the system again.		
Rationale:		

REQ-CM (41)

Identifier: REQ-CM (41)	Rel. Use case id :	Priority:
Title:		
Description: Restoration of configuration data from the backup shall be supported.		
Rationale:		

REQ-CM (42)

Identifier: REQ-CM (41)	Rel. Use case id :	Priority:
Title:		
Description: The creation/ restoration of an earlier CM configuration (snapshot) can be done per eNodeB/BSC/RNC, and it restores all CM data which was changed.		
Rationale:		

REQ-CM (43)

Identifier: REQ-CM (43)	Rel. Use case id :	Priority:
Title:		
Description: The creation/ restoration can be done per EMS, for some or all of the eNodeB/BSC/RNC this platform manages.		
Rationale:		

6.5.2.4 Software Management

REQ-CM (44)

Identifier: REQ-CM (44)	Rel. Use case id :	Priority:
Title:		
Description: A download & activation function (agent to manager) and a upload function (manager to agent) for transferring information from NE to EMS or from EMS to NE and storing the information on NE and EMS has to be provided. The information transferred could be: a. Configuration data records. b. Set of parameters, including those on hardware version, operating system software, firmware and other relevant network typical information.		
Rationale:		

REQ-CM (45)

Identifier: REQ-CM (45)	Rel. Use case id :	Priority:
Title:		
Description: The means for a complete monitoring of procedures for the upload and download function has to be provided.		
Rationale:		

REQ-CM (46)

Identifier: REQ-CM (46)	Rel. Use case id :	Priority:
Title:		
Description: The means for a cancelling / terminating of already started procedures for the upload and download function has to be provided.		
Rationale:		

REQ-CM (47)

Identifier: REQ-CM (47)	Rel. Use case id :	Priority:
Title:		
Description: An automated software download to all or selected NEs has to be enabled by configurable scripts or procedures.		
Rationale:		

REQ-CM (48)

Identifier: REQ-CM (48)	Rel. Use case id :	Priority:
Title:		
Description: The automated software download has to be manageable via NBI and the EMS GUI.		
Rationale:		

REQ-CM (49)

Identifier: REQ-CM (49)	Rel. Use case id :	Priority:
Title:		
Description: Already existing configuration data records have to be completely taken over, when a change in software happens.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (50)

Identifier: REQ-CM (50)	Rel. Use case id :	Priority:
Title:		
Description: Considering all feasibility aspects, all work to be performed prior, during and after remote installation of a new Software Release and taking into account that the process is handled by just one operator, a new Software Release shall be installable on a single Network Element/ EMS within [to be filled in by the Supplier for each type of applicable NE and to be distinguished between different kinds of Upgrade and/or Updates if applicable] minutes.		
Rationale:		

REQ-CM (51)

Identifier: REQ-CM (51)	Rel. Use case id :	Priority:
Title:		
Description: During the process described no manual intervention and active task apart from the regular Network monitoring shall be needed, neither on the Network Elements nor on the EMS / management application.		
Rationale:		

REQ-CM (52)

Identifier: REQ-CM (52)	Rel. Use case id :	Priority:
Title:		
Description: During activation of a new Software Release or roll back there shall be no downtime for fully redundantly covered Network Elements/ EMSs.		
Rationale:		

REQ-CM (53)

Identifier: REQ-CM (53)	Rel. Use case id :	Priority:
Title:		
Description: During activation of a new Software Release for not redundantly covered Network Elements/EMSs the downtime as described in an SLA shall be calculated.		
Rationale:		

6.5.2.5 Inventory Management

REQ-CM (54)

Identifier: REQ-CM (54)	Rel. Use case id :	Priority:
Title:		
Description: Inventory data (network resource related) has to be managed by the EMS.		
Rationale:		

REQ-CM (55)

Identifier: REQ-CM (55)	Rel. Use case id :	Priority:
Title:		
Description: A main position within the inventory listing is the electronic type label.		
Rationale:		

REQ-CM (56)

Identifier: REQ-CM (56)	Rel. Use case id :	Priority:
Title:		
Description: The EMS has to provide a feature to capture all information regarding a NE.		
Rationale:		

REQ-CM (57)

Identifier: REQ-CM (57)	Rel. Use case id :	Priority:
Title:		
Description: A search based on relevant parameters has to be supported. The parameters for the search are identical to those on a NE's type label.		
Rationale:		

REQ-CM (58)

Identifier: REQ-CM (58)	Rel. Use case id :	Priority:
Title:		
Description: The entering of single or combined search parameters has to be supported.		
Rationale:		

REQ-CM (59)

Identifier: REQ-CM (59)	Rel. Use case id :	Priority:
Title:		
Description: The result of the search activity has to be documented in a data file.		
Rationale:		

REQ-CM (60)

Identifier: REQ-CM (60)	Rel. Use case id :	Priority:
Title:		
Description: The file structure has to be published (see 6.5.3. Interface Information and Documentation Requirements).		
Rationale:		

REQ-CM (61)

Identifier: REQ-CM (61)	Rel. Use case id :	Priority:
Title:		
Description: The result of the search activity has to be printed by a printer, listed in the GUI and stored on an external data carrier on request by the user.		
Rationale:		

REQ-CM (62)

Identifier: REQ-CM (62)	Rel. Use case id :	Priority:
Title:		
Description: All inventory information stored in the NE has to be accessible via the EMS.		
Rationale:		

REQ-CM (63)

Identifier: REQ-CM (63)	Rel. Use case id :	Priority:
Title:		
Description: Available and unused resources have to be exposed to the NMS NBI.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (64)

Identifier: REQ-CM (64)	Rel. Use case id :	Priority:
Title:		
Description: Reports on reserved, available and unused, etc. resources have to be listed on the GUI.		
Rationale:		

REQ-CM (65)

Identifier: REQ-CM (65)	Rel. Use case id :	Priority:
Title:		
Description: These reports have to be configurable by flexible filters to create views based on e.g. network topologies, selected NEs, etc.		
Rationale:		

REQ-CM (66)

Identifier: REQ-CM (66)	Rel. Use case id :	Priority:
Title:		
Description: The format/ structure of the data files have to be described by the Supplier.		
Rationale:		

REQ-CM (67)

Identifier: REQ-CM (67)	Rel. Use case id :	Priority:
Title:		
Description: The status of a component (inventory unit or configuration item) has to be documented in the report.		
Rationale:		

REQ-CM (68)

Identifier: REQ-CM (68)	Rel. Use case id :	Priority:
Title:		
Description: The existing inventory data and configuration data on components and connections have to be accessible through the Northbound Interface of the EMS.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (69)

Identifier: REQ-CM (69)	Rel. Use case id :	Priority:
Title:		
Description: The initiation for reading out this data must be given by a super ordinate discovery process (initiated by an NMS) through the Northbound Interface of the EMS.		
Rationale:		

6.5.2.6 SON specific O&M requirements

REQ-CM (70)

Identifier: REQ-CM (70)	Rel. Use case id :	Priority:
Title:		
Description: Network Management and Element Management System shall be synchronized in real time following SON initiated network changes. Notifications following SON initiated network changes shall be available real-time on the CM Northbound Interfaces to the NMS.		
Rationale:		

6.5.3 Interface Information and Documentation Requirements

6.5.3.1 The Operators pain - Expenses for CM-Northbound Interface Integration

During network configuration planning and plan data building, many types of constraints and dependencies need to be noted and taken care of. The risk that new erroneous or incomplete plan harms network functioning after activation to network elements needs to be minimized.

Current practice for CM OSS tool adaptation and deployment as well as operations results are far from being satisfactory due to partially missing/ unclear documentation of the information model and the dependencies

- Huge Implementation Expense
  - high effort for first Interface implementation
  - with new Software Release new Parameters need to be manually included to CM-OSS.

- Incomplete documentation of Information model and Dependency Definitions
  - partially planned changes are rejected by the EM/ NE because dependencies and value range checks have not been implemented due to incomplete documentation
  - new night work for the configuration tasks has to be scheduled because these dependency and value range checks could not be implemented
  - Planned changes lead to unpredictable behaviour of network with loss of quality and revenue
  - To obviate these problems the “information requirements” in the following sections are defined – their implementation will lead to

- Reduced Implementation Expense

- Standardization will nearly erase the efforts for first implementation
    - Standardization will erase the efforts for the integration of new adaptations.

- Implementation of Dependency Definitions
    - manual definition of simple easy dependencies is no longer required, as already included into the interface files in machine readable format
    - more complex dependencies might still require work on CM-OSS – but delivery in machine readable format will enable the automation of the tool-adaptation process.

- Success factors
    - Incentives for all industry players.

6.5.3.2 Meta Model, Domain Information Model and Concrete Configuration

To describe the information requirements the following conventions apply:

Three model levels are used

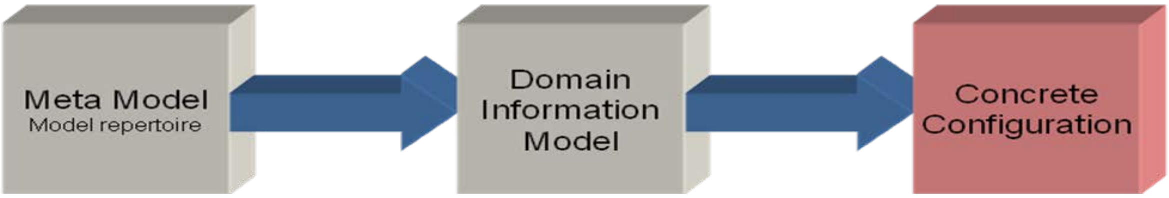


Figure 6.5-2: Information models

where

- **The Meta Model (model repertoire)**
  [ftp://ftp.3gpp.org/TSG_SA/WG5_TM/Ad-hoc_meetings/Virtual-TMF-Align/S5vTMFa312.zip]
  Defines the structure/content of the Information Model
- **Domain Information Model**
  Defines the Object Classes together with their Attributes for a specific managed interface
- **Concrete Configuration**
  Contains a list of (planned) Object Instances together with their (planned) Attribute Values for a set of specific network elements

REQ-CM (71)

Identifier: REQ-CM (71)	**Rel. Use case id :**	**Priority:**
Title:		
Description: The **Meta Model** should be in line with the FMC model repertoire		
Rationale:		

REQ-CM (72)

Identifier: REQ-CM (72)	Rel. Use case id :	Priority:
Title:		
Description: In addition to REQ-CM (71) the following **Object Class Properties** are required: • **Maxinstances** Defines the number of object instances that can exist as child of a parent • **dependencies** Lists all related objects and their required settings, so that the object can be correctly defined		
Rationale:		

REQ-CM (73)

Identifier: REQ-CM (73)	Rel. Use case id :	Priority:
Title:		
Description: In addition to REQ-CM (71) the following **Attribute Properties** are required: • **multiplicity** Defines the number of values an attribute can simultaneously have. Example: NE is supporting 3 different Handover-Algorithmes "1-IntraFrequency Quality Handover", "2-InterFrequency Quality Handover", "3-InterRAT Load-Handover". If this property=yes --> from 3 possible Algorithms 1 & 2 are allowed, 3 is not • **dependency** Lists all related parameters and their required settings, so that the parameter could be changed / set • **ServiceImpactOfModification** what happens if this attribute is modified (textual description - conditions) – examples: For "cell frequency" parameter change: Cell unavailability for x Minutes For Transport or Security Parameter change: Site Reboot required or Board reset required • **isStandardized** Identifies the name of the standardized attribute it complies with whereby priority is that the name has to be identical to the name given in the standard specification • **featureRelevance** Identifies that the attribute is relevant for the named feature (traceback) • **newInThisRelease** Identifies whether attribute is new in the current release - explicitly marked		
Rationale:		

REQ-CM (74)

Identifier: REQ-CM (74)	Rel. Use case id :	Priority:
Title:		

Description:

The **Domain Information Model** defines all object classes based on the meta model requirements

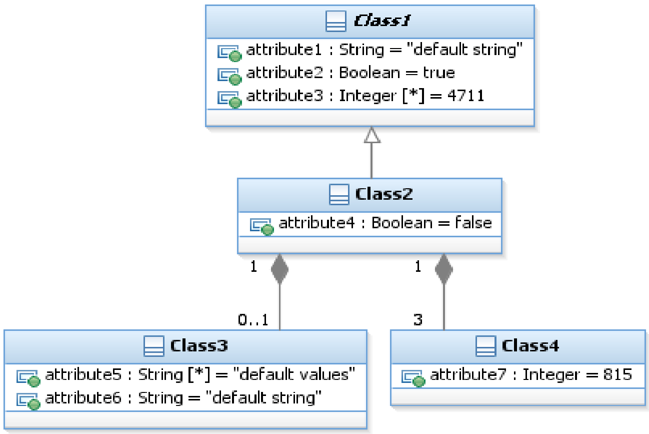


Figure 6.5-3: Domain Information Model

Rationale:

REQ-CM (75)

Identifier: REQ-CM (75)	Rel. Use case id :	Priority:
Title:		

Description:

The **Concrete Configuration** defines the required configuration as collection of object instances and their attribute values

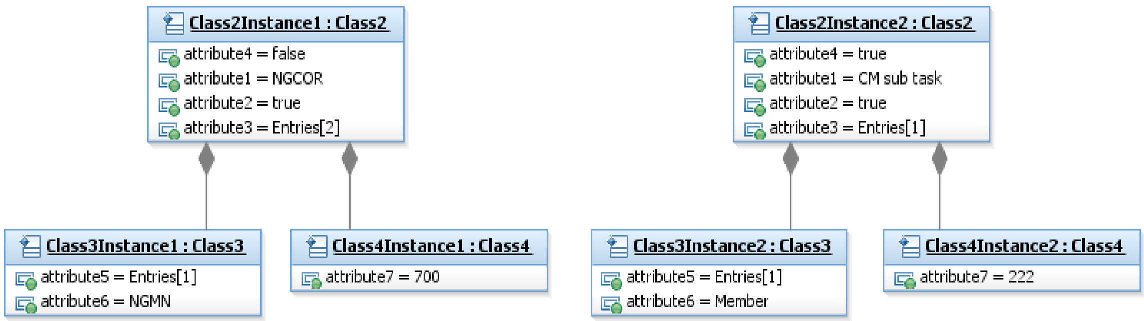
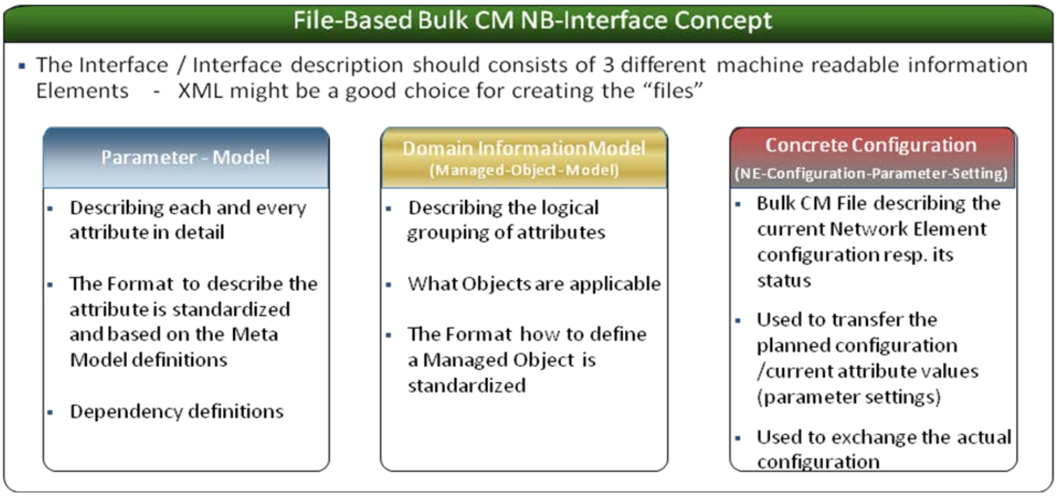


Figure 6.5-4: Concrete Configuration

Rationale:

6.5.3.3 Parameter / Attribute documentation, Interface documentation & information exchange

REQ-CM (76)

Identifier: REQ-CM (76)	**Rel. Use case id :**	**Priority:**
Title:		
Description: The Interface/ Interface description shall consists of 3 different machine readable information Elements:  **Figure 6.5-5: Interface describing elements** The Parameter Model - a static model for a release - describes the parameters / attributes and dependencies in detail. The description complies with the definitions of the Meta model. The Managed object model - a static model for a release - complies with the definitions from the Domain information model. The NE configuration parameter setting file -a dynamic file transferred via the interface between EMS and the NMS - complies with the definitions from the Specific configuration.		
Rationale:		

REQ-CM (77)

Identifier: REQ-CM (77)	Rel. Use case id :	Priority:
Title:		
Description: For each Parameter an entry in the Parameter Model needs to be available/ provided by the Vendor. The parameter model - a static model for a release - describes the parameters / attributes and dependencies in detail.		
Rationale:		

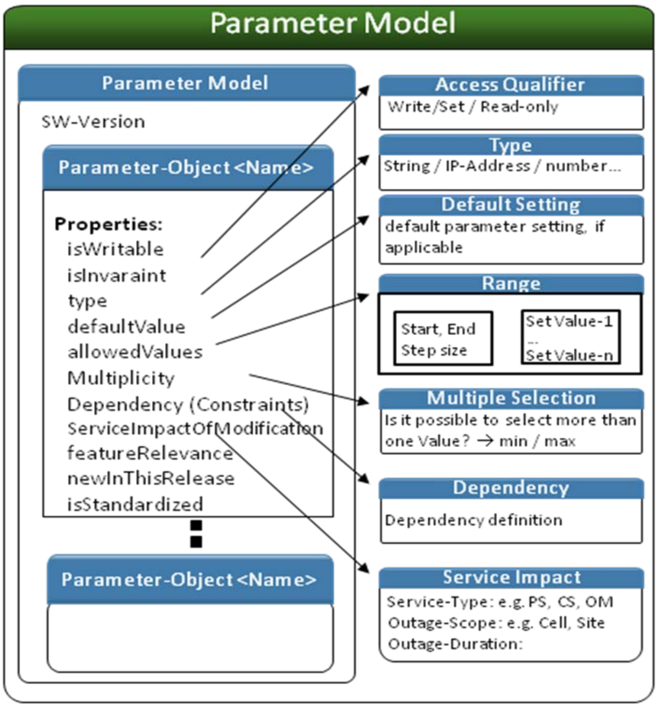
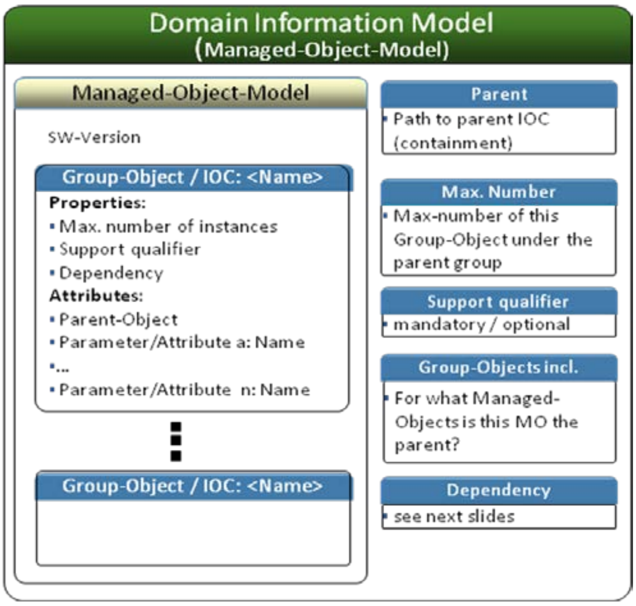


Figure 6.5-6: Parameter model

REQ-CM (78)

Identifier: REQ-CM (78)	Rel. Use case id :	Priority:
Title:		
Description: The Vendor shall - for every parameter - provide a list with dependencies, with easy condition settings. Dependency Definition shall be constructed out of simple operators: • if • and / or / not … • + - * : > / < / = / ==		
Rationale:		

REQ-CM (79)

Identifier: REQ-CM (79)	Rel. Use case id :	Priority:
Title:		
Description: The Object Model documentation - Covering all standardized and vendor specific MOs - will be delivered by the Vendor. It will allow the CM-OSS to identify configuration limits and dependencies to HW, SW and Licences.  **Figure 6.5-7: Managed object model**		
Rationale:		

REQ-CM (80)

Identifier: REQ-CM (80)	Rel. Use case id :	Priority:
Title:		
Description: The parameter model and the Domain Information Model (Managed object model) will be stored on the EMS.		
Rationale:		

REQ-CM (81)

Identifier: REQ-CM (81)	Rel. Use case id :	Priority:
Title:		
Description: With every update for a new release on the EMS the EMS will notify the NMS - if subscribed - via the NBI about this change.		
Rationale:		

REQ-CM (82)

Identifier: REQ-CM (82)	Rel. Use case id :	Priority:
Title:		
Description: The EMS offers the capability to a NMS to read the Parameter Model and the Domain Information Model via the NBI as XML coded files. This machine readable model information will be used to automate the adaptation of the CM OSS interfaces (GUI and NBI manager) and the information model in the configuration inventory to the new EMS model release.		
Rationale:		

REQ-CM (83)

<table>
<tr><td>Identifier: REQ-CM (83)</td><td>Rel. Use case id :</td><td>Priority:</td></tr>
<tr><td colspan="3">Title:</td></tr>
<tr><td colspan="3">Description: The NE configuration parameter setting file - a dynamic file, transferred via the interface between EMS and the NMS - complies with the definitions from the Concrete Configuration.

The File carries the planned or actual configuration parameter setting/attribute values and the references to templates if any (with predefined values for parameters that had been transferred to the EMS before).

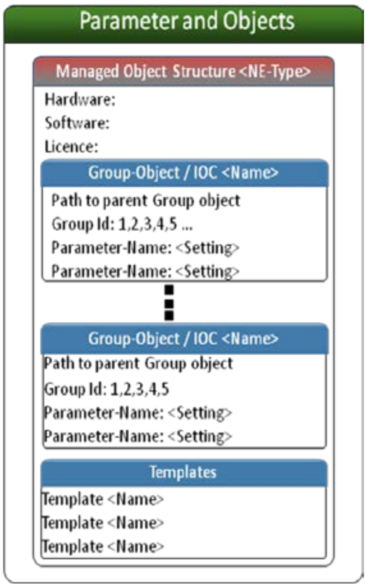


Figure 6.5-8: Configuration parameter file

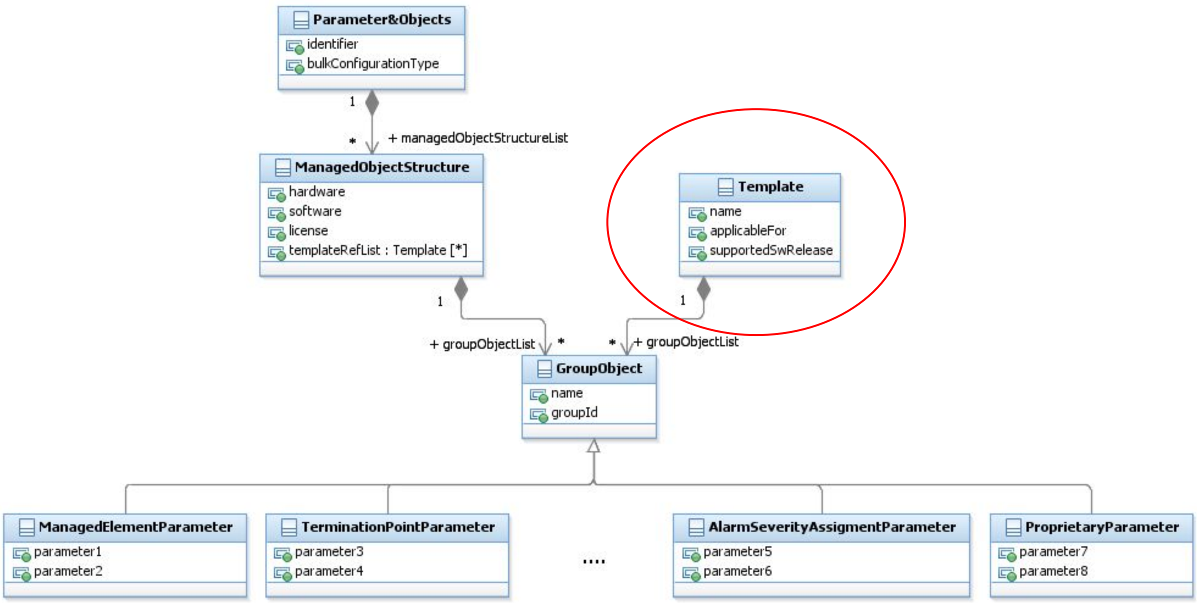


Figure 6.5-9: Templates in the object model</td></tr>
<tr><td colspan="3">Rationale:</td></tr>
</table>

6.5.4 Configuration Management Requirements to support the deployment process

6.5.4.1 … Radio, Site & Transmission planning processes

The resulting requirements from Use Case Id: RP - 1:

REQ-CM (84)

Identifier: REQ-CM (84)	Rel. Use case id : RP - 1	Priority:
Title:		
Description: The Planning tool shall allow a consistent planning of all these attribute values, maintain them in its database and provide an interface to the CMS for parameter transfer: • Site specific eNodeB parameters; • Dummy cell parameter; • Standard cell spec. parameters having a generic, net wide nature and underlying a change from time to time; • Operator specific transport parameters having a generic, net wide nature; • Vendor specific parameters that are not touched by the Operator but needed by vendors.		
Rationale:		

REQ-CM (85)

Identifier: REQ-CM (85)	Rel. Use case id : RP - 1	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting the above mentioned set of dedicated parameters including ANR specific values for each planned eNodeB (normally prepared by the planning processes).		
Rationale:		

REQ-CM (86)

Identifier: REQ-CM (86)	Rel. Use case id : RP - 1	Priority:
Title:		
Description: The CMS shall provide an interface to the Planning Tools for parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)).		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

The resulting requirements from Use Case Id: RP - 2:

REQ-CM (87)

Identifier: REQ-CM (87)	Rel. Use case id : RP - 2	Priority:
Title:		
Description: The Planning tool shall allow a consistent planning of these black/ white lists, maintain them in its database and provide an interface to the CMS for parameter transfer.		
Rationale:		

REQ-CM (88)

Identifier: 0	Rel. Use case id : RP - 2	Priority:
Title:		
Description: The CMS shall provide an interface to the Planning Tools for black/ white list transfer (Initial black/ white list is defined by the planning tool).		
Rationale:		

REQ-CM (89)

Identifier: REQ-CM (89)	Rel. Use case id : RP - 2	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting a black list and a white list for each cell.		
Rationale:		

6.5.4.2 … Radio Deployment process

The resulting requirements from Use Case Id: RD – 1:

The DHCP Server has to be set up with a pool of temporary IP addresses. The CMS shall allow to

REQ-CM (90)

Identifier: REQ-CM (90)	Rel. Use case id : RD – 1	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting via GUI and interface a central IP Address pool for temporary and final addresses.		
Rationale:		

REQ-CM (91)

Identifier: REQ-CM (91)	Rel. Use case id : RD – 1	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting via GUI and interface Information about resources that is allocated from a “resource pool”; in terms of a maximum number of resources available, number of resources in use, reserved and vacant.		
Rationale:		

The resulting requirements from Use Case Id: RD – 2:

REQ-CM (92)

Identifier: REQ-CM (92)	Rel. Use case id : RD – 2	Priority:
Title:		
Description: See SecGW and PKI configuration in Use Case Ids: SID - 1 and SID – 2		
Rationale:		

The resulting requirements from Use Case Id: RD – 3:

REQ-CM (93)

Identifier: REQ-CM (93)	Rel. Use case id : RD – 3	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting via GUI and interface a set of dedicated radio- and IP-parameters for each planned eNodeB. (normally prepared by the planning processes)		
Rationale:		

REQ-CM (94)

Identifier: REQ-CM (94)	Rel. Use case id : RD – 3	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting via GUI and interface a set of default parameter sets for eNodeBs.		
Rationale:		

The resulting requirements from Use Case Id: RD – 4:

REQ-CM (95)

Identifier: REQ-CM (95)	Rel. Use case id : RD – 4	Priority:
Title:		
Description: The CMS shall have an interface to the Planning/ Configuration Inventory database for bidirectional parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)) – from RP – 1.		
Rationale:		

REQ-CM (96)

Identifier: REQ-CM (96)	Rel. Use case id : RD – 4	Priority:
Title:		
Description: The CMS shall provide the capability to generate the commissioning configuration file (CCF) out of the respective data sources.		
Rationale:		

REQ-CM (97)

Identifier: REQ-CM (97)	Rel. Use case id : RD – 4	Priority:
Title:		
Description: The CMS shall provide the capability to transfer this CCF (with the "basic" parameter set) to the EMS in accordance with the northbound interface specification of the EMS for Plug & Play configuration of the eNodeB.		
Rationale:		

The resulting requirements from Use Case Id: RD – 5:

REQ-CM (98)

Identifier: REQ-CM (98)	Rel. Use case id : RD – 5	Priority:
Title:		
Description: The CMS shall allow requesting an inventory upload (from the EMS). This upload contains: a) The resource inventory information for each installed eNodeB/ RAN & Core NE b) The configuration information for each installed eNodeB/ RAN & Core NE in near real-time respectively at dedicated intervals (<= 24h). The CMS shall be able to reconcile between planned data and uploaded data. Reconciliation		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

policy - defining who is master of the truth (Plan data or network data) - shall be configurable. The CMS shall allow to forward (to the inventory DBs): a) The resource inventory information for each installed eNodeB/ RAN & Core NE b) The configuration information for each installed eNodeB/ RAN & Core NE in near real-time respectively at dedicated intervals (<= 24h).
Rationale:

REQ-CM (99)

Identifier: REQ-CM (99)	**Rel. Use case id : RD – 5**	**Priority:**
Title:		
Description: The CMS shall have access to these parameter sets on the EMS on request (in accordance with the northbound interface specification of the EMS).		
Rationale:		

REQ-CM (100)

Identifier: REQ-CM (100)	**Rel. Use case id : RD – 5**	**Priority:**
Title:		
Description: The inventory information is exchanged via NBI/Itf-N using XML file transfer.		
Rationale:		

REQ-CM (101)

Identifier: REQ-CM (101)	**Rel. Use case id : RD – 5**	**Priority:**
Title:		
Description: An Automatic Inventory function located on the EMS shall support synchronisation in real time with the Service Provider's inventory systems through notifications.		
Rationale:		

6.5.4.3 … Core Network Deployment processes

left blank intentionally

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.5.4.4 … RAN Transmission (Backhaul) Deployment process

The resulting requirements from Use Case Id: TD-1:

REQ-CM (102)

Identifier: REQ-CM (102)	Rel. Use case id : TD-1	Priority:
Title:		
Description: The CMS shall allow the Configuration of the Access routers. This needs functionality to extract transport configuration data from the planning database and to generate & transfer the respective configuration file(s) to a (possibly integrated) Management Node that configures the AR automatically based on these received configuration files.		
Rationale:		

6.5.4.5 … Security Infrastructure Deployment processes

The resulting requirements from Use Case Id: SD-1:

REQ-CM (103)

Identifier: REQ-CM (103)	Rel. Use case id : SD-1	Priority:
Title:		
Description: The CMS has to provide new functionalities to fetch the keys from a Database or FTP Server and copy them into the PKI Server.		
Rationale:		

6.5.4.6 … RAN Optimization process

The resulting requirements from Use Case Id: OPT-1:

REQ-CM (104)

Identifier: REQ-CM (104)	Rel. Use case id : OPT-1	Priority:
Title:		
Description: The CMS shall allow maintaining and presenting via GUI a NR black list and a NR white list for each cell.		
Rationale:		

REQ-CM (105)

Identifier: REQ-CM (105)	Rel. Use case id : OPT-1	Priority:
Title:		
Description: The CMS shall allow ANR to be switched on or off. This should be in accordance with a standardized northbound interface specification of the respective element manager.		
Rationale:		

REQ-CM (106)

Identifier: REQ-CM (106)	Rel. Use case id : OPT-1	Priority:
Title:		
Description: The CMS shall provide the capability to populate the EMS with these NR lists (in accordance with the northbound interface specification of the network element manager).		
Rationale:		

The resulting requirements from Use Case Id: OPT-2:

REQ-CM (107)

Identifier: REQ-CM (107)	Rel. Use case id : OPT-2	Priority:
Title:		
Description: The CMS shall provide an upload functionality of Neighbour relationship lists from the EMS on request (change notification from eNodeB -> EMS -> CMS) in real-time or the CMS shall provide a bulk upload functionality for these Neighbour relationship lists from the network element manager (in accordance with the northbound interface specification of the network element manager).		
Rationale:		

REQ-CM (108)

Identifier: Fehler! Verweisquelle konnte nicht gefunden werden.	Rel. Use case id : OPT-2	Priority:
Title:		
Description: The CMS shall provide reconciliation functionality for these Neighbour relationship lists if ANR is switched off.		
Rationale:		

The resulting requirements from Use Case Id: OPT-3:

REQ-CM (109)

Identifier: REQ-CM (109)	Rel. Use case id : OPT-3	Priority:
Title:		
Description: The CMS shall provide the complete history of configuration data for eNodeBs for a timeframe of n months (where n is not less than 6). The relevant data details have to be identified and agreed. All details to be specified bilaterally.		
Rationale:		

REQ-CM (110)

Identifier: REQ-CM (110)	Rel. Use case id : OPT-3	Priority:
Title:		
Description: The CMS shall provide visibility of actual network configuration data via its GUI not later than 3 hours after a change of a configuration has happened.		
Rationale:		

REQ-CM (111)

Identifier: REQ-CM (111)	Rel. Use case id : OPT-3	Priority:
Title:		
Description: Enhanced analysis functions have to be provided by the CMS, for manual and automated, scheduled analysis.		
Rationale:		

6.5.4.7 … Change management & Provisioning and Activation processes

The resulting requirements from Use Case Id: ChM-1:

The operational cell specific parameter set and the generic cell parameter sets designed to model the characteristic of different types of cells (maintained by the Operator in several different templates) are aggregated into the NIF (Network Integration File) and are downloaded to the EMS.

REQ-CM (112)

Identifier: REQ-CM (112)	Rel. Use case id : ChM-1	Priority:
Title:		
Description: The CMS shall allow to access and retrieve these parameters from the planning database.		
Rationale:		

REQ-CM (113)

Identifier: REQ-CM (113)	Rel. Use case id : ChM-1	Priority:
Title:		
Description: The CMS shall be able to request an upload of the current configuration from the EMS (in accordance with the northbound interface specification of the network element manager),		
Rationale:		

REQ-CM (114)

Identifier: REQ-CM (114)	Rel. Use case id : ChM-1	Priority:
Title:		
Description: The CMS shall allow to generate the delta between current and planned configuration and		
Rationale:		

REQ-CM (115)

Identifier: REQ-CM (115)	Rel. Use case id : ChM-1	Priority:
Title:		
Description: The CMS shall allow to download the delta configuration information onto the EMS in accordance with the northbound interface specification of the EMS, for each installed eNodeB in real-time respectively at dedicated intervals (<= 24h).		
Rationale:		

The resulting requirements from Use Case Id: ChM-3:

REQ-CM (116)

Identifier: REQ-CM (116)	Rel. Use case id : ChM-3	Priority:
Title:		
Description: The CMS shall discover changes in the networks that are monitored by the Network Element Mgmt Services.		
Rationale:		

REQ-CM (117)

Identifier: REQ-CM (117)	Rel. Use case id : ChM-3	Priority:
Title:		
Description: The CMS shall discover changes in resource details, topology and configuration made to a network element.		
Rationale:		

REQ-CM (118)

Identifier: REQ-CM (118)	Rel. Use case id : ChM-3	Priority:
Title:		
Description: The discovery features shall be configurable in respect to: a) what type of information that the discovery feature shall cover b) how often the discovery feature shall interact with the EMS and the network elements.		
Rationale:		

The resulting requirements from Use Case Id: ChM-4:

REQ-CM (119)

Identifier: REQ-CM (119)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: The CMS shall be responsible for the identification of discrepancies between information in the NMS inventory and the EMS.		
Rationale:		

REQ-CM (120)

Identifier: REQ-CM (120)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: The CMS shall notify those user(s) held in a pre-defined distribution list if discrepancies between NMS inventory and network are detected.		
Rationale:		

REQ-CM (121)

Identifier: REQ-CM (121)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: The CMS shall be responsible to start the reconciliation of discrepancies between information in the NMS inventory and the EMS: a) manually b) automatically		
Rationale:		

REQ-CM (122)

Identifier: REQ-CM (122)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: The CMS shall support to apply rules and a set of criteria to decide if the information shall be manually or automatically reconciled: a) If automatically reconciliation; user can define the master (NMS inventory or network) – this means which database shall be updated. CMS shall initiate the required upload/download & activate. b) If manual reconciliation; user can define which users to notify about the required manual reconciliation. CMS shall do no further activities for reconciliation then.		
Rationale:		

REQ-CM (123)

Identifier: REQ-CM (123)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: The CMS shall notify user(s) about the outcome of the reconciliation, i.e., after inconsistent data are reconciled.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (124)

Identifier: REQ-CM (124)	Rel. Use case id : ChM-4	Priority:
Title:		
Description: EMS shall always notify CMS whether a download & activation (here: after delta generation based on the reconciliation) was successful or not.		
Rationale:		

6.5.4.8 … Configuration Management & Common Data Management processes

The resulting requirements from Use Case Id: CM-1:

REQ-CM (125)

Identifier: REQ-CM (125)	Rel. Use case id : CM-1	Priority:
Title:		
Description: Information required is to be stored as Configuration Items in a Configuration Management system (CMS). The CMS must link all relevant data sources consolidated into a Common Functional Architecture with an agreed harmonised, common data model. The categorization of information stored should be split into: Service Inventory, Resource Inventory, Configuration Inventory and policy Inventory.		
Rationale:		

REQ-CM (126)

Identifier: REQ-CM (126)	Rel. Use case id : CM-1	Priority:
Title:		
Description: The information stored must be labelled with which lifecycle state it is describing e.g. Planned, Active or Removed.		
Rationale:		

REQ-CM (127)

Identifier: REQ-CM (127)	Rel. Use case id : CM-1	Priority:
Title:		
Description: Standard interfaces for presenting information to Engineering/ Design systems, Planning and Deployment systems and Operations Event management and workflow systems must be provided.		
Rationale:		

The resulting requirements from Use Case Id: CM-2:

REQ-CM (128)

Identifier: REQ-CM (128)	Rel. Use case id : CM-2	Priority:
Title:		
Description: The CMS shall deliver the capability to manage all required configuration data centrally. The location of the data must not be a constraint.		
Rationale:		

REQ-CM (129)

Identifier: REQ-CM (129)	Rel. Use case id : CM-2	Priority:
Title:		
Description: The CMS shall deliver the capability to report on what configurations where used (downloaded and activated) when and where at a given point in time.		
Rationale:		

REQ-CM (130)

Identifier: REQ-CM (130)	Rel. Use case id : CM-2	Priority:
Title:		
Description: The CMS shall deliver the capability to correlate this data with workflow tickets for IM, CM, ChM, PM and Planning/ Deployment.		
Rationale:		

The resulting requirements from Use Case Id: CM-3:

The CMS has to support the creation, modification, removal, evaluation and acceptance of templates and sources of Master Data for CIs in the Configuration Management System.

REQ-CM (131)

Identifier: REQ-CM (131)	Rel. Use case id : CM-3	Priority:
Title:		
Description: The CMS should have abilities to create and store templates for all resources and network elements that are represented in the system. These templates (specifications) shall define information and configuration details.		
Rationale:		

REQ-CM (132)

Identifier: REQ-CM (132)	Rel. Use case id : CM-3	Priority:
Title:		
Description: The CMS should provide functionality for creating and storing specialisations of an existing design template. These specialisations shall be available to a particular user or user group.		
Rationale:		

REQ-CM (133)

Identifier: REQ-CM (133)	Rel. Use case id : CM-3	Priority:
Title:		
Description: For each design template the CMS shall allow users to define resource and network element specific: a) Parameters b) Allowed parameter values or range of values.		
Rationale:		

REQ-CM (134)

Identifier: REQ-CM (134)	Rel. Use case id : CM-3	Priority:
Title:		
Description: Auto-generation of values: Design templates stored in the CMS shall have support for parameters that automatically are given a value from a number specified range.		
Rationale:		

REQ-CM (135)

Identifier: REQ-CM (135)	Rel. Use case id : CM-3	Priority:
Title:		
Description: The CMS should provide functionality for modifying and deleting design templates that are in the CMS: a) Copy and rename design template b) Delete design template c) Add, change and delete parameters and parameter values to the design template.		
Rationale:		

REQ-CM (136)

Identifier: REQ-CM (136)	Rel. Use case id : CM-3	Priority:
Title:		
Description: The CMS shall be able to separate between design templates in production and those that are drafts and		

thus only available to a particular user group.
Rationale:

The resulting requirements from Use Case Id: CM-4:

REQ-CM (137)

Identifier: REQ-CM (137)	**Rel. Use case id : CM-4**	**Priority:**
Title:		
Description: Ensure that only authorized and identifiable CI s are accepted and recorded, from receipt to disposal. It ensures that no CI is created, modified, or removed without appropriate controlling documentation.		
Rationale:		

REQ-CM (138)

Identifier: REQ-CM (138)	**Rel. Use case id : CM-4**	**Priority:**
Title:		
Description: All requirements for automatic inventory (SON Feature 2.2) must be addressed with this requirement. Automatic updates of inventory must be performed in a controlled way in the responsibility of the Data Owner.		
Rationale:		

REQ-CM (139)

Identifier: REQ-CM (139)	**Rel. Use case id : CM-4**	**Priority:**
Title:		
Description: Support by the CMS (and workflow solutions) for Configuration control from the initial creation of CIs (LC state Planned), through operational implementation (LC state Planned), and removal (LC state removed).		
Rationale:		

REQ-CM (140)

Identifier: REQ-CM (140)	**Rel. Use case id : CM-4**	**Priority:**
Title:		
Description: The CMS solution must support auto-discovery for reconciliation between the documented state of the CIs in question and real life status of Network elements to enable the automatic update of CIs in the Inventory.		
Rationale:		

REQ-CM (141)

Identifier: REQ-CM (141)	Rel. Use case id : CM-4	Priority:
Title:		
Description: The CMS solution must support the SON functionality Automatic inventory by enabling an audit trail of changes, confirmation of automatic updates by the data owners, and correlation of automatic updates with Changes performed with Change Management.		
Rationale:		

REQ-CM (142)

Identifier: REQ-CM (142)	Rel. Use case id : CM-4	Priority:
Title:		
Description: The automatic update solution must support the manual confirmation of the data owners indicating that the update can be performed.		
Rationale:		

The resulting requirements from Use Case Id: CM-5:

REQ-CM (143)

Identifier: REQ-CM (143)	Rel. Use case id : CM-5	Priority:
Title:		
Description: Modifications to CI s and their records have to be traceable.		
Rationale:		

REQ-CM (144)

Identifier: REQ-CM (144)	Rel. Use case id : CM-5	Priority:
Title:		
Description: Support from the CMS solution to provide a unique CI-ID across the whole organisation to enable reporting of all current and historical data concerned with each CI throughout its life cycle.		
Rationale:		

REQ-CM (145)

Identifier: REQ-CM (145)	Rel. Use case id : CM-5	Priority:
Title:		
Description: The Requests for Reporting capabilities must be supported by a Workflow component.		
Rationale:		

REQ-CM (146)

Identifier: REQ-CM (146)	Rel. Use case id : CM-5	Priority:
Title:		
Description: The reporting of metrics to contribute to Key Performance Indicators for the process must be supported by the CMS and Workflow components.		
Rationale:		

REQ-CM (147)

Identifier: REQ-CM (147)	Rel. Use case id : CM-5	Priority:
Title:		
Description: The capability for correlation of information between the audit trail of RFCs (from Change Management, Incidents and Problems from the Operations workflow system(s)), and the audit trail in the inventory systems must be possible.		
Rationale:		

The resulting requirements from Use Case Id: CM-6:

REQ-CM (148)

Identifier: REQ-CM (148)	Rel. Use case id : CM-6	Priority:
Title:		
Description: Capability for logical audits between the CMS and real life configurations.		
Rationale:		

REQ-CM (149)

Identifier: REQ-CM (149)	Rel. Use case id : CM-6	Priority:
Title:		
Description: Capability to tag CIs with a last audit date for physical (live looking physically at the equipment) or logical audits (discovery) between the CMS and real life configurations.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

The resulting requirements from Use Case Id: CM-7:

REQ-CM (150)

Identifier: REQ-CM (150)	Rel. Use case id : CM-7	Priority:
Title:		
Description: All changes resulting from SELF-x - that have to be reported via notifications from the EMS - are tracked automatically, are auditable, and reportable at all times.		
Rationale:		

6.5.5 Reduced Parameter handling efforts for the eNodeB configuration

More than 80% of a cellular network's equipment and operating costs are associated with the Radio Access Network - the base station product costs and the deployment, operation and optimisation expenses.

An enormous amount of thought and design has gone into making LTE easily to rollout and manage from a radio planning perspective. However, LTE will co-exist with 2G/ 3G systems for many years to come - at least a decade if not longer.

With LTE, operators will need to match radio parameters including neighbour lists between three different systems. There will be a need for additional cross checking, and design rules including handover policy across the different network technologies and frequency bands. The careful management of these rules and resulting radio parameters will be required to achieve optimal performance and end-user experience. This involves staging the parameters generated by Radio planning tools and downloading them to the various vendors systems in a controlled manner.

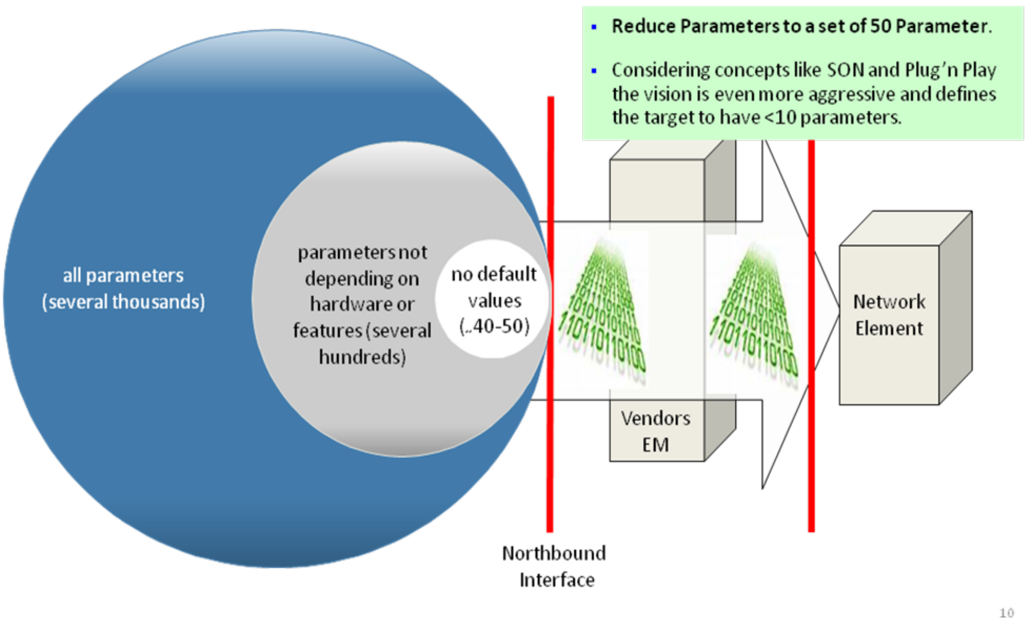


Figure 6.5-10: Parameter reduction – status and target vision

And there are not some but thousands of parameters that drive the GSM/ UMTS/ LTE network service quality. This huge number of parameters complicates the deployment and optimisation task. So operators usually start at the beginning of the site roll-out by implementing standard templates of reduced parameter sets and then apply fine-tunings to specific sites/ areas. The declared goal in this situation is a reduction of parameters that planning and configuration engineers have to touch.

Thus the requirements enabling to focus on the configuration of the essential parameters so that

- a minimum number of parameter must be set by the operator and
- all other parameters are managed by the system transparently

have to be explored in detail. This can be achieved by identifying those parameters from an operator's perspective and by automating the parameter handling via template mechanisms. It is important to understand first the parameter classification and the algorithms they are involved in and afterwards to deal with their handling.

6.5.5.1 Configuration parameters and their use during commissioning and optimization

6.5.5.1.1 Methodology / Procedure

It's observable practice that changes and new deployments in the topology and the configuration of a SP's radio access network are implemented following a methodology / procedure that is organizing the work in a number of time slices (usually 8 to 12 or more) per year and that is adopting a life cycle model like the one in Figure 6.5-11: Lifecycle states – from X.731.

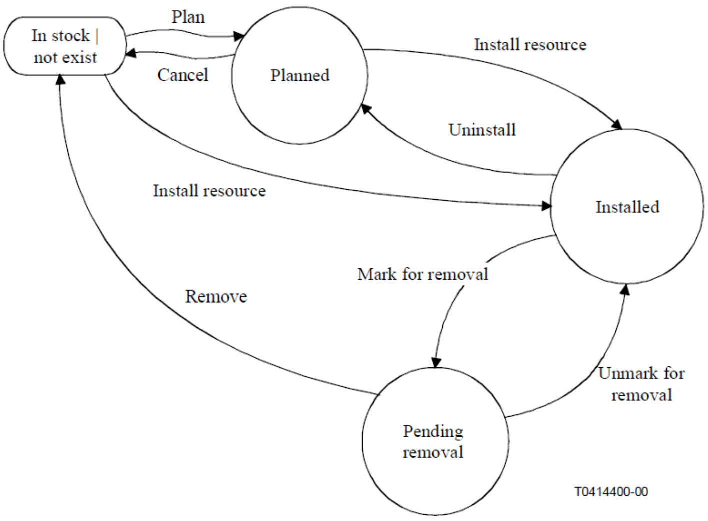


Figure 6.5-11: Lifecycle states – from X.731

A new deployment of an eNodeB – running through the NE-states planned to installed up to a sub-state commercial – needs the steps shown in Figure 6.5-12: Configuration deployment during the lifecycle states of a NE.

To commission BTSs/ NodeBs and eNodeBs a Commissioning Configuration File (CCF) has to be created and implemented in these network nodes.

To profit from the full benefits of SON, the CCF has to be automatically created and transferred to the eNodeB's EMS' for later SON enabled self configuration (also called Plug & Play) [see: 3GPP SA5 draft S5-11papl - Full multi-vendor Plug and Play].

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

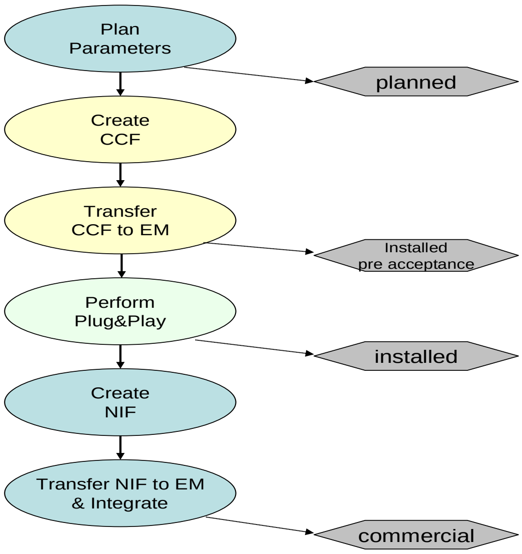


Figure 6.5-12: Configuration deployment during the lifecycle states of a NE

Following this procedure the planning department provides all Planning-Data for month *n* at a defined day of month *n-1* as export or report from their planning database or the planned part of a configuration inventory. Let's call this set PDS-RAN (**Pl**an **D**ata **S**et **RAN**). Data in such a PDS-RAN describe activities to be performed and are:

1. Hardware- & topology related data
    a. Information about new deployments
    b. Hardware changes
    c. Transport related information
2. Configuration-data
    a. Configuration-data for RAN NEs with only cell "dummy" data
    b. Transport related configuration-data for Access Router (AR)
    c. Configuration-data for DHCP Server, PKI Server and IPSec Gateway

The PDS-RAN is placed anywhere in the OSS architecture with respective access rights for all involved process parties. Often workflow tickets are issued by the planning department as trigger for the configuration team to start the work for the respective time slice.

After successful installation and commissioning of the network element with a reduced - better a minimal - parameter set in the CCF, an eNodeB is finally set up with additional cell specific parameters to enable its commercial use. Cell specific configuration data are provided by the planning department (deployment) resp. an optimisation team (changes from optimisation).

These parameters are grouped together in a NIF (Network Integration File), provided to its EMS via download and pushed to the eNodeB by the EMS (this is called network integration). Configuration management tools are used to generate the NIF and download it to the EM.

Data in such a NIF are:

3. Cell specific configuration-data
    a. Cell specific Configuration-data e.g. neighbour relationships,
    b. others

6.5.5.1.2 Parameter Sets

The complete set of configuration data for an eNodeB - some being relevant during installation and commissioning and others being relevant during the network integration - is built from five groups or subsets of parameters:

1. Site specific eNodeB parameters
   like NodeID, IP addresses, VLAN addresses, cells and their id's etc.

2. Cell parameters
   like frequencies, scrambling codes, neighbour cell relations etc.
   a. As dummy cell parameter set (used during commissioning)
   b. As operational cell parameter set (valid during the commercial phase of an eNodeB)

3. Generic radio parameters
   a. Standard cell parameter set (used during commissioning organized as a template) having a generic, net wide nature and underlying a change from time to time
   b. Generic cell parameter sets designed to model the characteristic of different types of cells maintained also in several, different templates

4. Transport parameters
   SP specific transport parameters having a generic, net wide nature and underlying a change from time to time

5. Vendor specific parameters
   Vendor specific parameters that are not touched by the SP but needed by the vendors' technology and which are subject to change during release upgrades

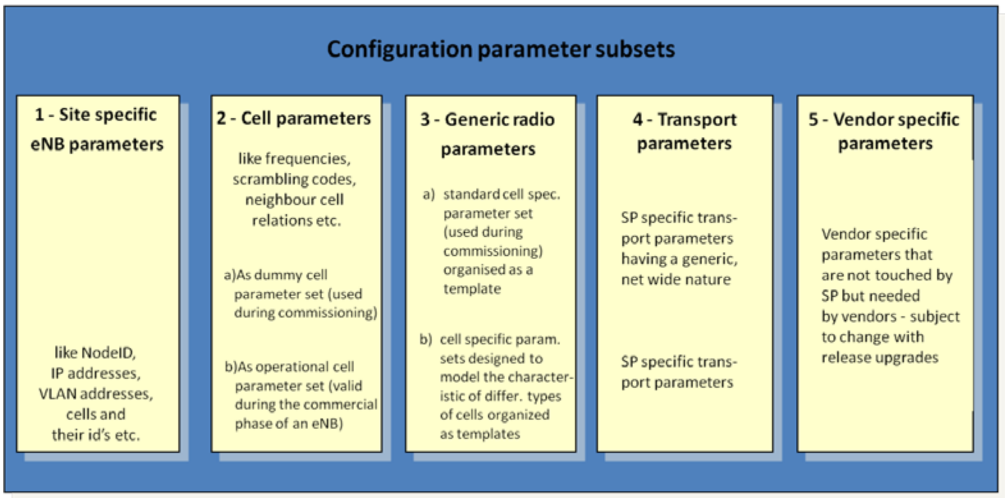


Figure 6.5-13: eNodeB configuration parameter sets

During installation and commissioning an eNodeB has to be configured in some of the above mentioned aspects. For that a number of parameter values have to be planned. These basic parameters are grouped together in the CCF and transferred to its EMS for later SON enabled Plug & Play configuration.

The CCF incorporates at minimum the parameter subsets 1, 2a, 3a, 4 and 5.

For 2G and 3G, where today the SP delivers parameters covering subset 1 (from the above list) in the PDS for such new deployments to the respective vendor or installation service provider, CCF generation and transfer onto the EMS is in most cases in the vendor's or installation service provider's responsibility.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

With the introduction of SON/ LTE this CCF has to be generated by the SP and transferred onto the respective EM. The mechanisms needed are more or less the same than those already implemented for the generation and integration of the 2G/ 3G network integration file.

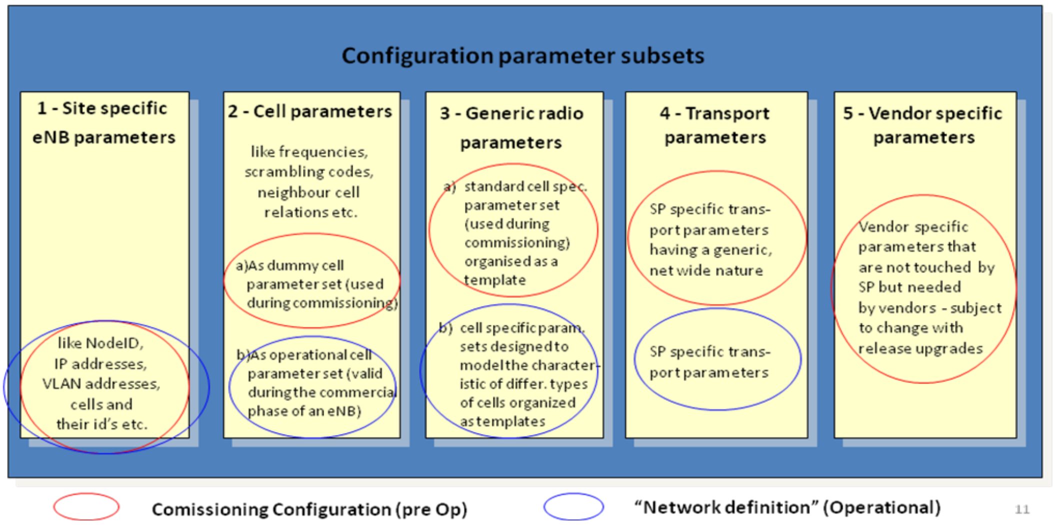


Figure 6.5-14: eNodeB configuration parameter sets and their relation to CCF and NIF

During the further life cycle phase commercial/operational the same mechanism (the integration of a NIF) is used 6 - 12 times a year to map network expansion and optimisation results, elaborated by the Optimisation team, into the real network. So the NIF incorporates the parameter subsets 2b and 3b.

6.5.5.2 Guiding Use Cases

The motivation of this chapter is to give typical operator use cases as examples how template management could simplify configuration management to hide complexity and vendor specific parameters in templates and give operator opportunity to manage templates in a standardized way in a multi-vendor system.

Identifier: Initial Commissioning of a Radio base station	**Use Case Id: OPT - 3a**
Originating Process : Radio Planning	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB is physically installed and all physical connectors are plugged in. It has an IP Address assigned and intends to retrieved its configuration data / parameter set via an end-to-end connections to the network element manager.	
Scenario description: Input: a) BTS individual planning parameter as BTS ID, essential planning parameter as type, used frequency resources, others (less than 20 parameters) b) A lot of additional parameters (could be handled via templates: so also a input for the described algorithm are paramters in templates) including e.g. proprietary vendor specific parameter, parameter which can be handled as operator default generic ones for the complete network. Output: proprietary BTS specific configuration of a single infrastructure vendor Algorithm: apply vendor specific rules for the generation of specific parameter if config file is based on planning parameters (e.g. planning value for number of sectors is equal 3: this leads to configure 3 sector objects with all related detailed	

parameter describing a sector) apply vendor specific object structure of config file considering all parameter which are mandatory to be set based planning parameter based on given operator default values **(could be handled by templates)** based on given vendor default values **(could be handled by templates)**
The resulting requirements: See following section
Justification (Business benefits/ Impact if not Implemented): **With templates:** ▪ A lot of additional parameters can be handled via templates: so also a input for the described algorithm are parameters in template including e.g. proprietary vendor specific parameter, parameter which can be handled as default generic ones for complete network. The appropriate templates could be optionally defined and handled via NBI to give operator best control. ▪ On NBI level not all single parameter are handled but only one template -> reduced number of parameters to be touched and send via NBI ▪ High abstraction level simplifies daily live work
Miscellaneous Comments/ Useful hints: ▪ Periodicity: one time for a single BTS; concurrent configuration of only few BTS ▪ Time need: short (minutes)

Required timeline (link to roadmap)/ Priority:	**Requirement Owner / Date (MM-DD-YYYY):**
1	NGMN NGCOR/ fl

Identifier: Update of individual parameter set in the complete network	**Use Case Id: OPT- 3b**
Originating Process : Change Management	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB is up, connection to neighbouring eNodeBs, to EMS and MME/SGW established. A prior configuration for commercial use of the eNodeB has been successfully performed.	
Scenario description: ▪ Input: for BTS individual parameter: set of individual parameters and their individual values given e.g. by a planning tool ▪ Output: the defined parameter are changed to the individual or default value ▪ Algorithm: configure downwards the individual parameter values according to input for every BTS in the network	
The resulting requirements: See following section	
Justification (Business benefits/ Impact if not Implemented):	
Miscellaneous Comments/ Useful hints: ▪ Periodicity: few times in a year ▪ Time need: must be restricted on low traffic period (night time) Usage of templates for these individual parameters doesn't make sense	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ fl

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Identifier: Update of generic parameter set in the complete network	**Use Case Id: OPT - 3c**
Originating Process : Change Management	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB(s) is/are up, connection to neighbouring eNodeBs, to EMS and MME/SGW established. A prior configuration for commercial use of the eNodeB has been successfully performed.	
Scenario description: ▪ Input: for generic default parameter: new template version with changed "new" parameter value for this parameter which must be updated ▪ Output: the defined parameter are changed to the individual or default value ▪ Algorithm: **via template handling:** ▪ new template is downloaded into EMS via NBI: ▪ EMS organizes delta comparison with old template version and triggers configuration of those parameters to be changed	
The resulting requirements: See following section	
Justification (Business benefits/ Impact if not Implemented): ▪ On NBI level not all single parameter are handled but only one template -> reduced number of parameters to be touched and send via NBI ▪ High abstraction level simplifies daily live work	
Miscellaneous Comments/ Useful hints: ▪ Periodicity: few times in a year ▪ Time need: must be restricted on low traffic period (night time)	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ fl

Identifier: Update of a parameter set in a network cluster	**Use Case Id: OPT - 3d**
Originating Process : Change Management	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB(s) is/are up, connection to neighbouring eNodeBs, to EMS and MME/SGW established. A prior configuration for commercial use of the eNodeB has been successfully performed.	
Scenario description: ▪ Input: 1) for BTS individual parameter: set of individual parameters and their individual values given e.g. by a planning tool 2) for generic default parameter: new template version with changed "new" parameter value for this parameter which must be updated ▪ Output: the defined parameter has been changed to the individual or default value ▪ Algorithm: 1) configure downwards the individual parameter values according to input for every BTS in the network 2) via **template handling**: new template is downloaded into NEM via NBI: NEM organize delta comparison with old template version and triggers configuration for to be changed parameters	
The resulting requirements: See following section	
Justification (Business benefits/ Impact if not Implemented): ▪ On NBI level not all single parameter are handled but only one template -> reduced number of parameters	

to be touched and send via NBI ▪ High abstraction level simplifies daily live work	
Miscellaneous Comments/ Useful hints: ▪ Periodicity: few times in a year ▪ Time need: must be restricted on low traffic period (night time)	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Delta Check & Update for a parameter set in a network cluster	**Use Case Id: OPT - 3e**
Originating Process : Change Management	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB(s) is/are up, connection to neighbouring eNodeBs, to EMS and MME/SGW established. A prior configuration for commercial use of the eNodeB has been successfully performed.	
Scenario description: ▪ Input: 1) set of parameter and their new default values 2) for generic default parameter: new template version with changed "new" parameter value for this parameter which must be updated ▪ Output: the defined parameter has been changed to the individual or default value ▪ Algorithm: 1) Option 1 ▪ get current value of all BTS in the network ▪ compare "is-value" with given default value ▪ if a delta is identified the parameter values according to input is configured 2) Option 2 with **template handling** ▪ new template is downloaded into EMS via NBI ▪ EMS organize delta comparison with old template version and triggers configuration of those parameters to be changed	
The resulting requirements: See following section	
Justification (Business benefits/ Impact if not Implemented): ▪ On NBI level not all single parameter are handled but only one template -> reduced number of parameters to be touched and send via NBI ▪ High abstraction level simplifies daily live work	
Miscellaneous Comments/ Useful hints: ▪ Periodicity: few times in a year ▪ Time need: must be restricted on low traffic period (night time)	
Required timeline (link to roadmap)/ Priority: 1	**Requirement Owner / Date (MM-DD-YYYY):** NGMN NGCOR/ mm

Identifier: Configure feature specific parameter set	**Use Case Id: OPT - 3f**
Originating Process : Change Management	**Actor role:** Radio Planner
Precondition(s) and Dependencies: The eNodeB(s) is/are up, connection to neighbouring eNodeBs, to EMS and MME/SGW established. A prior configuration for commercial use of the eNodeB has been successfully performed.	
Scenario description: Define a so called feature template which covers the full parameter set to control certain functionality.	

Example: Intra-frequency LTE Handover: there is a collection of parameter controlling this as among others HO Offset value, thresholds for triggering event measurements etc. All these parameter are in one template. Typically this template is given by vendor to operator. Operator can create then special template versions with adapted parameter values. ▪ Input: See TM-1 ▪ Output: the defined parameter has been changed to the individual or default value ▪ Algorithm: See TM-1
The resulting requirements: See following section
Justification (Business benefits/ Impact if not Implemented): ▪ On NBI level not all single parameter are handled but only one template -> reduced number of parameters to be touched and send via NBI ▪ High abstraction level simplifies daily live work ▪ Parameters for influencing functionality are not spread over a lot of places in the object model but concentrated into one template
Miscellaneous Comments/ Useful hints: Update works with adapted algorithm as described in the use cases before. Some BST individual parameter values must be chosen (e.g. for the handover the HO cell individual offset is not generic in a network). So beside the template also some parameters must be handled as a specific individual value. The administration to handle real generic parameter which is the same in complete network and individual ones might lead to more implementation efforts. One solution to avoid such implementation efforts could be that the feature template is flexible to be defined: if a parameter needs individual treatment it is handled outside of the template. More clever concepts would make it possible that via template a first default value can be set but later on the parameter can be overwritten and handled in an individual way. ▪ Periodicity: few times in a year ▪ Time need: must be restricted on low traffic period (night time)

Required timeline (link to roadmap)/ Priority:	**Requirement Owner / Date (MM-DD-YYYY):**
1	NGMN NGCOR/ mm

6.5.5.3 Template Management and Requirements

As requested before the EMS offers via the NBI the capability to NMS components to create, read, update and delete instances of IOCs/ MOCs and update Parameter values per ME type.

To avoid the need for manually defining values for all mandatory parameters - a time consuming, error prone and thus expensive procedure that really isn't intellectually challenging - a template mechanism is proposed.

Templates allow to define a collection of parameter values for a particular managed object class and later to use these predefined value sets instead of typing them in manually. Templates can be assigned both for new planned (to be created) and existing actually managed objects.

We differentiate two types of templates:

- Equipment provider templates or “Base templates”

  There is a **single** equipment provider template supporting the latest network element version for each managed object class. The equipment provider template values are defined according to the latest release of the network element. **Versioning** of templates has to be **supported** in equipment provider templates (different versions in production). These templates are provided by the equipment provider as part of EMS and they cannot be edited by users.

- Service provider templates or “Operator templates”

  Multiple service provider templates can exist for a single managed object class or there can be none. A service provider template should contain values that differ from the equipment provider template as the equipment provider template is always automatically used before the service provider template to provide all missing values.

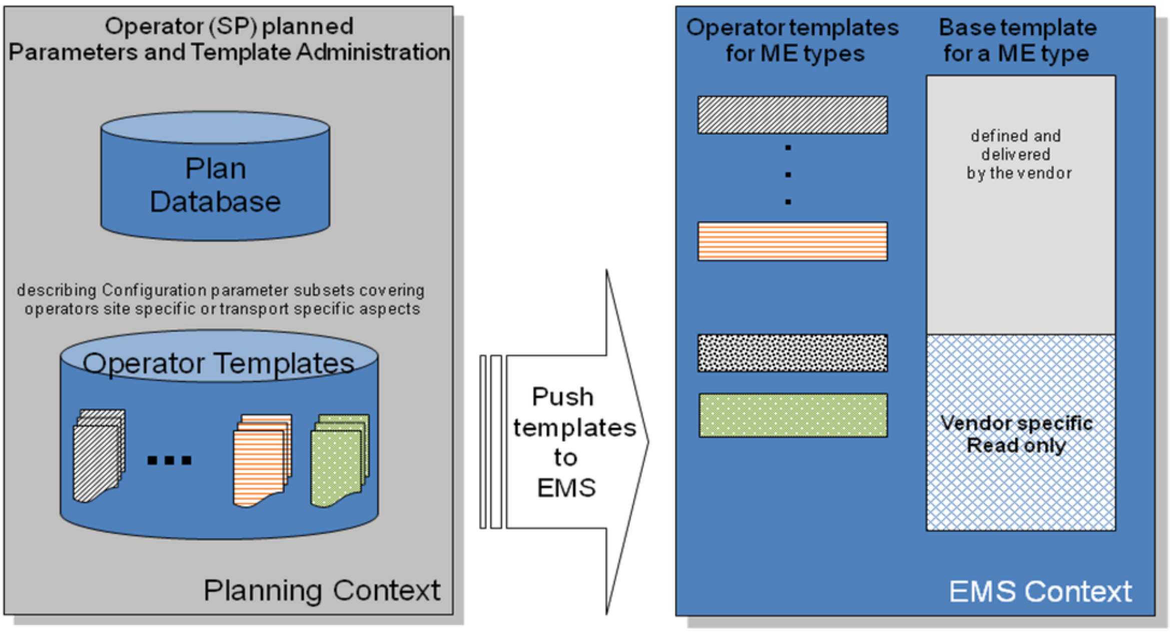


Figure 6.5-15: Parameter Template definition and administration

For the administration of service provider templates the following applies:

- Service provider templates are created and modified in the NMS/OSS layer.
- New service provider templates can be defined and imported into the EMS via a standard NBI function.
- Only service provider templates can be modified and imported by the user into the EMS via a standard NBI function.
- Service provider templates that are not used in actual configurations but have been imported into the EMS via a standard NBI function can be deleted.
- Deletion or renaming of a service provider template is only possible if this template is not assigned to any managed object in the actual configuration.

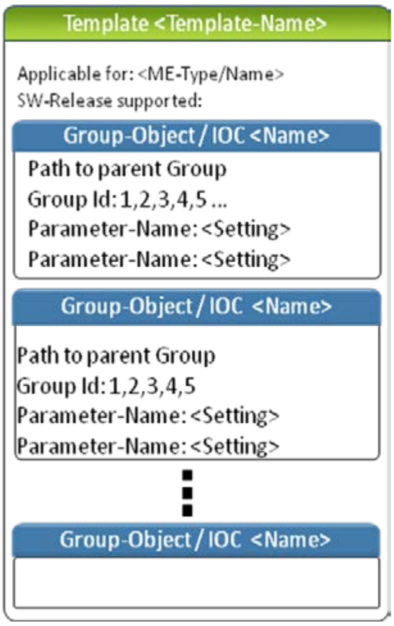


Figure 6.5-16: Parameter Template structure

The detailed requirements for the template management:

REQ-CM (151)

Identifier: REQ-CM (151)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Templates are defined as a collection of parameter values - a subset - for a set of particular managed object classes belonging to a dedicated ME type - thus a template is always related to exactly one ME type.		
Rationale:		

REQ-CM (152)

Identifier: REQ-CM (152)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: There are two types of templates: “operator templates” (defined by the operator/ service provider) and “base templates” (equipment provider defined) per ME type.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (153)

Identifier: REQ-CM (153)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: A base template is the complete set of parameter default values for a ME type covering standardised (if any) and vendor specific parameters – it is provided by the vendor.		
Rationale:		

REQ-CM (154)

Identifier: REQ-CM (154)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Attribute / Parameter values that are determined or calculated based on dependencies from other parameter values that might have no default shall not be part of a base template. However the dependencies have to be described in the model (see Interface Information and Documentation Requirements).		
Rationale:		

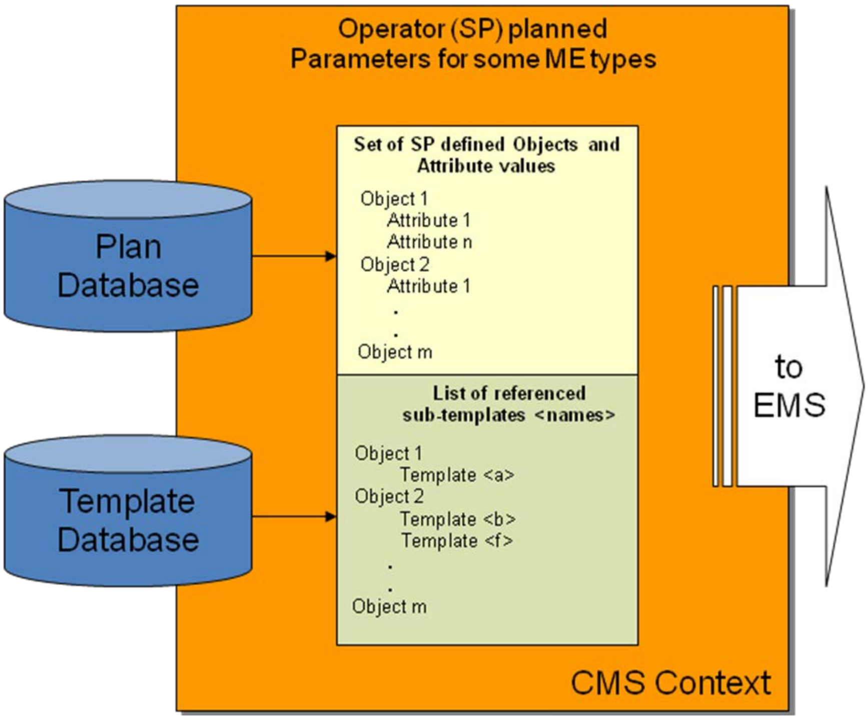
REQ-CM (155)

Identifier: REQ-CM (155)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: "Operator templates" are primarily used to define a parameter set (or subset) and its operator specific default values for one or multiple managed object(s) instances – they will be created and administrated by the operator.		
Rationale:		

REQ-CM (156)

Identifier: REQ-CM (156)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: One or several "operator templates" containing different, overlapping or identical parameter sets with partly or completely different parameter values can be assigned to a managed element (depending on its life cycle state) to define all or part of its parameter values/attribute values.		
Rationale:		

REQ-CM (157)

Identifier: REQ-CM (157)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: It is feasible that one or multiple "operator templates" are used to represent the complete or only a partial set of parameter values for a particular managed element.  **Figure 6.5-17: Template management mechanisms – template references in the configuration download data**		
Rationale:		

REQ-CM (158)

Identifier: REQ-CM (158)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The EMS offers via the NBI the capability to create, read, update, delete and request a directory of existing operator templates per ME type. There shall be two types of standard protocols via the NBI that allow the CMS to read/write the template database held by the EMS. One type is file based. The other is the synchronised type allowing the CMS to read/write only some specific object attribute values of a template.		
Rationale:		

REQ-CM (159)

Identifier: REQ-CM (159)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The CMS is responsible to manage the consistency of operator templates on the NM layer with those created in the EM layer and thus has to recognize and resolve discrepancies if any. If the CMS decides that the EMS's template database is required to be modified in order to synchronize databases for consistency reasons and the required modification is not 'big', CMS can use a synchronous-type of write onto EMS's database. CMS is not obliged to use a file based download in case the EMS supports both types of standard protocol.		
Rationale:		

REQ-CM (160)

Identifier: REQ-CM (160)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title: Impact of "Operator Template" modifications onto instantiated NEs.		
Description: The EMS shall have a log of those templates that had been applied in a NE configuration. After a template modification the EMS shall check all the impacted NEs (for their configuration the template was used) whether the respective parameter(s) is configured as in the modified "Operator Template". If not the EMS could set it to the new value. The latter decision by the EMS potentially has to be supported by a policy mechanism. This gives an idea how "Operator Templates" could also touch instantiated NEs. There is more detailed discussion on that needed.		
Rationale:		

REQ-CM (161)

Identifier: REQ-CM (161)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: "Base templates" are preinstalled on the EMS. The Base template defines a full set of parameters needed by the EMS and NE in order to create an NE instance of that ME type. This means that the range of Base templates in an EMS defines the set of NE types that can be instantiated. Each NE type has a specified set of parameters that could be set over NBI or through Operator Templates . A certain NE hardware type might support more than one NE type (in the case of generic hardware). In this case there might be need for EMS functionality by which the operator can tailor the basic NE product flexibility by defining intended NE types through their Base templates.		
Rationale:		

REQ-CM (162)

Identifier: REQ-CM (162)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: “Base templates” in the EMS cannot be changed via the NBI.		
Rationale:		

REQ-CM (163)

Identifier: REQ-CM (163)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Configuration data for MEs is delivered as “Download-file” from the CMS to the EMS via the NBI with download and activate requests (see example 3gpp IRP).		
Rationale:		

REQ-CM (164)

Identifier: REQ-CM (164)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: This “Download-file” contains a set of object creation/deletion requests plus a set of “Parameter values” per ME plus optional a list of references to “Operator templates” per ME.		
Rationale:		

REQ-CM (165)

Identifier: REQ-CM (165)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: References to “Operator templates” in the Download-file are given as name following a naming mechanism.		
Rationale:		

REQ-CM (166)

Identifier: REQ-CM (166)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The EMS has - for a particular managed element - the capability to merge: o a set of Operator-/SP-defined Parameter values (received via NBI), o the values from referenced “Operator templates” (residing in the EMS after former creation) and o the values in the ”Base-template” (in this order of decreasing precedence) resulting in a “complete” collection of parameter values for a particular managed element. Mandatory values not provided in a download file on the NBI can such be taken from the “Base template”.		

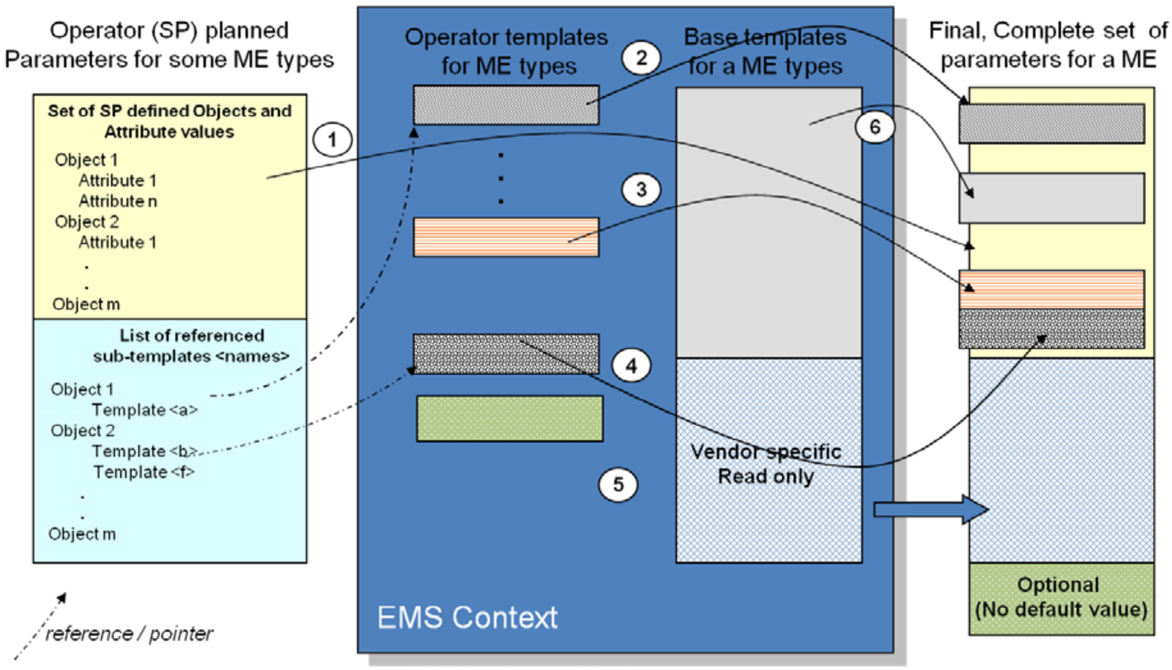


Figure 6.5-18: Template management mechanisms – EMS generation of the configuration data via merge

Rationale:

REQ-CM (167)

Identifier: REQ-CM (167)	**Rel. Use case id : OPT-3a to OPT-3f**	**Priority:**
Title:		
Description: If the same attribute is assigned a value from more than one “Operator template” in a downloaded configuration file, a mechanism has to be provided to define the precedence of templates such that the EMS gets instructed on the ordered sequence of template input into the of merge process.		
Rationale:		

REQ-CM (168)

Identifier: REQ-CM (168)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The configuration via the northbound interface shall be transparent regarding hardware. (Background: All HW-specific parameters we see today as e.g. - That a configuration must be done to indicate the pure existence of a HW unit or - Configuration of HW dependent details (as e.g. a HW port in a rack) HAVE NOT to be explicitly configured but can only be read. Parameters which influence the functionality of a HW unit of course have to be configurable.)		
Rationale:		

REQ-CM (169)

Identifier: REQ-CM (169)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Parameters in "Operator Templates" shall be HW-independent. Only parameters influencing functionality and behaviour of the system shall be content of templates visible for the operator.		
Rationale:		

REQ-CM (170)

Identifier: REQ-CM (170)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The EMS has the capability to evaluate whether a collection of parameter values for a ME merged from the sources referred to in REQ-CM (166) plus its actual configuration attribute values is complete – covers all configuration information for the respective ME.		
Rationale:		

REQ-CM (171)

Identifier: REQ-CM (171)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The EMS has the capability to evaluate whether a collection of parameter values for a ME merged from the sources referred to in REQ-CM (166) plus its actual configuration attribute values fits to the installed type and HW topology of the ME and behaves like follows: a) If this collection doesn't fit and the ME is in the state "configuration previously successfully activated" then the collection of parameters for that ME is rejected/ ignored and a notification is generated. b) If this collection doesn't fit and the ME is in the state "no configuration previously activated" then those parameters for that ME are activated that enable a remote management via the O&M link and a notification is generated.		
Rationale:		

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

REQ-CM (172)

Identifier: REQ-CM (172)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The CMS has the capability to evaluate whether an uploaded collection of parameter values for a ME/ MO still complies with the operator-template's values as they are stored on the EMS that had been referenced in the latest download.		
Rationale:		

REQ-CM (173)

Identifier: REQ-CM (173)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: The CMS has the capability to deliver on demand the delta - if any - if an uploaded collection of parameter values for a ME/ MO does not comply with the values in the operator-templates as they are stored on the EMS that had been referenced in the latest download.		
Rationale:		

REQ-CM (174)

Identifier: REQ-CM (174)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Versioning - there is a set of "base templates" supporting the latest n network element interface releases (version of the information model on the interface) for each managed object type. Each "Base template's" values are defined according to the respective releases of the network element interface.		
Rationale:		

REQ-CM (175)

Identifier: REQ-CM (175)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Versioning - "Operator templates" indicate via an attribute "SW version supported" which one of the latest n interface releases (version of the information model on the interface) of the network element type they are valid for. Each operator template's parameters and their values are defined according to the respective release of the network element. [This means that all templates have to be touched with every release upgrade – but it enables consistency checks in an early phase]		
Rationale:		

REQ-CM (176)

Identifier: REQ-CM (176)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: Synchronisation of EMSs – In a multi EMS environment the CMS shall have the capability to take the role of a “distribution manager” for templates.		
Rationale:		

REQ-CM (177)

Identifier: REQ-CM (177)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: An EMS offers the capability to subscribe to template changes to a “distribution manager”. - it is playing the role of a “distribution agent”.		
Rationale:		

REQ-CM (178)

Identifier: REQ-CM (178)	Rel. Use case id : OPT-3a to OPT-3f	Priority:
Title:		
Description: A CMS playing the role of a “distribution manager” takes the responsibility to distribute templates, to the subscribed “distribution agents”.		
Rationale:		

6.5.5.4 Template Management solution sets

The requirements are described from a perspective that is characterized by the assumptions:

- All operator templates are defined and administrated on the NM layer by a CMS.
- The EMS’s north bound interface or Itf-N knows templates and enables operator templates to be created, updated & deleted on the EMs under CMS control.
- Templates and merge mechanism reside on the EMs layer - EMS generates the final parameter value set through a merger of templates and explicitly SP defined parameter values.
- “Template management” is distributed on the NM and the EM layer.

An implementation of these requirements constitutes a solution with solution profile A.

A solution profile B characterized by

- The EMS’s north bound interface or Itf-N doesn’t know templates.
- Templates and merge mechanism reside on the NM layer – a CMS generates the final parameter value set through a merger of templates and explicitly operator defined parameter values.
- “Template management” functionality resides solely on the NM layer.

would also fulfill the requirements but implies a much bigger number of implementations of these functionalities in the OSS on the NM layer.

6.5.6 CM interfaces to resource inventory / discovery / reconciliation

Requirements for CM interfaces to resource inventory / discovery / reconciliation have been analyzed during phase I of the NGCOR project and are detailed in Chapter 6.6.2 Architecture Scenario: Resource Inventory Management Support for Resource Configuration of NGCOR I – see [2] NGMN Alliance - NGCOR Consolidated Requirements Phase I, Version 1.3, April 16, 2012

6.5.7 CM requirements evolving from RAN sharing scenarios

Requirements for the CM Context of RAN sharing scenarios, the requirements Req-NS (5) to Req-NS (16) are exposed in chapter Converged Operations Requirements of this document.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.6 CONCLUSIONS/RECOMMENDATIONS

6.6.1 SURVEY-RESULTS: THE TEMPLATE APPROACH - EXPECTED BENEFITS & RISKS

During the face to face meetings of the project in October 2012, January 2013 and May 2013 - where the partners were invited for a first overview and to actively contribute with their feedback – as well as during the work stream conference calls in the timeslot February 2013 to May 2013 it showed up that a survey amongst the NGMN operator community would make sense to validate the given perspective of benefits and/or pitfalls of the template approach.

A questionnaire (see details in chapter 6.9 Appendix: SURVEY - BENEFITS OF A STANDARDIZED TEMPLATE MECHANISM) was sent via the NGMN office to all members. About 35% of these members sent back their answers.

Nevertheless the majority of participants gives the positive feedback

- the concept is usable, complete and feasible
- a distributed implementation is useful as this will avoid NEP proprietary - functional not consistent - implementations and leads to a standardized and unified mechanism being helpful in multivendor environment
- there are more benefits than risks – this partially is based on own experience of the answering parties
- a migration concept will be needed and supported by the NEPs

A synopsis of the answers is following:

3.1 Feasibility, usability and completeness of the concept

- It is certainly usable, complete, effective and feasibility. May need phased robust introduction and paradigm change - a migration concept.
- The concept is very useful and would increase the efficiency of configuration management functions.
- We understand that establishment and standardization of template management processes is a good step for improvement.
- Currently, we use vendor provided templates, changing reduced set of parameters which should not be configured as default. Template management will just organize the same in more suitable form.
- As for completeness, we do not see any statements regarding template management and SON issue: if operational parameters change by SON would affect template management?
- Due to the huge number of RAN configuration parameters to be set, templates are of utmost importance to save time and avoid errors when configuring (e)NodeBs. The concept is useful and already in use today.

3.2 Distributed implementation or single layer implementation

- Distributed implementation seems to be more effective since it may lead to standardisation on both EMS and NMS layers.
- Ability in both must be supported but which and why depends on operator deployment and policy. Over time both approaches co-exist. In addition compliant with 3GPP standards on (SON conflict-resolution) Policy, even an EMS-centric approach should have NMS as default when needed.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

- Implementation of template management and distribution on NMS level looks more "practical". NMS maintains all templates and utilize unified NBI to communicate to EMSs of various vendors.
- Distributed implementation - Operators' reality is to use multiple EMS from different vendors, while at the same time a NMS layer allows for flexibility to model network facing services and their representation in terms of sets of configuration parameters in a common fashion across the different vendor domains. Besides, Operators have already considerable investment in existing NMS and operational processes are very dependent on them, so a complete replacement of NMS with new EMS functionality does not seem to be realistic or pragmatic.
- An implementation on the NMS layer plus on the EMS layer is necessary. The reason is that, at the EMS layer, templates are vendor-specific. The benefit of having, in addition, an implementation at the NMS layer is that Service Providers can define their own templates or use templates offered by network planning and optimization tools.

3.3 Benefits of an implementation - perspective

Benefits:

- Competition between vendors of EMS and NMS may increase, reduction of parameters to be set up may make easier implementation of LTE networks.
- Our view is that template mechanisms - even the current proprietary EMS template mechanisms - have significant positive quality impact on the network. Also man-power efforts in handling parameter information are reduced.
- Save time, Avoid configuration errors, Enable operational staff to concentrate on non-repetitive tasks.
- The anticipated benefits will be:
  - configuration data accuracy
  - high consistency across network elements
  - lower labour efforts during re-configurations and re-tuning of RAN networks
  - faster deployments of new clusters and new technologies
  - less troublesome software upgrades (in cases of required significant configuration parameter changes)
  - faster rollout of new markets
  - saved labour costs from reduced cases of correcting configuration errors
  - better flexibility when replacing one RAN vendor with another

Positive ROI:

- Since the document is handled mostly by technical team its difficult to provide feedback regarding financial issue like ROI – therefore items 3.3.3 and 3.3.4 below are not filled.
- There may be initial challenges to address but achieving standardized and portable solutions, plus efficient mechanisms result in cost and energy efficiency, plus potential areas of performance optimization, all contributing positively.
- A positive ROI will emerge probably after 3-4 years post deployment, when the operational processes would have been modified and based on templates so that the full benefit of templates can be realized. It will take time to transition existing systems and processes as well as to pay off an initial deployment capital cost, thus a delay in turning a positive ROI.
- Yes.

3.3.1 … and its contribution to quality enhancements of the configuration data files

- High ~ 70 (answers: 40% to 100%)

3.3.2 … and its contribution to Process automation

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

- High ~ 75 (answers: 60% to 80%)

3.3.3 … and its contribution to CAPEX and/or OPEX reduction

- Medium ~ 50 (answers: 40% to 60%)

3.3.4 … and its contribution to Time to market and cash flow enhancements

- Low ~ 35 (answers: 20% to 80%)

3.4 Benefits of an implementation – real experience

- N/A (but supportive of its prospects)
- There are no experiences of proposed concept in its 'clean' form like mentioned before. However, regarding the experiences, the template mechanisms using proprietary capabilities provided by EMSs from main network vendors we have been utilizing for number of years. EMS templates are interchanged with radio planning system (most used parameters are moved in the interface plus the template name).
- The arrangement has proven valuable and improved quality of information compared that situation when the default parameters were left into the network. Also the situation without templates made the situation very difficult to handle (the elements themselves had some version dependant defaults)
- We have no detail measured figures available but we have gained in quality improvements and reduced manpower efforts
- We have low experience here. The practice we use: just to use some scripts to simplify vendor provided templates attributing.
- No real experience at this time.
- Our company is already using templates to configure RAN equipment. It was not possible to collect figures on savings or quality enhancements related to using such a concept.

3.4.1 … and its contribution to quality enhancements of the configuration data files

- This is a clearly positive perspective - even if some answers claim that they can't fill sub-items in detail.

3.4.2 … and its contribution to Process automation

- This is a clearly positive perspective - even if some answers claim that they can't fill sub-items in detail.

3.4.3 … and its contribution to CAPEX and/or OPEX reduction

- Most answers claimed that they can't fill sub-items in detail but a contribution is clearly visible.

3.4.4 … and its contribution to Time to market and cash flow enhancements

- Most answers claimed that they can't fill sub-items in detail.

3.5 Risks and financial impacts of an implementation – perspective

- It is intuitive in long term but we anticipate a phased roadmap to justify business case. Testing is required to evaluate gains and risks. Plus given the sensitivity, a dual mechanism graceful

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

evolution is needed where both legacy and new measures work together or legacy as backup until fully proven and stable.

- At the moment we do not see any big risks.
  It could be problem with comparison between different vendors based on descriptions, namely without huge testing activities. It's also not very evident regarding quality of network if some standard parameters without country-specifics will be utilized.
- Uncertainty how the proposed concept will be progressing in concrete standardization work.
  Uncertainty of vendor EMS roadmaps regarding the new concept.
  Potentially living with two generation of CM/EMSs, this concept and old one.
- Anticipated risks :
  - EMS and NMS vendors will charge high licensing prices for the new functionality
  - EMS and NMS vendors will roll out the new functionality in multiple steps with associated incremental costs and delayed benefit for the operators
  - EMS and NMS vendors will offer unreasonably high annual maintenance or licensing for the new features
  - Successful deployment of SON features may diminish the value of templates-based CM
- Depending on multiple cost factors the ROI may not turn as positive as expected/wished for.
- No risk identified so far.

3.6 Risks and financial impacts of an implementation – real experience

- No measurable figures available.
- No figure available so far.
- In our current set-up we of course encounter vendor dependencies and proprietary integration needs. Unfortunately we are not able provide any figures regarding the viewpoints below in 3.7

3.7 Integration and operation cost percentage

3.7.1 Average annual integration expenses percentage for EMS – NMS (OSS) interfaces

- if interface was following a standard Low ~25
- if interface was proprietary Medium ~50

3.7.2 Average annual OSS interface license cost percentage if any

- Medium ~40

3.7.3 Average annual OSS interface maintenance and adaption cost percentage if any

- High ~80

6.6.2 THE NGCOR CM REQUIREMENTS AND THEIR ADDRESSEES

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	1	x		
REQ-CM	2	x		
REQ-CM	3	x	x	x

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	4		x	
REQ-CM	5		x	x
REQ-CM	6		x	x
REQ-CM	7		x	
REQ-CM	8		x	
REQ-CM	9		x	
REQ-CM	10	x	x	x
REQ-CM	11	x	x	x
REQ-CM	12	x	x	x
REQ-CM	13		x	x
REQ-CM	14		x	
REQ-CM	15		x	
REQ-CM	16	x	x	x
REQ-CM	17		x	x
REQ-CM	18		x	x
REQ-CM	19		x	x
REQ-CM	20		x	
REQ-CM	21		x	
REQ-CM	22		x	
REQ-CM	23		x	
REQ-CM	24		x	
REQ-CM	25		x	
REQ-CM	26		x	
REQ-CM	27		x	
REQ-CM	28		x	
REQ-CM	29		x	
REQ-CM	30		x	
REQ-CM	31		x	
REQ-CM	32		x	
REQ-CM	33	x	x	
REQ-CM	34		x	
REQ-CM	35		x	
REQ-CM	36		x	
REQ-CM	37		x	
REQ-CM	38		x	
REQ-CM	39		x	
REQ-CM	40		x	
REQ-CM	41		x	
REQ-CM	42		x	
REQ-CM	43		x	
REQ-CM	44		x	
REQ-CM	45		x	

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	46		x	
REQ-CM	47		x	
REQ-CM	48	x	x	x
REQ-CM	49		x	x
REQ-CM	50		x	
REQ-CM	51		x	
REQ-CM	52		x	
REQ-CM	53		x	
REQ-CM	54		x	
REQ-CM	55		x	
REQ-CM	56		x	
REQ-CM	57		x	
REQ-CM	58		x	
REQ-CM	59		x	
REQ-CM	60		x	
REQ-CM	61		x	
REQ-CM	62		x	
REQ-CM	63		x	
REQ-CM	64		x	
REQ-CM	65		x	
REQ-CM	66		x	
REQ-CM	67		x	
REQ-CM	68		x	
REQ-CM	69		x	x
REQ-CM	70	x	x	
REQ-CM	71	x		
REQ-CM	72	x		
REQ-CM	73	x		
REQ-CM	74	x		
REQ-CM	75	x		
REQ-CM	76		x	
REQ-CM	77		x	
REQ-CM	78		x	
REQ-CM	79		x	
REQ-CM	80		x	
REQ-CM	81		x	
REQ-CM	82	x	x	
REQ-CM	83	x	x	
REQ-CM	84			x
REQ-CM	85			x
REQ-CM	86			x
REQ-CM	87			x

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	88			x
REQ-CM	89			x
REQ-CM	90			x
REQ-CM	91			x
REQ-CM	92			x
REQ-CM	93			x
REQ-CM	94			x
REQ-CM	95			x
REQ-CM	96			x
REQ-CM	97		x	x
REQ-CM	98		x	x
REQ-CM	99		x	x
REQ-CM	100		x	x
REQ-CM	101		x	x
REQ-CM	102	x	x	x
REQ-CM	103			x
REQ-CM	104			x
REQ-CM	105	x	x	x
REQ-CM	106		x	x
REQ-CM	107		x	x
REQ-CM	108		x	x
REQ-CM	109		x	x
REQ-CM	110		x	x
REQ-CM	111			x
REQ-CM	112			x
REQ-CM	113		x	x
REQ-CM	114			x
REQ-CM	115	x	x	x
REQ-CM	116		x	x
REQ-CM	117		x	x
REQ-CM	118			x
REQ-CM	119			x
REQ-CM	120			x
REQ-CM	121		x	x
REQ-CM	122			x
REQ-CM	123			x
REQ-CM	124		x	x
REQ-CM	125			x
REQ-CM	126		x	x
REQ-CM	127			x
REQ-CM	128			x
REQ-CM	129			x

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	130			x
REQ-CM	131	x	x	x
REQ-CM	132			x
REQ-CM	133			x
REQ-CM	134			x
REQ-CM	135			x
REQ-CM	136			x
REQ-CM	137			x
REQ-CM	138		x	x
REQ-CM	139			x
REQ-CM	140		x	x
REQ-CM	141			x
REQ-CM	142			x
REQ-CM	143		x	x
REQ-CM	144			x
REQ-CM	145			x
REQ-CM	146			x
REQ-CM	147			x
REQ-CM	148		x	x
REQ-CM	149			x
REQ-CM	150		x	x
REQ-CM	151	x	x	x
REQ-CM	152	x	x	x
REQ-CM	153		x	
REQ-CM	154		x	
REQ-CM	155	x	x	x
REQ-CM	156	x	x	x
REQ-CM	157	x	x	x
REQ-CM	158	x	x	x
REQ-CM	159	x	x	x
REQ-CM	160		x	
REQ-CM	161	x	x	
REQ-CM	162	x	x	
REQ-CM	163	x	x	x
REQ-CM	164	x		x
REQ-CM	165	x	x	x
REQ-CM	166	x	x	x
REQ-CM	167	x	x	x
REQ-CM	168	x	x	x
REQ-CM	169	x	x	x
REQ-CM	170	x	x	x
REQ-CM	171	x	x	x

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Requirement Nr		SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CM	172			x
REQ-CM	173			x
REQ-CM	174	x	x	x
REQ-CM	175	x	x	x
REQ-CM	176			x
REQ-CM	177	x	x	x
REQ-CM	178			x

Table 2: CM Requirements - Whom these requirements are addressed to

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.7 REFERENCES

[1] NGMN Alliance - NGMN TOP OPE Requirements Version 1.0

[2] NGMN Alliance - NGCOR Consolidated Requirements Phase I, Version 1.3, April 16, 2012

[3] 3GPP TS 32.101 Telecommunication management; Principles and high level requirements

[4] 3GPP TS 32.102 Telecommunication management; Architecture

[5] 3GPP TS 32.150 Telecommunication management; Integration Reference Point (IRP) Concept and definitions

[6] 3GPP TS 32.501 Telecommunication management; Self-configuration of network elements; Concepts and requirements

[7] 3GPP TS 32.600 Configuration Management; Concept and high-level requirements

[8] 3GPP TS 32.602 Configuration Management (CM); Basic CM Integration Reference Point (IRP)

[9] 3GPP TS 32.611 Configuration Management (CM); Bulk CM Integration Reference Point (IRP): Requirements

[10] 3GPP TS 32.612 Configuration Management (CM); Bulk CM Integration Reference Point (IRP): Information Service (IS)

[11] 3GPP TS 32.622 Configuration Management (CM); Generic network resources Integration Reference Point (IRP); Network Resource Model (NRM)

[12] 3GPP TS 28.620 Fixed Mobile Convergence (FMC) Federated Network Information Model (FNIM) Umbrella Information Model (UIM)

[13] Software-Defined Networking: The New Norm for Networks, ONF White Paper, April 13, 2012

[14] http://www.sdncentral.com/sdn-blog/openflow-northbound-api-olympics/2012/07/

[15] TM Forum eTOM Release 9.0, GB921 Addendum D Version 9.3, April 2011

[16] TM Forum http://www.tmforum.org/MTOSI/2319/home.html

[17] http://www.netconfcentral.org/netconf_docs

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.8 GLOSSARY

Abbreviation	Meaning & Terms	Further explanation
2G/3G/LTE	Standards for mobile communication network and devices capabilities	
3GPP	3rd Generation Partnership Project	http://www.3gpp.org
3GPP SA5	Telecom Management group within 3GPP	http://www.3gpp.org/SA5-Telecom-Management
AAA	Authentification and Authorization & Accounting	Function providing a network service related to billing & charging system
ABR	Asynchronous Batch Response	Is a message exchange pattern. This is a multiple response pattern. The response of the first invocation returns an acknowledgement. The result set will then be sent in chunks to the service consumer (via the call back receptacle) as the data becomes available in the service producer. The consumer usually has control over the size of the chunks specified in the initial call.
ADSL	Asynchronous Digital Subscriber Line	
AFB	Asynchronous (File) Bulk Response	Is a message exchange pattern. The initial request is non-blocking and the service consumer gets notified when the transfer is completed.
AFI	Autonomic Future Internet	ETSI's pre-standardization body
AN	Asynchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
ANR	Automatic Neighborhood Relation	
API	Application Programming Interface	
ARPU	Average Revenue Per User	Commercial KPI used in business plan
ARR	Asynchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
ASCII	American Standard Code of Information Interchange	ASCII
ASN.1	Abstract Syntax Notation One	
ASP	Application Service Provider	
ATM	Asynchronous Transfer Mode	ATM technology
B2B	Business-To-Business	
BA	Business Agreement (TM Forum)	Requirements and usage scenario specification.
BBF	Broadband Forum	http://www.broadband-forum.org
BER	Bit Error Ratio	Is the number of bit errors divided by the total number of transferred bits during a studied time interval.
BNG	Broadband Network Gateway	It's an evolution of the existing BRAS the Gatway for Fixed Access Network
BSS	Business Support Systems	Business Support Systems
CAPEX	Capital Expenditures	costs to set up/ change a network
CBE	Common Business Entity	TMF SID term
CCV	Common Communications Vehicle	A communication infrastructure connecting Operations Systems (e.g., CORBA platform, JMS platform)
CDR	Call Details Records	

Abbreviation	Meaning & Terms	Further explanation
CFS	Customer Facing Service	TMF SID term
CFSS	Customer Facing Service Specification	TMF SID term
CI	Configuration Item	ITIL term
close loop	Autonomous Operated SON Function	
CM	Configuration Management	
CMDB	Configuration Management Data Base	ITIL term
CMIP	Common Management Information Protocol	CMIP is a protocol for network management.
CMS	Configuration Management System	ITIL term
CN	Core Network	
CORBA	Common Object Request Broker Architecture	CORBA
CORBA	Common Object Request Broker Architecture	CORBA is a standard defined by the Object Management Group (OMG) that enables software components written in multiple computer languages and running on multiple computers to work together.
COTS	Commercial Off the Shelf	COTS
CPE	Customer Premises Equipment	
CRUD	Create, Read, Update, Delete	
csv	Comma Seperated Value	
CTK	Compliance Test Kit	Part of TM Forum interface specification.
DDP	Document Delivery Package	The MTOSI interface specification is structured in DDPs based on eTOM level 2/3 processes.
DSLAM	Digital Subscriber Line Access Multiplexer	
DT	Deutsche Telekom (Operator)	
e2e	end-to-end	
EM	Element Management	EM
EMS	Element Management System	EMS
eNB	Enhanced NodeB	
EPC	Evolved Packet Core	Mobile Core Network for 4G
eTOM	Enhanced Telecommunication Operations Map	eTOM
ETSI	European Telecommunications Standards Institute (SDO)	
FAB	Fulfillment, Assurance and Billing	
FCAPS	Fault, Configuration, Assurance, Performance	FCAPS
FDD	Feature Description Document	TMF concept
FIM	Federated Information Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Information Model part of these models contains the static data; i.e., the object classes with their attributes and the content of the notifications."
FM	Fault Management	Fault Management
FMC	Fixed Mobile Convergence	http://en.wikipedia.org/wiki/Fixed-mobile_convergence

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Abbreviation	Meaning & Terms	Further explanation
FOM	Federated Operations Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Operations Model part of these models contains the dynamics; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
FRU	Field Replaceable Unit	
FT IRP	File Transfer Integration Reference Point	
GDMO	Guidelines for the Definition of Managed Objects	GDMO is a specification for defining managed objects of interest to the Telecommunications Management Network for use in CMIP.
GEN	Generic Next Generation Operational Requirements	
GPON	Gigabit-capable Passive Optical Network	
GWCN	Gateway Core Network	A variant of core network sharing model
HLR	Home Location Register	
HO	handover	
HSS	Home Subscribe Server	It's an evolution of the current HLR used as a location server for 2G/3G networks
HTTP	Hyper Text Transfer Protocol	
HW	Hardware	Hardware
IA	Information Agreement (TM Forum)	UML model specification
IDL	Interface Definition Language	OMG IDL
IETF	Internet Engineering Task Force (SDO)	IETF
IIS	Interface Implementation Specification (TM Forum)	Protocol specification; e.g., using XML or CORBA
IM	Information Management	
IMS	IP Multimedia Subsystem	http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem
InvM	Inventory Management	
IP	Internet Protocol	http://en.wikipedia.org/wiki/Internet_Protocol
IPR	Intellectual Property Rights	
IRP	Integration Reference Point (3GPP term)	3GPP 32.103
ISG	Industry Specification Group	ETSI's pre-standardization instrument
ITIL	Information Technology Infrastructure Library	
itSMF	IT Service Management Forum	
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector (SDO)	ITU-T
JMS	Java Message Service	JMS is a Java Message Oriented Middleware API for sending messages between two or more clients.
JPA	Java Persistence API	JPA is a Java programming language framework managing relational data in applications using a Java Platform.
JVT	Java Value Types	
LCC	Lower Camel Case	An approach to indicate word boundaries using medial capitalization, thus rendering "two words" as "twoWords".

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Abbreviation	Meaning & Terms	Further explanation
		This convention is commonly used in Java.
LTE	Long Term Evolution	http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution
MEF	Metro Ethernet Forum (SDO)	MEF
MEP	Message Exchange Pattern	The combination of a communication pattern and a communication style which fully identifies the messages and the choreography (sequencing and cardinality) of messages through a management interface.
MME	Mobility Management Entity	
MMS	Multimedia Messaging Service	
MO	Managed Object	Managed_object
MOCN	Multi-Operator Core Network	Model of Network sharing which does not share the Core Networks
MOM	Message Oriented Middleware	
MORAN	Multi-Operator Radio Access Network	A model of Network sharing at Radio access level
MPLS	Multi Protocol Label Switching	MPLS
MRI	Manage Resource Inventory	
MSI	Manage Service Inventory	
MT	Modelling and Tooling	Project sub stream of NGCOR
MTNM	Multi Technology Network Management	
MTOSI	Multi Technology OS interface	TM Forum interface product. It is an XML-based Operations System (OS)-to-OS interface suite. The Network Management System-to-Element Management System communication is also covered as a special case.
MVNE	Mobile Virtual Network Environment	
MVNO	Mobile Virtual Network Operator	
MW	Management World	TM Forum event
MW	TM Forum Management World	
NE	Network Element	Network_element
NBI	Northbound Interface	Interface between EMS and NMS
NGCOR	Next Generation Converged Operations Requirements	NGMN project
NGMN	Next Generation Mobile Network	http://www.ngmn.org
NGN	Next Generation Network	http://en.wikipedia.org/wiki/Next_Generation_Networking
NGOSS	Next Generation Operation Systems and Software	
NM	Network Management	Network_management
NMS	Network Management System	Network_management_system
NOC	Network Operation Centre	
NRM	Network Resource Model (3GPP)	Contains the static data of an interface specification.
O	Orange (Operator)	
OA&M	Operation, Administration & Maintanance	OA&M
OC	Operating Committee (NGMN)	

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Abbreviation	Meaning & Terms	Further explanation
OCL	Object Constraint Language	OCL is a declarative language for describing rules that apply to Unified Modeling Language (UML) models.
OPE	Operational Efficiency	Requirements specification from NGMN.
OpenFlow		OpenFlow is the first standard communications interface defined between the control and forwarding layers of an SDN architecture.
OPEX	Operational Expenditures	Costs of running a network
OS&R	Operation, Support and Readiness	Is a Level 1 process grouping of the Business Process Framework. OS&R contains processes for ensuring operational readiness in the fulfillment, assurance and billing areas.
OSA	Open Services Access	
OSS	Operations Support System	Operations_support_system
OSSJ	OSS through Java	
PBB-TE	Provider Backbone Bridges - Traffic Engineering	
PCC	Policy Charging and Control	
PCRF	Policy and Charging Rules Function	It's a functional block in the EPC network architecture for charging & Policy
PDF	Portable Document Format	
PDH	Plesiochronous Digital Hierarchy	
PM	Performance Management	http://en.wikipedia.org/wiki/FCAPS
PT	Portugal Telecom (operator)	
QoS	Quality of Service	QoS
RAM	Resource Alarm Management	Used as an abbreviation for the FM Interface specification workstream of the TMForum
RAN	Radio Access Network	http://en.wikipedia.org/wiki/Radio_access_network
RAT	Radio Access Technology	
RFS	Resource Facing Service	
RFSS	Resource Facing Service Specification	
RI	Reference Implementation	Part of TM Forum interface specification.
Rinv	Resource Inventory	
RM	Resource Mangement	
RM&O	Resource Management & Operations	
RPC	Remote Procedure Call	RPC is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction.
SACM	Service Asset and Configuration Management	
SAE	System Architecture Evolution	**SAE** is the core network architecture of 3GPP's future LTE wireless communication standard. SAE is the evolution of the GPRS Core Network, with some differences: ▪ simplified architecture

Abbreviation	Meaning & Terms	Further explanation
		▪ All IP Network (AIPN) support for higher throughput and lower latency radio access networks (RANs) ▪ support for, and mobility between, multiple heterogeneous RANs, including legacy systems as GPRS, but also non-3GPP systems (say WiMAX) The main component of the SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC will serve as equivalent of GPRS networks (via the Mobility Management Entity, Serving Gateway and PDN Gateway subcomponents).
SDH	Synchronous Digital Hierarchy	SDH technology
SDN	Software Defined Networking	
SDO	Standards Developing Organisation	All committes, fora and partnerships that create standards, recommendations and technical reports.
SecM	Security Management	
SFB	Synchronous (File) Bulk Response	Is a message exchange pattern. The service consumer requests a response set to be uploaded to a storage server and the blocking call returns when the transfer is complete.
S-GW	Serving Gateway	
SI&P	Strategy, Infrastructure & Product	
SID	Shared Information & Data model (TM Forum)	http://www.tmforum.org/InformationFramework/1684/home.html
SIT	Synchronous Iterator	Is a message exchange pattern. This is a multiple response pattern. This is the classical Iterator design pattern. The response of the first invocation returns a partial data set as well as a pointer to an Iterator interface. The service consumer will then invoke the Iterator to receive the subsequent result data set partitions. The consumer has control of the flow, the service provider needs to maintain the state related to the pending Iterator.
SLA	Service Level Agreement	KPI describing user requirements tro be translated into QOS objective at operator side within an agreement
SM	Security Management	http://en.wikipedia.org/wiki/FCAPS
SM&O	Service Management &Operations	
SN	Synchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
SNMP	Simple Network Management Protocol	SNMP is an "Internet-standard protocol for managing devices on IP networks"
SOA	Service Oriented Architecture	Service-oriented_architecture
SOAP	Simple Object Access Protocol	
SON	Self Organizing Network	
SONET	Synchronous Optical Network	SONET
SP	Service Provider	Company, which provides access to telephone and related communications services
SPR	Subscription Profile Repository	It's a data base for user profiles
SQM	Service Quality Management	eTOM definition: "SQM encompasses monitoring,

Abbreviation	Meaning & Terms	Further explanation
		analyzing and controlling the performance of the service perceived by customers"
SRR	Synchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
SuM	Subscription Management	
SW	Software	Software
TA	Tracking Area	
TAM	Telecom Appplications Map	TMF term
TMF	TM Forum	www.tmforum.org
TWG SC	Technical Working Group Steering Committee	NGMN group
UCC	Upper Camel Case	An approach to indicate word boundaries using medial capitalization, thus rendering "two words" as "TwoWords". This convention is commonly used in Java.
UDC	User Data Convergence	Evolution of unified data bases
UE	User Equipment	
UML	Unified Modelling Language	UML
UMTS	Universal Mobile Telecommunication System	UMTS
USIM	Universal Subscriber Identity Module	
VF	Vodafone (operator)	
WDM	Wavelength Division Multiplexing	WDM
WiMax	Worldwide Interoperability for Microwave Access	WiMAX
WLAN	Wireless Local Area Network	WLAN
WS	Web Service	Web Services
WSDL	Web Service Description Language	WSDL
XMI	XML Metadata Interchange	http://en.wikipedia.org/wiki/XMI
XML	Extensible Markup Language	XML
Xpath	XML Path Language	XPATH is a query language for selecting nodes from an XML document.
XSD	XML Schema	XSD
	alarm interface	An interface which transports alarm - informations between OSS systems
	Business Services	These are the operations in TM Forum terminology.
	Business Use Case	High level uses case driven by a business scenario.
	common architecture	All interfaces should be part of a common architecture
	Common Core Network	Business architecture Scenario
	Common Information Model	This term is used to reference information models like TMForum SID
	Communication Partners	OSS systems, which exchange information
	Converged Framework Model	Harmonised design guidelines for tooling.
	cross-domain	Cross mobile and fixed domains
	cross-domain	Cross mobile and fixed domains

Abbreviation	Meaning & Terms	Further explanation
	Domain	Related to the partioning of the network
	Dynamic Requirement	Requirements which describe the operations part of the management interface.
	Element Management Layer	EMS level in layering architecture
	Element Manager	Element_Manager
	EMS (server)	The SW component which implements the interface in the OSS systems, which delivers a service to other OSS systems
	EMS-OSS layer	Summary of all OSS systems which deliver an EMS functionality
	eNodeB	Base Station for LTE
	entity	An entity is some tangible or conceptual thing , entity word is typically used when presenting things without a real name name or label. Entities are characterized by attributes and relationships.
	EPC Network	Mobile Core Network for 4G
	federated information / data model	See sub-task MT
	Federated Model	see Operations Model
	Federated Network Resource Model	see Operations Model
	femtoCell	Home NodeBB (Base Station deployed in the Home)
	implementation technology	Technology used to implement a functionality
	Infrastructure Domain	
	Interfacing / Integration	
	inventory component	An instance of the objects in an inventory database
	logical resource	Logical resources are e.g., subnetwork connection, topological link, termination point etc..
	management architecture	Defines the architecture between Operations Systems and the between Operations Systems and the network.
	management area	These are e.g., alarm management, inventory, performance management etc..
	Management Interface	An instance of an interface between two OSes used for management.
	Management Model	Generic term for information model and operations model.
	management operation	Operations executed via the management interface.
	management recommendations	ITU-T standards are called Recommendations.
	management workflows	Specific sequence of operations executed via the management interface.
	multi-domain network	Domains are e.g., access, metro, backhaul, core.
	multi-technology network	Technologies are e.g., ATM, OTN, SDH, Ethernet, DSL, LTE, 2G, 3G, HSPA.
	Network Abstraction Layer	A logical layer between the network and the management layer which relay an abstracted view (from management point of view) of the network.
	network data	Data which describes - from management point of view - the underlying network in an abstract way. This data can be used by all different management areas.
	Network Level Interface	An interface which is able to provide an end-to-end view of the underlying network.

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Abbreviation	Meaning & Terms	Further explanation
	network level management	A management function which is able to manage an end-to-end view of the underlying network.
	Network Operator	Company, which provides access to telephone and related communications services
	Network Resource Model	Data model representing the equipment of a network. It's 3GPP terminology
	network technology	For Mobile , it means 2G, 3G or 4G
	network type	The type of the network (e.g. UMTS- Radio, DWH, IP, etc. ..)
	NGOSS concepts	Concepts (like eTOM, SID, etc…) which are summarized within the "Next Generation Operation Support Systems" - concept of the TMForum
	NMS (client)	The SW component which implements the interface in the OSS systems, which requests a service from another OSS system.
	OA&M functional domain	It refers to ITU-T "FCAPS"
	open loop	Operator controlled SON function
	Operations Model	Contains the dynamic part of the model; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the information model through the management interfaces.
	Operator	Role, responsible for the management of a network and/or service
	operator-wide OSS application	Applications developed by the operator to ensure FM, PM, CM,
	OSS application	An application which delivers a capability dedicated to the OSS domain
	OSS environment	
	OSS Interface	Interface between OSS systems
	physical resource	Physical resources are e.g., network elements, cables, fibres etc..
	primitive	Simplest element provided by a programming language
	resource	Resource is any physical or virtual component of a telecommunications network
	Resource Configuration Management	TMForum TAM definition: "The Resource Configuration Management application generates a resource plan to fulfill a resource order."
	Resource Fault Management	TMForum TAM definition: "Fault Management applications are responsible for the management of faults, or troubles, associated with the service provider's resources. "
	resource management layer	Covers all Resource Management processes as defined in the TM Forum Business Process Framework (eTOM) "Resource Management & Operations" (RM&O) layer within the operations & support, fulfillment, and assurance verticals. This process grouping maintains knowledge of resources (application, computing and network infrastructures) and is responsible for managing all these resources.(e.g. networks, IT systems, servers, routers, etc.) utilized to deliver and support services required by customers.
	service catalogue	Storage of all service specifications and instances
	service configuration and activitation	Operator process dealing with delivery

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Abbreviation	Meaning & Terms	Further explanation
	Service Inventory	TMForum TAM definition: Service Inventory represents the applications which contain and maintain information about the instances of services in a telecom organization
	service management layer	Covers all Service Management processes as defined in the TM Forum Business Process Framework (eTOM) "Service Management & Operations" (SM&O) layer within the operations & support, fulfilment, and assurance verticals. This process grouping focuses on the knowledge of services (Access, Connectivity, Content, etc.) and includes all functionalities necessary for the management and operations of communications and information services required by customers.
	service platform	A resource, which delivers a telecommunication service
	service type	The type of a service (e.g. MMS or SMS - Service)
	shared network	Generic term which includes different model sharing (at core, access network)
	type acceptance	Type Acceptance is the process of verifying that a certain product has passed performance tests and quality assurance tests or qualification requirements stipulated in contracts, regulations, or specifications.
	Umbrella Model	Part of the model containing artefacts that can be used/inherited in both wireline and wireless network models.
	Usage Scenario	TMF term for "use case"; are defined for each required operation
	Use Case	It refers to Business architecture scenarios and Generic & Basic architecture scenarios

Acronym / Term	Definition
O&M	Operations & Maintenance
LTE	Long Term Evolution of UTRAN – Now called E-UTRAN
SAE	System Architecture Evolution **SAE** is the core network architecture of 3GPP's future LTE wireless communication standard. SAE is the evolution of the GPRS Core Network, with some differences: ▪ simplified architecture ▪ All IP Network (AIPN) support for higher throughput and lower latency radio access networks (RANs) ▪ support for, and mobility between, multiple heterogeneous RANs, including legacy systems as GPRS, but also non-3GPP systems (say WiMAX) The main component of the SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC will serve as equivalent of GPRS networks (via the Mobility Management Entity, Serving Gateway and PDN Gateway subcomponents).
EPC	Enhanced / Evolved Packet Core **Evolved Packet Core** is the IP-based core network defined by 3GPP in release 8 for use by LTE and other access technologies. The goal of EPC is to provide a simplified all-IP core network architecture to efficiently give access to various services such as the ones provided in IMS (IP Multimedia Subsystem). EPC consists essentially of a **Mobility Management Entity** (MME) and access agnostic

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

	Gateways for routing of user datagrams
MME	Mobility Management Entity The **Mobility Management Entity** is the main signaling node in the EPC. It is responsible for initiating paging and authentication of the mobile device. It also keeps location information at the Tracking Area level for each user and is involved in choosing the right gateway during the initial registration process. MME connects to eNodeBs through the S1-MME interface and connects to S-GW through the S11 interface. Multiple MMEs can be grouped together in a pool to meet increasing signaling load in the network. The MME also plays an important part in handover signaling between LTE and 2G/3G networks.
S-GW	Serving Gateway The **SGW** routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and PGW). For idle state UEs, the SGW terminates the DL data path and triggers paging when DL data arrives for the UE. It manages and stores UE contexts, e.g. parameters of the IP bearer service, network internal routing information. It also performs replication of the user traffic in case of lawful interception.
HSS	Home Subscribe Server The **Home Subscribe Server** is the main IMS database which also acts as database in EPC. The HSS is a super HLR that combined legacy HLR and AuC functions together for CS and PS domains. In the IMS architecture, the HSS connects to application servers as well as the Call Session Control Function (CSCF) using the DIAMETER protocol.
PGW	PDN Gateway The **PDN Gateway** provides connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one PGW for accessing multiple PDNs. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful Interception and packet screening. Another key role of the PGW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).
eNodeB	Enhanced NodeB – the central element within LTE RAN
NGMN	Next Generation Mobile Network
SON	Self Organizing/Optimizing Network - incorporating Self-X
Self-X	All possible technical functions enabling the network to manage and organize itself in an autonomous way
ANR	Automatic Neighbour Relation the purpose of the ANR function is to relieve the operator from the burden of manually managing Neighbour Relations (NRs).
HO Black List, HO White List	**HO Blacklist**: List of cells to which the eNodeB shall neither establish nor keep a neighbour relation. Black lists can be provided to prevent the UE from reselecting to specific intra- and inter-frequency neighbouring cells.

	HO White list: List of cells to which the eNodeB shall always establish and maintain a neighbour relation. [An IRPManager shall be able to request that HO be prohibited from source cell to target cell and that no other entity than an IRPManager can remove that request. This is termed as HO black-listing. An IRPManager shall be able to request that HO be allowed from source cell to target cell and that no other entity than an IRPManager can remove that request. This is termed as HO white listing.]
NGSSM	Next Generation Service And System Management
CMS	Configuration Management System
FCAPS	Fault, Configuration, Accounting, Performance and Security
QCI	QoS Class Identifier
CEM	Customer Experience Management
QoS	Quality of Service
IP-Sec	Internet Security Protocol
eTOM	Enhanced Telecom Operations Map (source: TeleManagementForum)
SOA	Service Oriented Architecture

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

6.9 APPENDIX: SURVEY - BENEFITS OF A STANDARDIZED TEMPLATE MECHANISM

SURVEY

BENEFITS
OF A
STANDARDIZED TEMPLATE MECHANISM
AS ENABLER OF
MORE EFFICIENT
CONFIGURATION MANAGEMENT

BY NGMN LTD.

DATE: 23-MAY-2013

VERSION 1.0

PUBLICATION	NGMN CONFIDENTIAL WITH LIMITED DISSEMINATION
PROJECT	NGCOR
EDITOR IN CHARGE	MANFRED MACKERT - DT
EDITING TEAM	
DOCUMENT STATUS	VERSION 1.0
APPROVED BY	BOARD / 7TH NOVEMBER 2013

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

Contents

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

1 SHORT INTRODUCTION AND PURPOSE OF THE DOCUMENT

1.1 Project NGCOR

The convergence of mobile and fixed networks is on the way to dramatically increase the complexity of operating the network. Each operator has to consider that the mode of operation is changing.

As a summary the challenge for each operator is to operate their networks in today's context of:

- Introduction of LTE (architecture change)
- Convergence of mobile and fixed line (considering various technologies e.g. WiFi, DSL, etc.)
- Change of mode of operations (sharing options (e.g. 3GPP TS 23.251), managed services, Cloud services, Cloud RAN, etc.)
- Heterogenous multivendor Networks
- Considerations of currently implemented networks (GSM, UMTS…)

Considering that OSS solutions, interfaces and models are less standardized, it is not possible to efficiently and effectively run through this transformation process. Thus a prerequisite is to standardize at least the interface between the element management layer and the NMS layer as well as its capabilities and to harmonize the information models based on operations requirements.

As approved by the Board NGMN has started the Next Generation Converged Operations Requirement (NGCOR) project in March 2011. Its objective is to define converged OA&M requirements to ensure that the operational activities within the converged networks can perform optimally. The project claims to give guidance to SDOs and industry bodies (e.g. 3GPP or TM Forum) as well as ISVs in order to prioritize their work of standardisation and implementation. Developing solutions for the most important requirements is the first and specifying the recommendations for the best solutions is the second target.

The rationale for building OSSs based on standardized interfaces and COTS OSS components is that they will involve less development time by taking advantage of existing, market proven, vendor supported products, thereby reducing overall system development costs and time to market for new services.

Having implemented the NGCOR project's main goal - the standardization of the interfaces between the element management layer and the OSS layer and the harmonization of the information models - a cost reduction of up to 70% is achievable. Not to mention the reduction of effort to maintain the OSS landscape and the reduction of process time.

The NGCOR phase II deliverables are currently in a final review and will be available after approval by the NGNM OC in July 2013 or after.

The requirements built up in the NGCOR project are derived from use cases which themselves are triggered by **Business Scenarios** and **Architecture Scenarios** – the High level requirements for Converged Operations (CON).

Base for the standardisation processes are the definitions which are described in the **Modelling and Tooling** part and that should give guidance to SDOs/organisations and industry bodies (e.g. 3GPP or TM Forum) in order to prioritize the work.

In general the operations tasks of service providers are well described and defined as a part of the ISO Telecommunication Management Network well known as FCAPS. The project in its actual phase II is focussing on

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

the management domains **Performance Management, Service Inventory Management** and **Configuration Management**.

1.2 Survey on needs, value and experience with template management capabilities

This survey intends to capture the views of NGMN members concerning a dedicated set of requirements posted in the NGCOR Configuration Management stream – the approach to introduce an OSS template capability in configuration management to reduce the number of RAN parameters that have to be actively planned to a minimum set of “non default” values.

Background, explanations and requirement descriptions can be found in the following chapter 2 of the document.

The questionnaire in chapter 3 is structured as follows:

- Give your statement on the feasibility and tell us about your view of the usability and completeness of the concept.
- Does it make sense to distribute an implementation to the EMS plus the NMS layer or is it more useful to concentrate an implementation onto the EMS or the NMS layer?
- What are the benefits of an implementation from your perspective? Would you see a positive ROI?
- Does your company have experience with the implementation of such a concept and can you provide real figures on savings (manpower, time to provision the network, time to market for new services …) and/or quality enhancements of configuration data that lead to a more straightforward process?
- Which risks could result in an implementation and what could be the financial impacts if any?

As anonymity of the survey is key for the survey the responses will be strictly processed according to the following rules:

- The Legal Counsel of NGMN (LC NGMN) will send out the questionnaires and receive the responses which are to be provided in writing and properly authorized;
- LC NGMN will confirm receipt of response to individual partners;
- LC NGMN will consolidate the responses and will forward to the NGMN office in an anonymized and aggregated form only;
- Except as otherwise agreed explicitly with the responder all information must not be disclosed in any way other than described in this document.

2 THE CONCEPT UNDER EVALUATION

Copy of chapter 5.5

3 QUESTIONS - VALUE OF TEMPLATE MANAGEMENT FUNCTIONALITY FOR YOUR ORGANISATION

How do you estimate the importance / value of standardized template management functionality in the sense of of efficiency, effectiveness and flexibility for your organisation?

Please give free text or mark one of the boxes that fit to your degree of importance – 1 means less, 5 means highly important.

3.5 Feasibility, usability and completeness of the concept

Please give your statement on the feasibility and tell us about your view of the usability and completeness of the concept:

3.6 Distributed implementation or single layer implementation

Does it make sense to distribute an implementation to the EMS plus the NMS layer (as reflected in the requirements in chapter 2) or is it more useful to concentrate an implementation onto the EMS or the NMS layer?

Please don't forget a justification for your answer.

3.7 Benefits of an implementation - perspective

What are the benefits of an implementation from your perspective?

Would you see a positive ROI?

3.7.1 … and its contribution to quality enhancements of the configuration data files

20%	40%	60%	80%	100%

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

3.7.2 … and its contribution to Process automation

20%	40%	60%	80%	100%

3.7.3 … and its contribution to CAPEX and/or OPEX reduction

20%	40%	60%	80%	100%

3.7.4 … and its contribution to Time to market and cash flow enhancements

20%	40%	60%	80%	100%

3.8 Benefits of an implementation – real experience

Does your company have experience with the implementation of such a concept and can you provide real figures on savings (manpower, time to provision the network, time to market for new services …) and/or quality enhancements of configuration data that lead to a more straightforward process?

3.8.1 … and its contribution to quality enhancements of the configuration data files

20%	40%	60%	80%	100%

3.8.2 … and its contribution to Process automation

20%	40%	60%	80%	100%

3.8.3 … and its contribution to CAPEX and/or OPEX reduction

20%	40%	60%	80%	100%

3.8.4 … and its contribution to Time to market and cash flow enhancements

20%	40%	60%	80%	100%

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

3.9 Risks and financial impacts of an implementation – perspective

Which risks could result in an implementation and what could be the financial impacts if any?

3.10 Risks and financial impacts of an implementation – real experience

Does your company have experience with the implementation of such a concept and can you provide real figures on risks encountered in an implementation and their financial impacts if any?

3.11 Integration and operation cost percentage

How do you estimate the CAPEX / OPEX (integration cost, running annual cost) spent for standardized OSS implementation and rollout for your organization as part of total OSS expenses?
Please mark one of the boxes that fit to your figures.

3.11.1 Average annual integration expenses percentage for EMS – NMS (OSS) interfaces

if interface was following a standard

20%	40%	60%	80%	100%

if interface was proprietary

20%	40%	60%	80%	100%

3.11.2 Average annual OSS interface license cost percentage if any

(not the complete OSS package – only the interface to dedicated EMSs)

20%	40%	60%	80%	100%

3.11.3 Average annual OSS interface maintenance and adaption cost percentage if any

(not the complete OSS package)

20%	40%	60%	80%	100%

ngmn Ltd.
Friedrich-Ebert-Anlage 58 • 60325 Frankfurt • Germany
office@ngmn.org • www.ngmn.org

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

STREAM "PERFORMANCE MANAGEMENT"

by NGMN Alliance

Version:	**1.3**
Date:	**2013-07-22**

PUBLICATION	<CONFIDENTIAL & RESTRICTED / NGMN CONFIDENTIAL/ NGMN CONFIDENTIAL WITH LIMITED DISSEMINATION/ PUBLIC>
PROJECT	NGCORE PHASE 2
EDITOR IN CHARGE	
EDITING TEAM	
DOCUMENT STATUS	APPROVED FOR PUBLICATION
APPROVED BY	NGMN BOARD 7TH NOVEMBER 2013

DOCUMENT HISTORY

DATE	VERSION	AUTHOR	CHANGES
25/05/2012	V 0.1		INITIAL VERSION
22/11/2012	V 1.3	MA ZHI	ADJUST THE ORDER OF SUB SECTIONS IN SECTION 5. PUT SUB SECTION OF GENERAL REQUIREMENTS BEFORE SUB SECTION OF HIGH LEVEL FUNCTIONAL REQUIREMENTS. ADD NEW SUB SECTION 4.2 NAMED HIGH LEVEL ARCHITECTURE FOR THE SCENARIO. CUT BUSINESS SCENARIO WORKPLACE AS A SERVICE USING CLOUD SERVICES. REFINE THE FIGURES AND TEXT OF BUSINESS SCENARIO OF TELEMEDICINE.
23/11/2012	V 1.4	MASSIMO BANZI	REORGANIZED REQUIREMENTS BY INTRODUCING GENERIC REQUIREMENTS CH. BETTER OUTLINED GENERIC REQUIREMENTS BASIC EXPLANATION ON KQI, KPI, PI IN THE INTRODUCTION
25/11/2012	V 1.5	MASSIMO BANZI MA ZHI	RIFORMULATION OF REQUIREMENTS AND FULL DOCUMENT REVISION
7/12/2012	V1.7	MA ZHI	ADD THIRD SCENARIO WALKMAN
14/12/2012	V1.8	CECILIA CORBI MASSIMO BANZI	REVISED OVERALL STRUCTURE
11/01/2013	V1.10	MA ZHI ZOU LAN NIU WEIGUO MASSIMO BANZI	FURTHER REVISIONS AND INTEGRATION TO ALL THE CHAPTERS OF THE DOCUMENT
15/01/2013	V1.11	YVONNE DOERNHOFER	EDITORIAL REVIEW
07/03/2013	V1.13	MA ZHI NIU WEIGUO MASSIMO BANZI	IMPLEMENTED FEEDBACK FROM BEIJING NGCOR AND MULTISDO MEETINGS
11/04/2013	V1.14	MA ZHI NIU WEIGUO JILI MASSIMO BANZI	INTRODUCTION OF KPIS (PIS) FOR THE WIRELESS NETWORK FOR SCENARIO VIDEO COMMUNICATION ALIGNMENT OF REQUIREMENTS TO USE CASES IN THE SUITABLE SLOT WITHIN REQUIREMENT TABLES UPDATE OF TERMINOLOGY TABLE UPDATE OF REQUIREMENTS TITLE AND DESCRIPTION INTRODUCTION OF WEB BROWSING SCENARIO AND DELETION

			OF TELEMEDICINE
30/04/2013	**V1.16**	**MA ZHI** **NIU WEIGUO** **JILI** **MASSIMO BANZI**	
20/06/2013	**V1.18**	**YVONNE DOERNHOFER**	**EDITORIALS**
24/06/2013	**V1.19**	**MASSIMO BANZI** **MA ZHI**	**EDITORIALS** **VALIDATION OF COMMENTS**
25/06/2013	**V1.20**	**YVONNE DOERNHOFER**	**ADDED ADDRESSEES TABLE**
22/07/2013	**V1.30**	**THOMAS KULIK**	**NUMERATION OF CHAPTERS, FIGURES AND TABLES CHANGED**

7 REQUIREMENTS FOR PERFORMANCE MANAGEMENT (PM)

7.1 Stream General overview

- In Chapter 7.2 we give a description of the reason that leads to the document and its scope.
- In Chapter 7.3 we give a description of Performance Management as from Literature, trying to focus where this work is focused. Key Quality Indicators (KQIs) and Key Performance Indicators (KPIs) and their relation are also described.
- Chapter 7.4 is the one of scenarios: An entire description of Business Scenarios with sub-scenarios and related Indicators considered in this work is included. Note that in describing indicators we do not mean to be exhaustive, but just to identify some relevant ones that allows us to better focus on our scope.
- Chapter 7.5 lists the requirements: Generic Requirements, General Ones and High Level Functional Requirements.
- Chapter 7.6 is intended for analyzing the gap analysis in existing work.
- In Chapter 7.6.7 conclusion and recommendations are reported.

Appendices on existing standards lists and theoretical aspects follow.

7.2 Introduction

The interest in Performance Management has significantly increased due to the changes taking place in the newly competitive telecommunications industry which presents several challenges for service providers as follows. A variety of providers enters the marketplace and competes for customers. New entrants that are striving to gain market share and to establish themselves as viable suppliers can use performance to provide one means of attracting customers.

The rapid evolution of telecommunications-based applications is accelerating the rate of introduction of new services that use emerging networking technologies. Performance can help encourage customers to use these new services and technologies. The critical dependency between a constantly expanding set of essential business activities and the availability of communication networks and information services means that great numbers of customers are demanding increasingly stringent communications and information performance levels to insure business continuity. The widespread use of smartphones, tablet computers and other web-enabled mobile devices has caused wireless data services to explode. Service providers' networks see more bandwidth-hungry traffic each day: To survive, service providers need to decrease their cost per bit while simultaneously optimizing their network to handle more traffic.

Several emerging market needs place a new emphasis on specifying performance. These include the requirement to support emergency response personnel, the opening up of the telecom service market to competition, and the deployment of services based on network technologies. Additionally, the number of ebusiness requiring very high levels of service availability from their external networks and services, such as servers, databases, etc., continues to rapidly grow. The cell/ packet-based technologies raise new performance specification issues not present in services based on traditional circuit switched networks and leased lines. These new performance specifications are related to defining, monitoring and collecting performance data, and to transforming that data into useful service performance reports. LTE standards address this huge demand for higher bandwidth, lower latency, and advanced communication services. In LTE networks, many devices need to be managed, increasing the potential points of failure or degradation and service operators are working to compensate for network congestion through improved quality of service. (https://en.wikipedia.org/wiki/Quality_of_service)

These evolving market conditions have forced operators to manage overlapping 2G, 3G and 4G technologies and the convergence of mobile and fixed networks. In turn, it's more important than ever that Element Management Systems (EMSs) and Network Management Systems (NMSs) properly control network devices to ensure calls go through, video gets viewed, online games perform, and more.

Performance Management provides functions to evaluate and report on the behaviour of telecommunication equipment and the effectiveness of the network or network element. Therefore the constant monitoring of the quality of Services (Service Performance Management) and Networks (Network Performance Management) are becoming more critical.

Service Performance Management mainly includes:

(1) Service Support Performance
(2) Service Operability Performance
(3) Service Accessibility Performance
(4) Service Retainability Performance
(5) Service Integrity Performance
(6) Service Security Performance

In this document we focus mainly on categories **3**, **4**, and **5.** That leads to network performance indicators that include:

(1) Planning, Provisioning, and Administrative Performance (Resources and Facilities)
(2) Dependability with Availability Performance and related aspects (Grade of Service)
(3) Transmission Performance with Propagation aspects

This document refers mainly to items **2** and **3**.

7.2.1 Scope

Following objectives have been identified:

- Delivery of relevant services scenarios for Performance Management in an hybrid environment of converged heterogeneous networks.
- Delivery of recommendations and high level requirements on how to define modeled KQI/ KPIs for the identified service scenarios.
- In the second part of the stream timeframe (e.g. in January 2013) it will be evaluated to extend the scope of the stream to cover also the following objective:
- Based on the above 2 stream outcomes, a gap analysis of what already exists on Performance Management (mainly in 3GPP & TM Forum, (see also [1] and [2] for references) will be provided. Based on this analysis, a set of KQIs and KPIs of interest will be selected and high level requirements will be defined.
- Delivery of the OSS Requirements for PM on the northbound interface, e. g. performance job schedule, creation, modification and deletion. And performance file collection requirement.
- Solution requirement (requirements and recommendations for performance data template or file format, such as XML schema)

Out of scope

- Performance measurement definition. Performance detail measurements or counters definition is out of PM scope because there are plenty of measurements in the current network to sort out. Our concern is not the NE specific measurements of the KPIs, but the way to manage the Performance data and their exchanges for the operator's needs. Indeed, the operator shall be able to trigger from its OSS PM application, performance jobs for dedicated purpose and need (targeted NEs, or targeted Cells, or targeted domain/ zone/ area), and collect related PM measurements within its OSS PM application. All Performance Management related information exchanges between the EMS and OSS PM applications shall comply with standardized specifications.

7.2.2 References

[1] "NGMN Informative List of SON Use Cases", April 17th, 2007 - [OPS06] PERFORMANCE MANAGEMENT IN REAL TIME

[2] "NGMN Recommendation on SON and O&M Requirements", December 5th, 2008 -PERFORMANCE MANAGEMENT IN REAL TIME

[3] "Self-Optimizing Networks - The Benefits of SON in LTE", 4G Americas, July 2011 - SELF-TUNING X2 INDEPENDENT ALGORITHMS

[4] ITU-T Recommendations E.800

[5] ITU-T Recommendations E.801

[6] 3GPP TR 32.831 V1.0.0 , "Study on Alignment of 3GPP Performance Management and TM Forum Interface Program (TIP) Performance Management (Release 10)"

[7] 3GPP TS 32.410 Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM, Release 10

[8] 3GPP TS 32.450: Telecommunication management; Key Performance Indicators (KPI) for E-UTRAN: Definitions, Release 10

[9] 3GPP TS 32.455: Telecommunication management; Key Performance Indicators (KPI) for the Evolved Packet Core (EPC); Definitions, Release 10

[10] ETSI TS 102 250-2 V2.2.1 2011-4.

[11] 3GPP TS 32.401 Telecommunication management; Performance Management (PM); Concept and requirements

[12] 3GPP TS 32.451: Telecommunication management; Key Performance Indicators (KPI) for E-UTRAN; Requirements, Release 10

[13] TM Forum GB923 Wireless Service Measurements Handbook V3.0

[14] TM Forum GB922_Addendum_1_Performance_R12-5_v1-10 Performance Business Entities

[15] TM Forum GB917 SLA Management Handbook Volume 2 Concepts and Principles Release 2.5

[16] TM Forum GB929 TAM Application_Framework_R4_5__V4.3

[17] TM Forum TIP_PM_BA_V1_8 Performance Management Business Agreement

7.2.3 Terminology

Term	Definition	Origin
Network Element (NE)	A facility or equipment used in the provision of a telecommunications service. Such term also includes features, functions, and capabilities that are provided by means of such facility or equipment, including subscriber numbers, databases, signalling systems, and information sufficient for billing and collection or used in the transmission, routing, or other provision of a telecommunications service	Telecommunications Act of 1996, Federal Communication Commission
Element Management System (EMS)	Network Element Manager (EM): provides a package of end-user functions for management of a set of closely related types of Network Elements. These functions can be divided	3GPP TS 32.401 V11.0.0 (2012-09)

	into two main categories: • Element Management Functions for management of Network Elements on an individual basis. These are basically the same functions as supported by the corresponding local terminals. • Sub-Network Management Functions that are related to a network model for a set of Network Elements constituting a clearly defined sub-network, which may include relations between the Network Elements. This model enables additional functions on the sub-network level (typically in the areas of network topology presentation, alarm correlation, service impact analysis and circuit provisioning).	
Network Management System (NMS)	Network Manager (NM): provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EM(s) but it may also involve direct access to the Network Elements. All communication with the network is based on open and well-standardised interfaces supporting management of multi-vendor and multi-technology Network Elements.	3GPP TS 32.401 V11.0.0 (2012-09)
North Bound Interface (NBI)	It's the management interfaces between the Element Management System and Network Manage System.	3GPP TS 32.101 V11.1.0(2012-12)
South Bound Interface (SBI)	It's the management interfaces between the Network Element and Element Management System.	3GPP TS 32.101 V11.1.0(2012-12)
Service Management System (SMS)	All systems related to the Service Management Domain as explained in Chap 6 in TAM model	TM Forum - TAM Application_Framework_R4_5__V4.3.doc page 133
Resource Management Systems	All systems related to the Resource Management Domain as explained in Chap 7 in TAM model	TM Forum - TAM Application_Framework_R4_5__V4.3.doc pag 168
Service Performance Management System (PM System)	Service Performance Management Applications monitor, analyse, and report on the end-end service performance. This can include a Near Real Time, end-to-end view to ensure that each service is functioning correctly as well as a historical view. These applications build on the Resource Performance data and active end-end service performance test data to provide a view of a service. These applications provide a key input to determine the Quality of Service.	TM Forum - TAM Application_Framework_R4_5__V4.3.doc page 158
Service Inventory	Service Inventory Management represents the applications which contain and maintain information about the instances of services in a telecom organization. A Service Inventory application may store and manage any or all of the following entities: • Customer facing service (CFS) instances, and their attributes	TM Forum - TAM Application_Framework_R4_5__V4.3.doc page 135

	• Resource facing service (RFS) instances, and their attributes	
Resource Inventory	Resource Inventory applications manage information of all resources used to implement services and products. This application area is typically linked to various element management systems (i.e. building inventory for actual server, applications, network and resource assets) and resource inventory database systems which may or may not be combined with Service Inventory Application(s) or database(s). In addition, Resource management applications have a major role to play managing spare parts; passive resources including cable pairs and external plant and passive customer premises equipment. In addition, Resource Inventory applications are used to discover and manage underutilized or 'stranded' resources.	TM Forum - TAM Application_Framework_R4_5__V4.3.doc page 178
Configuration Management System	A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See Configuration Management Database, Service Knowledge Management System.	ITIL® V3 Glossary v3.1.24, 11 May 2007
Configuration Database (CMdb)	A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.	ITIL® V3 Glossary v3.1.24, 11 May 2007
Configuration Item (CI)	Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.	ITIL® V3 Glossary v3.1.24, 11 May 2007
Performance Indicator (PI)	Performance related data produced by Network Elements of wireline and wireless network. See lowest level of Figure 4.	TM Forum GB 917 Release 2.5
Key Performance Indicator (KPI)	KPI provides a measurement of a specific aspect of the performance of a service resource (network or non-network) or group of service resources of the same type. A KPI is restricted to a specific resource type.	TM Forum GB923 V3.0
Key Quality Indicator (KQI)	KQI provides a measurement of a specific aspect of the performance of the product, product components (services) or service elements and draw their data from a number of sources including the KPIs.	TM Forum GB923 V3.0
Service Accessibility	The ability of a service to be obtained, within specified	ITU-T Recommendation

Performance	tolerances and other given conditions, when requested by the user.	E.800
Service Retainability Performance	The ability of a service, once obtained, to continue to be provided under given conditions for a requested duration	ITU-T Recommendation E.800
Service Integrity Performance	The degree to which a service is provided without excessive impairments, once obtained.	ITU-T Recommendation E.800
Near Real Time	The term "Near Real Time" is a time constraint within which the described task/activity should take place; else the task/activity would be considered a failure. Whether the described task/activity could actually take place within the time constraint is dependent on factors such as complexity of task/activity involved, technology involved etc and should be examined on case by case basis. Near Real Time usually refers to a short period of time expressed in seconds or minutes.	
KPI Instance	A KPI Instance is used for defining an executable instance of the KPI template. A prerequisite to running the instance is that all input, including measurement values and constants must be defined. A KPI instance differs from a KPI template in that it is bound to specific attributes or parameters of network element and can be issued.	IBM Integrated Information Core, Version 1.5
KQI Instance	A KQI Instance is used for defining an executable instance of the KQI template. A prerequisite to running the instance is that all input, including KQI values and constants must be defined. A KQI instance differs from a KQI template in that it is bound to specific attributes or parameters of service and can be issued.	

7.3 Gap Analysis on existing previous work

Problem statement

We first have to consider that main problems arise not in managing single technologies, but the collection of data coming from several elements with different vendors, different technologies, etc. A gap analysis in this context has to keep into account the existence of this constraint as currently several SDOs have already addressed this problem. What has to be considered before doing this gap analysis is to define exactly the scenario and use cases that aim to cover our problem statement. For instance: 3GPP TR 32.831 V1.0.0, "Study on Alignment of 3GPP Performance Management and TM Forum Interface Program (TIP) Performance Management (Release 10)" [6]provides consistent and aligned PM and PM interfaces in 3GPP and TM Forum.

It:

- Identifies similarities and differences of the PM capabilities in 3GPP and TM Forum TIP PM BA;
- Proposes enhancements to 3GPP PM solutions for converged networks and to satisfy TM Forum TIP PM BA requirements;
- Identifies any required changes in the 3GPP specifications;
- Identifies any required changes in the TM Forum specifications (to be communicated to TM Forum).

Backwards compatibility of the PM IRP should be maintained as much as possible by re-using existing specifications to the maximum extent. The counter collected by each of the Network Elements (NE) and the definition of those are NE specific and there is no intention to harmonize those. However KPIs with a network view should be explored.

7.4 Scenarios/ Use Cases

According to statistics, web browsing and streaming would take up over 70% of all traffic flow, thus to ensure good experience of these services is of high priority from both operator and vendor's point of view. The following scenarios are applicable under the following general condition: As various technologies have developed over time, the monitoring of the performance of services provided over a network has to evolve accordingly. End-to-end performance indicators (PIs, KPIs, KQIs) are getting more and more important for the converged network where coexist 3G, 4G, copper and optical networks. These business scenarios cover both the wire-line and the wireless domain and future as well as existing technologies. Besides, OSS layers also impact the whole process of the performance indicators.

Business Scenarios	Scope	Additional Constraints/ Criticity
Video communication (BS1)	Data supplied from various network and service sources such as Media Servers, Transmission Network and acquired from either fixed or mobile terminals	Quality Perceived to be considered
Web browsing (BS2)	Data supplied from various network and service sources such as web portals	Short access time Integrity of web content
Walkman (BS3)	Walkman Service is one of mobile music services which is realized with music experience consumption platform and client music player software installed in the cell phone. This service can help users to listen to music online, download ringtones and songs.	For the download sub scenario , the user's behaviour would be browse songs list and select favourite song(s) or ringtone to download. Song(s) or ringtone download failure and slow download speeds of song(s) or ringtone are important customer perception.

Table 3: Business Scenario Decomposition

For sake of description we also introduce the following identification codes for KQI categories

KQI ID	KQI Category
A KQI	Service Accessibility Performance
R KQI	Service Retainability Performance
I KQI	Service Integrity Performance

Table 4: KQI Category

7.4.1 Video Communication (BS1)

The quality perceived by the customer is relevant more than the "simple" measurement throughput of data. There are two main class video service scenarios in networks at present:

- buffering video, e.g. YouTube.
- real time video, e.g. video call, video conference.

We focus on buffering video at the first place.
For buffering video, the quality of the streaming (e.g. picture, audio) itself is not a problem, the customer's perception usually focus on the accessibility, retainability and integrity related KQIs. From the service usage aspect, the following KQIs should be identified:

KQI Category	Key Quality Indicator	Definition
Service Accessibility Performance	Streaming Start Success Ratio	The Streaming Start Success Ratio describes the probability that the streaming can be started to play by the UE when requested by the user. At this point, the initial buffering process has been finished.
	Streaming Start Delay	The Streaming Start Delay describes the duration of a service access from requesting the stream at the portal until the streaming can be played at the UE
Service Integrity Performance	Streaming Stall Frequency	The Streaming Stall Frequency describes average times that the stream playing is stalled and the streaming goes into rebuffering mode during the whole streaming process.
	Average Streaming Stall Time	The Average Streaming Stall Time describes the average time that the every durations between a stream going into rebuffering mode and continuation of the stream
	Average Streaming Throughput	The Average Streaming Throughput describes the average download speed of the streaming data during the whole streaming process

Key Quality Indicator	Related KPI	Technology	PI

Streaming Start Success Ratio	[TS 32.450](eUTRAN): E-RAB Accessibility; [TS 32.410] (UTRAN): RAB Establishment Success Rate; RRC Connection Establishment Success Rate; Service Access Success Rate; PDP Context Activation Success Rate; [TS 32.455] (GERAN): EPS Attach Success Rate; Dedicated EPS Bearer Creation Success Rate; Service Request Success Rate;	Wireless network	[TS 32.425]: Attempted RRC connection establishments; Successful RRC connection establishments; Number of initial E-RABs attempted to setup; Number of initial E-RABs successfully established; [TS 32.426]: Attempted EPS attach procedures; Successful EPS attach procedures; [TS 32.405]: Attempted RAB establishments for PS domain; Successful RAB establishments without queuing for PS domain; Successful RAB establishments with queuing for PS domain; [TS 32.406]: Attempted GPRS attach procedures; Successful GPRS attach procedures;
Streaming Start Delay	[TS 32.455]: Dedicated Bearer Set-up Time by MME (Mean);	Wireless network	[TS 32.425]: RRC connection setup time; Mean E-RAB Setup time; Maximum E-RAB Setup time; [TS 32.405]: RAB PS connection set-up time (Mean); RAB PS connection set-up time (Maximum); RRC connection set-up time (Mean); RRC connection set-up time (Maximum); PDP Context set-up time; [TS 32.406]: PDP Context set-up time, initiated by MS; PDP Context set-up time, initiated by Network;

Streaming Stall Frequency	[TS 32.450]: E-RAB Retainability; [TS 32.410]: RAB Abnormal Release Rate; GERAN Service Abnormal Release Rate;	Wireless network	[TS 32.425]: DL PDCP SDU drop rate; DL PDCP SDU air interface loss rate; [TS 32.405]: Attempted RRC re-establishments; Failed RRC re-establishments;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate
Average Streaming Stall Time	[TS 32.450]: E-RAB Retainability; E-UTRAN IP Throughput; E-UTRAN IP Latency; [TS 32.410]: Percentage of Established RABs, TotalPS; [TS 32.455]: Mean Active Dedicated EPS Bearer Utilization;	Wireless network	[TS 32.425]: Average DL cell PDCP SDU bit-rate; Maximum DL cell PDCP SDU bit-rate; Average DL PDCP SDU delay; IP Throughput in DL; IP Latency in DL; [TS 32.426]: Number of incoming IP data packets on the S1-MME interface from eNodeB to MME; Number of outgoing IP data packets on the S1-MME interface from MME to eNodeB; [TS 32.406]: Number of outgoing GTP data packets on the Iu interface; Number of incoming GTP data packets on the Iu interface;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate
Average Streaming Throughput	[TS 32.450]: E-UTRAN IP Throughput; E-UTRAN IP Latency;	Wireless network	[TS 32.425]: IP Throughput in DL; IP Latency in DL; Average DL cell PDCP SDU bit-rate; Maximum DL cell PDCP SDU bit-rate;

			[TS 32.426]: Number of incoming IP data packets on the S1-MME interface from eNodeB to MME; Number of outgoing IP data packets on the S1-MME interface from MME to eNodeB; [TS 32.405]: Number of incoming IP data packets on the Gi interface; Number of outgoing IP data packets on the Gi interface; [TS 32.406]: Number of outgoing GTP data packets on the Iu interface; Number of incoming GTP data packets on the Iu interface;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate

Note: The above indicators are just some ones and not yet fully represented. What is to be done yet is to find in our services or in the literature some well represented examples of KQI and how they are related to KPI.

32. Each service KQI is impacted by more than one network KPI.
33. Not every network KPI will impact a service KQI.
34. Each service will have its own network KQI mapping.

7.4.2 Web Browsing (BS2)

In the networks, Web browsing is the one of most popular service and consumes much bandwidth. Http is the most widely used protocol; the following KQI description is based on the http process.

KQI Category	Key Quality Indicator	Definition
Service Accessibility Performance	Page Response Success Ratio	The Page Response Success Ratio describes the probability that the web page can be started to display by the UE when requested by the user.
	Page Response Delay	The Page Response Delay describes the duration of a service access from requesting the page at the UE until the

		page connection have been built.
Service Integrity Performance	Page Display Success Ratio	The Page Display Success Ratio describes the probability that the web page can be displayed successfully by the UE when request by the user.
	Page Display Delay	The Page Display Delay describes the duration of the time from the first data package is sent until the all page content is displayed successfully.
	Average Page Download Throughput	The Average Page Download Throughput describes the average download speed of the web page data during the whole web browsing process.

Key Quality Indicator	Related KPI	Technology	PI
Page Response Success Ratio	[TS 32.450] (eUTRAN): E-RAB Accessibility; [TS 32.410] (UTRAN): RAB Establishment Success Rate; RRC Connection Establishment Success Rate; Service Access Success Rate; PDP Context Activation Success Rate; [TS 32.455] (GERAN): EPS Attach Success Rate; Dedicated EPS Bearer Creation Success Rate; Service Request Success Rate;	Wireless network	[TS 32.425]: Attempted RRC connection establishments; Successful RRC connection establishments; Number of initial E-RABs attempted to setup; Number of initial E-RABs successfully established; [TS 32.426]: Attempted EPS attach procedures; Successful EPS attach procedures; [TS 32.405]: Attempted RAB establishments for PS domain; Successful RAB establishments without queuing for PS domain; Successful RAB establishments with queuing for PS domain; [TS 32.406]: Attempted GPRS attach procedures; Successful GPRS attach procedures;

Page Response Delay	[TS 32.455]: Dedicated Bearer Set-up Time by MME (Mean);	Wireless network	[TS 32.425]: RRC connection setup time; Mean E-RAB Setup time; Maximum E-RAB Setup time; [TS 32.405]: RAB PS connection set-up time (Mean); RAB PS connection set-up time (Maximum); RRC connection set-up time (Mean); RRC connection set-up time (Maximum); PDP Context set-up time; [TS 32.406]: PDP Context set-up time, initiated by MS; PDP Context set-up time, initiated by Network;
Page Display Success Ratio	[TS 32.450]: E-RAB Retainability; [TS 32.410]: RAB Abnormal Release Rate; GERAN Service Abnormal Release Rate;	Wireless network	[TS 32.425]: DL PDCP SDU drop rate; DL PDCP SDU air interface loss rate; [TS 32.405]: Attempted RRC re-establishments; Failed RRC re-establishments;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate
Page Display Delay	[TS 32.450]: E-RAB Retainability; E-UTRAN IP Throughput; E-UTRAN IP Latency; [TS 32.410]: Percentage of Established RABs, TotalPS; [TS 32.455]: Mean Active Dedicated EPS	Wireless network	[TS 32.425]: Average DL cell PDCP SDU bit-rate; Maximum DL cell PDCP SDU bit-rate; Average DL PDCP SDU delay; IP Throughput in DL; IP Latency in DL; [TS 32.426]: Number of incoming IP data packets on the S1-MME interface from eNodeB to MME;

	Bearer Utilization;		Number of outgoing IP data packets on the S1-MME interface from MME to eNodeB; [TS 32.406]: Number of outgoing GTP data packets on the Iu interface; Number of incoming GTP data packets on the Iu interface;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate
Average Page Download Throughput	[TS 32.450]: E-UTRAN IP Throughput; E-UTRAN IP Latency;	Wireless network	[TS 32.425]: IP Throughput in DL; IP Latency in DL; Average DL cell PDCP SDU bit-rate; Maximum DL cell PDCP SDU bit-rate; [TS 32.426]: Number of incoming IP data packets on the S1-MME interface from eNodeB to MME; Number of outgoing IP data packets on the S1-MME interface from MME to eNodeB; [TS 32.405]: Number of incoming IP data packets on the Gi interface; Number of outgoing IP data packets on the Gi interface; [TS 32.406]: Number of outgoing GTP data packets on the Iu interface; Number of incoming GTP data packets on the Iu interface;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate

7.4.3 Walkman (BS3)

Walkman Service is one of mobile music services which is realized with music experience consumption platform and client music player software installed in the cell phone. This service can help users to listen to music online, download ringtones and songs. The scenario of the service is as following.

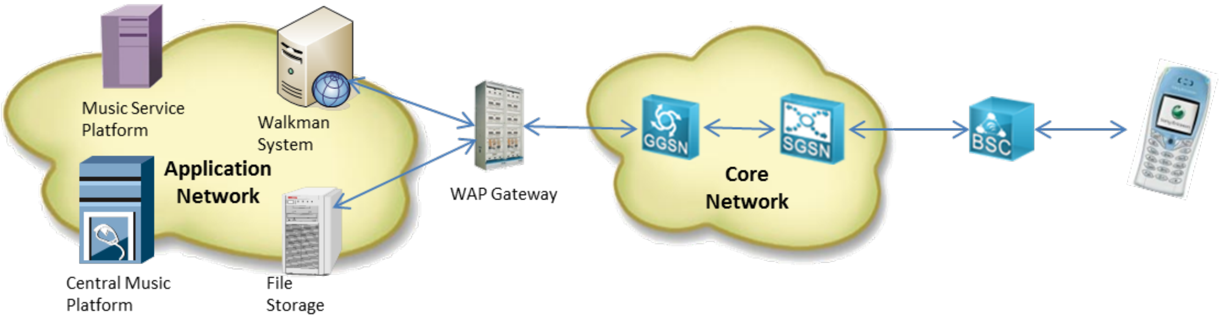


Figure 19: Network Topology for Walkman Business Scenario

- Users open Walkman client application installed in mobile phone and login Walkman System through core network and WAP gateway.
- Users browse songs list and select favourite song(s) or ringtone to download. Walkman System inquires of Central Music Platform the service policy and presents the result information of billing policy and prices to client application. Users confirm it, then client application gets ready to download song(s) or ringtone.
- Walkman System requests the download address from File Storage and returns the download address to client application. Client application starts to download song(s) and/or ringtone from File Storage with the download address. The service supports breakpoint resume.
- After the completion of song(s) and/or ringtone download, client application will return the success status to Walkman System. Then Walkman System notifies Music Service Platform to send the copyright of songs and/or ringtone to client application then charging begins.

Identified sub scenarios for Walkman use case are:

ID	SubScenario	Service Attribute	Key Quality Indicator
BS3.2	Download sub scenario	Download music is success, and not often failure.	Download Success Rate Data Rate
BS3.3	Audio Streaming	Audio stream is integrity, and not lose some tones or paused.	Data Error Rate

Table 5: SubScenarios of Walkman

7.4.3.1 Download sub scenario

For the download sub scenario, the user's behaviour would be browse songs list and select favourite song(s) or ringtone to download. Song(s) or ringtone download failure and slow download speeds of song(s) or ringtone are important customer perception. It involves wireless network, core network, WAP gateway, application network, Central Music Platform and Walkman System.

KQI Category	Key Quality Indicator	Definition

Service Accessibility Performance	File Download Response Success Rate	The Download Response Success Rate describes the probability that the user can set up the transmission successfully for download when requested by the user.
	File Download Response Delay	The Download Response Delay describes the download response duration from requesting the download at the portal until the transmission is setup successfully.
Service Integrity Performance	File Download Success Rate	The Download Success Rate describes the probability that the user can download the whole songs data successfully from the Walkman system.
	File Data Rate	The Data Rate describes the bit-rate of transmission that songs download from the Walkman system.
	File Download Delay	The Download Delay describes the download duration from the first data packet send to the UE until the whole songs data is download to the UE.

Key Quality Indicator	Related KPI	Technology	PI
File Download Response Success Rate	[TS 32.450]: E-RAB Accessibility; [TS 32.410]: RAB Establishment Success Rate; RRC Connection Establishment Success Rate; Service Access Success Rate; PDP Context Activation Success Rate; [TS 32.455]: EPS Attach Success	Wireless network	[TS 32.425]: Attempted RRC connection establishments; Successful RRC connection establishments; Number of initial E-RABs attempted to setup; Number of initial E-RABs successfully established; [TS 32.426]: Attempted EPS attach procedures; Successful EPS attach procedures; [TS 32.405]: Attempted RAB establishments for PS domain;

	Rate; Dedicated EPS Bearer Creation Success Rate; Service Request Success Rate;		Successful RAB establishments without queuing for PS domain; Successful RAB establishments with queuing for PS domain; [TS 32.406]: Attempted GPRS attach procedures; Successful GPRS attach procedures;
File Download Response Delay	[TS 32.455]: Dedicated Bearer Set-up Time by MME (Mean);	Wireless network	[TS 32.425]: RRC connection setup time; Mean E-RAB Setup time; Maximum E-RAB Setup time; [TS 32.405]: RAB PS connection set-up time (Mean); RAB PS connection set-up time (Maximum); RRC connection set-up time (Mean); RRC connection set-up time (Maximum); PDP Context set-up time; [TS 32.406]: PDP Context set-up time, initiated by MS; PDP Context set-up time, initiated by Network;
File Download Success Rate	[TS 32.450]: E-RAB Retainability; [TS 32.410]: RAB Abnormal Release Rate; GERAN Service Abnormal Release Rate;	Wireless network	[TS 32.425]: DL PDCP SDU drop rate; DL PDCP SDU air interface loss rate; [TS 32.405]: Attempted RRC re-establishments; Failed RRC re-establishments;
	PON/ONU Mean Time between Resynchronizations	Wireline network	Mean Time between Resynchronizations(MTBR)
File Download Delay	[TS 32.450]: E-UTRAN IP Throughput;	Wireless network	[TS 32.425]: Average DL cell PDCP SDU bit-rate;

	E-UTRAN IP Latency; Percentage of Established RABs, TotalPS; [TS 32.455]: Mean Active Dedicated EPS Bearer Utilization;		Maximum DL cell PDCP SDU bit-rate; Average DL PDCP SDU delay; DL PDCP SDU drop rate; DL PDCP SDU air interface loss rate; IP Throughput in DL; IP Latency in DL;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate
File Data Rate	[TS 32.450]: E-UTRAN IP Throughput; E-UTRAN IP Latency; [TS 32.410]: Percentage of Established RABs, TotalPS; [TS 32.455]: Mean Active Dedicated EPS Bearer Utilization;	Wireless network	[TS 32.425]: IP Throughput in DL; IP Latency in DL; Average DL cell PDCP SDU bit-rate; Maximum DL cell PDCP SDU bit-rate; Average DL PDCP SDU delay; DL PDCP SDU drop rate; DL PDCP SDU air interface loss rate;
	PON/ONU Upstream/Downstream Rate	Wireline network	PON/ONU Upstream/Downstream Rate

7.4.3.2 Audio Streaming sub scenario

For the audio streaming sub scenario, it has two main sub scenarios: buffering audio (the audio streaming data have been existed in the server) and real time audio streaming. It involves wireless network, core network, WAP gateway, application network, Central Music Platform and Walkman System.

Key Quality Indicator	KQI Category	Related KPI	KPI description	Technology	PI
Data Error Rate	Integrity	Data error rate per service	This KPI is obtained by network for each user from user end to application server end.	GSM/UMTS/LTE/WLAN	Data error rate per service per user.

		Packet Loss Ratio	This KPI is obtained by The interface of mobile boradband Network Packet Loss Ratio	MobileBroadBand	Packet Loss Ratio(%)
Delay	Integrity	Average Delay	This KPI is obtained by the interface of mobile boradband Network Average Delay	MobileBroadBand	Avg.Delay(ms)
		Minimum Delay	This KPI is obtained by the interface of mobile boradband Network Minimum Delay	MobileBroadBand	Min.Delay(ms)
		Maximum Delay	This KPI is obtained by the interface of mobile boradband Network Maximum Delay	MobileBroadBand	Max.Delay(ms)
Jitter	Integrity	Average Jitter	This KPI is obtained by the interface of mobile boradband Network Average Jitter	MobileBroadBand	Avg. Jitter (ms)

Table 6: KQIs and Related KPIs of Audio Streaming Sub Scenario

7.5 Requirements

7.5.1 Generic Requirements

The main actor analyzed for the Business scenarios above is the Performance Management System and their elements EMS, NMS, NEs. Following requirements would like to cover use cases that may cover both the wireline and the wireless domain and future as well as existing technologies. KQI shall be technology and network agnostic.

REQ-PM (1)

Identifier: REQ-PM (1)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs, OSS vendors**	**Context: OSS**
Title : Independent KQI				
Description: KQI should be network type, technology, and vendor independent.				
Rationale: The service can be provided on heterogeneous networks with fixed devices or mobile devices moving through them. It is necessary to ensure a suitable level of service independently from the context. This requirement relates all scenarios because it would allow measuring the quality when the service is accessed from either fixed network and mobile network.				

REQ-PM (2)

Identifier: REQ-PM (2)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs, Equipment vendors, OSS vendors**	**Context: EMS, OSS**

Title : Independent KPI
Description: KPI used to build KQI should be as much as possible network type, technology, and vendor independent.
Rationale: The service can be provided on heterogeneous networks with fixed devices or mobile devices moving through them. It is necessary to ensure a suitable level of service independently from the context. This requirement relates all scenarios because it would allow measuring the quality when the service is accessed from either fixed network or mobile network.

REQ-PM (3)

Identifier: REQ-PM (3)	Rel. Use case id :	Priority:	Addressed to: SDOs, Equipment vendors	Context: EMS
Title : Homogeneity of PIs				
Description: PIs shall be defined where relevant (applicable to wireline and wireless technology) in similar ways in every technology in order to allow KPIs to be as much as possible technology independent (according to REQ-PM-1)				
Rationale: PIs are already existing in each technology, but in order to compute KPIs it has to be possible to mix similar PIs coming from different technologies to produce common KPIs necessary for a global service KQI. In design of new network elements, it needs to take consideration existence of similar PIs in other technologies. This requirement addresses newly introduced NEs either in the fixed and mobile networks. And do not expect changes are performed on existing ones. It also addresses all the above described scenarios.				

REQ-PM (4)

Identifier: REQ-PM (4)	Rel. Use case id :	Priority:	Addressed to: SDOs, OSS vendors	Context: OSS
Title : KQIs derivation				
Description: In order to ensure performance management of services deployed jointly on different technology domains, it shall be possible to produce KQIs based on KPIs in Near Real Time from different technologies.				
Rationale: It might be necessary to collect PI(s) from different technology domains to produce/calculate KPIs and KQIs in Near Real Time in order to detect violation of agreed Service Level. It also addresses all the above described scenarios.				

7.5.2 General Requirements

According to ITU-T Recommendation E.800, six Quality of Service categories are defined as follows:

- Service Support Performance: The ability of an organization to provide a service and assist in its utilization.
- Service Operability Performance: The ability of a service to be successfully and easily operated by a user.

- **Service Accessibility Performance**: The ability of a service to be obtained, within specified tolerances and other given conditions, when requested by the user.
- **Service Retainability Performance**: The ability of a service, once obtained, to continue to be provided under given conditions for a requested duration.
- **Service Integrity Performance**: The degree to which a service is provided without excessive impairments, once obtained.
- Service Security Performance: The protection provided against unauthorized monitoring, fraudulent use, malicious impairment, misuse, human mistake and natural disaster.

According to the above categories, it seems suitable to ensure that related requirements on KQI/ KPI are impacted by the presence of several network technologies (fixed, mobile, new, old tech.,) This suggests to introduce a requirements for each of the above categories that may suffer different impact from the heterogeneous scenarios we are facing.

REQ-PM (5)

Identifier: REQ-PM (5)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs, OSS vendors**	**Context: OSS**
Title : Genericity of Accessibility KQI				
Description: All KQIs related to Accessibility shall be technology, network type independent. These should also be SDOs , vendors and operators independent.				
Rationale: In providing services to end-users, the first step is to get access to the service, independently from the network or technology used by the client. First after access to the service has been performed, the service can be used. If an accessibility measurement is not considered OK, then the network operator cannot investigate which steps that are required to improve the accessibility towards their customers. For example, the current wireless communication technologies contain GSM, UMTS, LTE, WLAN and etc., which have different features. So the performance measurements of accessibility for different wireless networks vary. The same for access from fixed network, For instance, performance measurement of RRC connection establishment and RAB establishment can reflect the accessibility of UMTS network. In case of Services relying on just one technology it is not necessary to have KQI independent from the technology.				

REQ-PM (6)

Identifier: REQ-PM (6)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs, OSS vendors**	**Context: OSS**
Title : Genericity of Retainability KQI				
Description: All KQIs related to Retainability shall be technology, network type independent. These should also be SDOs, vendors and operators independent.				
Rationale: When a service is used, it is important that it is not interrupted or aborted. If a retainability measurement is not considered OK, then the network operator cannot investigate which steps that are required to improve the retainability towards their customers. This measurement should be used for observing the impact of telecommunications network on end-users service retainability. For example, the current wireless communication technologies contain GSM, UMTS, LTE, WLAN and etc., which have different features. So the performance measurements of retainability for different wireless networks vary. For instance, performance measurement of RAB abnormal release could reflect the retainability of UMTS network directly. In case of Services relying on just one technology it is not necessary to have KQI independent from the technology.				

REQ-PM (7)

Identifier: REQ-PM (7)	**Rel. Use case id :**	**Priority:**	**Addressed to:**	**Context: OSS**

			SDOs, OSS vendors	
Title : Genericity of Integrity KQI				
Description: All KQIs related to Integrity shall be technology, network type independent. These shall also be SDOs, vendors and operators independent.				
Rationale: When a service is used, it is important that the quality of the service is acceptable. If an integrity measurement is not considered OK, then the network operator cannot investigate which steps that are required to improve the quality provided to their customers. This measurement should be used for observing the impact of telecommunications network on end-users service integrity. For example the current wireless communication technologies contain GSM, UMTS, LTE, WLAN and etc., which have different features. So the performance measurements of integrity for different wireless networks vary. For instance, performance measurement of E-UTRAN IP throughput could reflect the integrity of LTE network directly. In case of Services relying on just one technology it is not necessary to have KQI independent from the technology.				

7.5.3 High Level Functional Requirements

REQ-PM (8)

Identifier: REQ-PM (8)	Rel. Use case id :	Priority:	Addressed to: SDOs	Context: Interface
Title : Unified collection mechanism (standardization of NBI)				
Description: The PIs shall be collected by NMS via EMS from different types of network elements in a uniform way.				
Rationale: The same collecting approach (same processes, same tools, …) has to be used to collect Performance information from EMS to NMS for all Network Element types to ensure the possibility of collecting information efficiently for the proposed service, independently from the network , vendor, provider. For example in scenarios above, the file name that contains PI information and the method to get the performance file should be specified in same way for all kinds of NEs from wireline and wireless networks.				

REQ-PM (9)

Identifier: REQ-PM (9)	Rel. Use case id :	Priority:	Addressed to: SDOs	Context: Interface
Title : Homogeneity of PIs administration with respect to network type and technology (standardization of NBI)				
Description: Measurement jobs shall be done for collecting performance PI values in a converged management environment. The parameters of the job (e. g. frequency, timing,) shall be defined taking into account the presence of several technologies and network types.				
Rationale: Strictly associated to the need of a Uniform Collection Mechanism (Req. REQ-PM-8) also attributes (same scales for instance) need homogeneity in spite of the technology, to ensure their mixing in case of services provided contemporaneously on several networks and / or comparison. For example in the scenarios above, measurement job administration including addition, modification and deletion of attributes and jobs should be done in the same method.				

REQ-PM (10)

Identifier: REQ-PM (10)	Rel. Use case id :	Priority:	Addressed to: SDOs	Context: Architecture, Interface
Title : Transfer of PIs				
Description: It shall be possible to transfer PIs in the following ways: • from NE to EMS and then from EMS to NMS via North Bound Interface • from NEs to NMS • from NMS to NMS • from NMS to SMS				
Rationale: It is important to ensure the transfer of performance indicators between the various OSS layers: the PIs collected from the Network layer Element managers, should be passed to OSS Performance Management systems, and then reported to newly evolved Service Quality and Customer Experience management systems. In the case of some NEs without EMS, such as WLAN, router and switch etc. PIs produced from them should be transferred directly to NMS. All this should be done with maximum flexibility, allowing efficient collection through all technologies, harmonizing the existent in each single domain. For example in the scenarios above, for NEs with OMC, PIs should be transferred from NE to EMS then from EMS to NMS by NBI. For NEs without OMC like WLAN, PIs should be transferred directly from NEs to NMS.				

Identifier: REQ-PM (10)	Rel. Use case id :	Priority:	Addressed to: SDOs	Context: Architecture, Interface
Title : Transfer of KPIs				
Description: It shall be possible to transfer KPIs in the following ways: • from NMS to NMS • from NMS to SMS				
Rationale: It is important to ensure the transfer of key performance indicators between the various OSS layers: NMS, SMS.				

REQ-PM (11)

Identifier: REQ-PM (11)	Rel. Use case id :	Priority:	Addressed to: SDOs	Context: Architecture
Title : Unified templates for definition of PIs/KPIs				
Description: A single template shall be defined for definition of PIs, and another one for KPIs, covering different services in converged management environment. The KPI template should at least be based on the PI template. If possible, the template for PI and KPI should be common. The template shall include among others the name, formulation, type of measurements				
Rationale: Strictly associated to the need of a uniform collection mechanism (Req. REQ-PM-7) here it is stressed the idea that it is not only necessary to have the same tools and processes for the collection of PIs/KPIs across the network but also the availability of the same templates are a critical aspect that needs to be addressed for efficient collection of KPIs and calculation of the related				

Quality Indicators As far as possible PIs should be the same among vendors, to allow easier KPIs computation. This requirement relates to all scenarios above, because it would allow the availability of the same template when the service or services are accessed from either mobile network or fixed network. KQIs are to be the same for both accesses.

REQ-PM (12)

Identifier: REQ-PM (12)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: Interface**
Title : Unified performance data i.e. PI and KPI exchange format used by EMS and NMS				
Description: The performance data i.e. PI and KPI shall have one standard encoding format (e.g. output file format- independent from vendors and technology)				
Rationale: Note: add a reference from REQ-PM-8 and REQ-PM-10a to REQ-PM-12. . It needs one standard encoding format to output Performance Data to NMS independent from vendor and technology either in fixed networks or mobile networks.				

REQ-PM (13)

Identifier: REQ-PM (13)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: Interface**
Title : Unified exchange format for KPIs and KQIs at OSS/BSS Level				
Description: A common, harmonized and consistent exchange format for KPI (if it is calculated in OSS) or KQI agreed between interworking OSS/ BSS applications/areas for performance and service quality management shall be defined. Service PM system shall be able to keep and share quality information with all applications supporting SLA management independently from the network technology used and vendor.				
Rationale: It is close to REQ-PM-12 but related to the exchange of information among OSS /BSS applications. Whether a single format can be defined for REQ-PM-12 and REQ-PM-13 will be addressed when defining the solution. This requirement relates all scenarios above because the quality information should be shared to support SLA management independently from technology and vendor.				

REQ-PM (14)

Identifier: REQ-PM (14)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: OSS**
Title : Multi-technology OSS Performance Management systems				
Description: OSS Performance Management system shall be able to manage KQIs/KPIs/PIs for both fixed and mobile networks, whatever network technology is used.				
Rationale: Also Performance Management Systems need to be able to manage data coming from several technologies to produce SQA metrics to measure SLA compliancy.				

This requirement relates all scenarios above because OSS Performance Management system has the ability to manage performance data covering both fixed and mobile networks to support SLA management independently from technology and vendor.

REQ-PM (15)

Identifier: REQ-PM (15)	**Rel. Use case id :**	**Priority:**	**Addressed to: Equipment vendors**	**Context: EMS**
Title : EMS as a collector to provide Near Real Time PIs to NMS				
Description: EMS shall be able to provide PIs to NMS in Near Real Time to enable NMS 1. to calculate KPIs, if necessary, from the PIs 2. to forward KPIs to Service Management System				
Rationale: It is necessary to feed NMS with PIs in Near Real Time so that NMS can calculate KPIs to monitor the network. This requirement relates all scenarios above because it should be ensured that NMS has ability to obtain performance data without delay to monitor network performance and report to Service Management System.				

REQ-PM (16)

Identifier: REQ-PM (16)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: OSS**
Title : NMS as a collector provides Near Real Time KPIs to Service Management System				
Description: NMS shall be able to provide KPIs to Service Management System in Near Real Time to enable Service Management System 1. to calculate KQIs from the KPIs 2. to enable Service Management System to verify SLA compliance				
Rationale: It is necessary to feed SMS with KPIs in Near Real Time so that SMS can check SLA fulfilment. This requirement relates all scenarios above because it should be ensured that Service Management System has ability to obtain quality information without delay to monitor service quality and verify SLA compliance.				

REQ-PM (17)

Identifier: REQ-PM (17)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: Architecture, Interface**
Title : Relationship between PI values and related resource instances				
Description: It shall be possible to keep relation between PI values and the related resource instances for all technologies, vendors, and network types.				
Rationale:				

This is necessary to ensure the exact identification of the resources impacted by possible lack of performance in multi technology service provisioning. This requirement relates all scenarios above because PIs should conduct network performance assessment and perform various aspects of trend analysis against specific resource instance, including error rate and cause analysis and resource degradation.

REQ-PM (18)

Identifier: REQ-PM (18)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: Architecture, Interface**
Title : Relationship between KPI values and related resource instances				
Description: It shall be possible to keep relation between KPI values and the related resource instances for all technologies, vendors, and network types.				
Rationale: This is necessary to ensure the exact identification of the Resources impacted by possible lack of performance in multi technology service provisioning. This requirement relates all scenarios above because KPIs should collect, correlate, consolidate, and validate various performance statistics against specific resource instance.				

REQ-PM (19)

Identifier: REQ-PM (19)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: Architecture, OSS**
Title : KPIs values storage				
Description: KPIs values have to be stored at OSS level e.g. in a Database at level of the PM System allowing easy extraction and correlation among technologies, network type and vendors data. KPI values have to be kept in the database to a required period according to the O&M requirements and SLA.These KPI are the ones to be considered when designing KQIs and SLA for newly defined services				
Rationale: It is necessary to save and retrieve historical data related to the Performance of the Resources Independently from the technology, vendor, and network type to be able to measure the historical evolution of the Quality of the Service. This requirement relates all scenarios above because KPIs should collect, correlate, consolidate, validate and evaluate various performance data for the service quality management and SLA compliance.				

REQ-PM (20)

Identifier: REQ-PM (20)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: Architecture, OSS**

Title : Relationship between KQI values and related service instances				
Description: A given service has associated some quality indicators (KQI) and the relation has to be kept to be able to associate the service to the indicators, eventually distributed according different levels of quality for the service (Silver, Gold, Platinum)				
Rationale: It has to be possible to correlate Service Instances to related Quality indicators to be able to produce SLA fulfilment indicators for each given service instance. This can be obtained through suitable correlation between KQIs and services. This requirement relates all scenarios above because KQIs should collect, correlate, consolidate, and validate various quality statistics against specific service instance.				

REQ-PM (21)

Identifier: REQ-PM (21)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: Architecture, OSS**
Title : KQI values storage				
Description: Quality indicators for a service are defined within the Service Design process and stored in a database at OSS level.. These KQI are the ones to be measured using the converged KPIs.				
Rationale: This requirement relates all scenarios above because KQIs should be ensured to output the accurate value without time and location effects even supporting several applications.				

REQ-PM (22)

Identifier: REQ-PM (22)	**Rel. Use case id :**	**Priority:**	**Addressed to: OSS vendors**	**Context: Architecture, OSS**
Title : Relationship among Service Instances and Resource Instances				
Description: OSS Inventory management system has to keep relations among all Service Instances and related resource instances. Instantiated service to a specific customer uses a specific set of resources that have to be known when ensuring SLA fulfillment.				
Rationale: This requirement relates all scenarios above. KQIs provide a measure of specific aspect of a service and are based on a number of sources including the KPIs. KPIs provide a measurement of a specific aspect of the performance of a service resource or group of service resources of the same type. These are usually computed on the basis of relationship among service instances and resource instances.				

REQ-PM (23)

Identifier: REQ-PM (23)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: Architecture, Interface**
Title: KPIs have to be made available for the adjustment of the Network configuration (e.g. SON functionalities)				
Description: The above defined Exchange format <reference> shall be used to make KPIs available to OSS configuration management system (e.g. SON functionalities) in a Near Real Time mode, to re-configure the NEs if necessary to ensure SLA fulfillment				

Rationale:
Performance Management provides constant monitoring of the performance of networks to evaluate and report on the behaviour of telecommunication equipment and the effectiveness of the network, which helps to support the opening up and the deployment or reconfiguration of services with high levels of service availability for customers. This requirement relates to Walkman scenario. When a service is used it is important that it is not interrupted or aborted. If a retainability measurement is not considered OK, then it is required to improve the retainability towards customers. This measurement should be shared to OSS configuration management system for observing the impact of telecommunications network on end-users service retainability and to re-configure the NEs if necessary. For instance, performance measurement of RAB abnormal release could reflect the retainability of UMTS network directly.

REQ-PM (24)

Identifier: REQ-PM (24)	**Rel. Use case id :**	**Priority:**	**Addressed to: SDOs**	**Context: OSS**
Title: the KQI definition should cover the most used typical services in the networks.				
Description: The KQI definition shall cover the most used typical services in the networks, e.g. video, web browsing, file download, email.				
Rationale: All the application scenarios are composed by several typical services, if the KQIs of the services which are used in the scenario are defined, the KQIs of the application scenario can be derived from the basic typical services KQIs.				

7.5.4 Other

<For each requirement introduce a table like the following one clearly identifying each entry to allow cross traceability with Use Cases >

Identifier:	**Rel. Use case id :**	**Priority:**
Title :		
Description:		
Rationale:		

7.6 Performance Management DETAILED INFORMATION

Fehler! Verweisquelle konnte nicht gefunden werden. is showing a framework intended to provide a general guide to the factors which contribute collectively to the overall quality of service as perceived by the user of a telecommunication service. The terms in the diagram can be thought of as generally applying either to the quality of service levels actually achieved in practice, to objectives which represent quality of service goals, or to requirements which reflect design specifications. The figure is structured to show that one quality of service factor can depend on a number of others. It is important to note – although it is not explicitly stated in any of the definitions contained in this document – that the value of a characteristic measure of a particular factor may depend directly on corresponding values of other factors which contribute to it. This necessitates, whenever the value of a measure is given, that all of the conditions having an impact on that value be clearly stated.

The essential aspect of the global evaluation of a service is the opinion of the users of the service. The result of this evaluation expresses the users' degrees of satisfaction. This Recommendation provides a framework for:

- The quality of service concept;
- Relating quality of service and network performance;
- A set of performance measures.

It is obvious that a service can be used only if it is provided, and it is desirable that the provider has a detailed knowledge about the quality of the offered service. From the provider's viewpoint, network performance is a concept by which network characteristics can be defined, measured and controlled to achieve a satisfactory level of service quality. It is up to the Service Provider to combine different network performance parameters in such a way that the economic requirements of the Service Provider as well as the satisfaction of the user are both fulfilled.

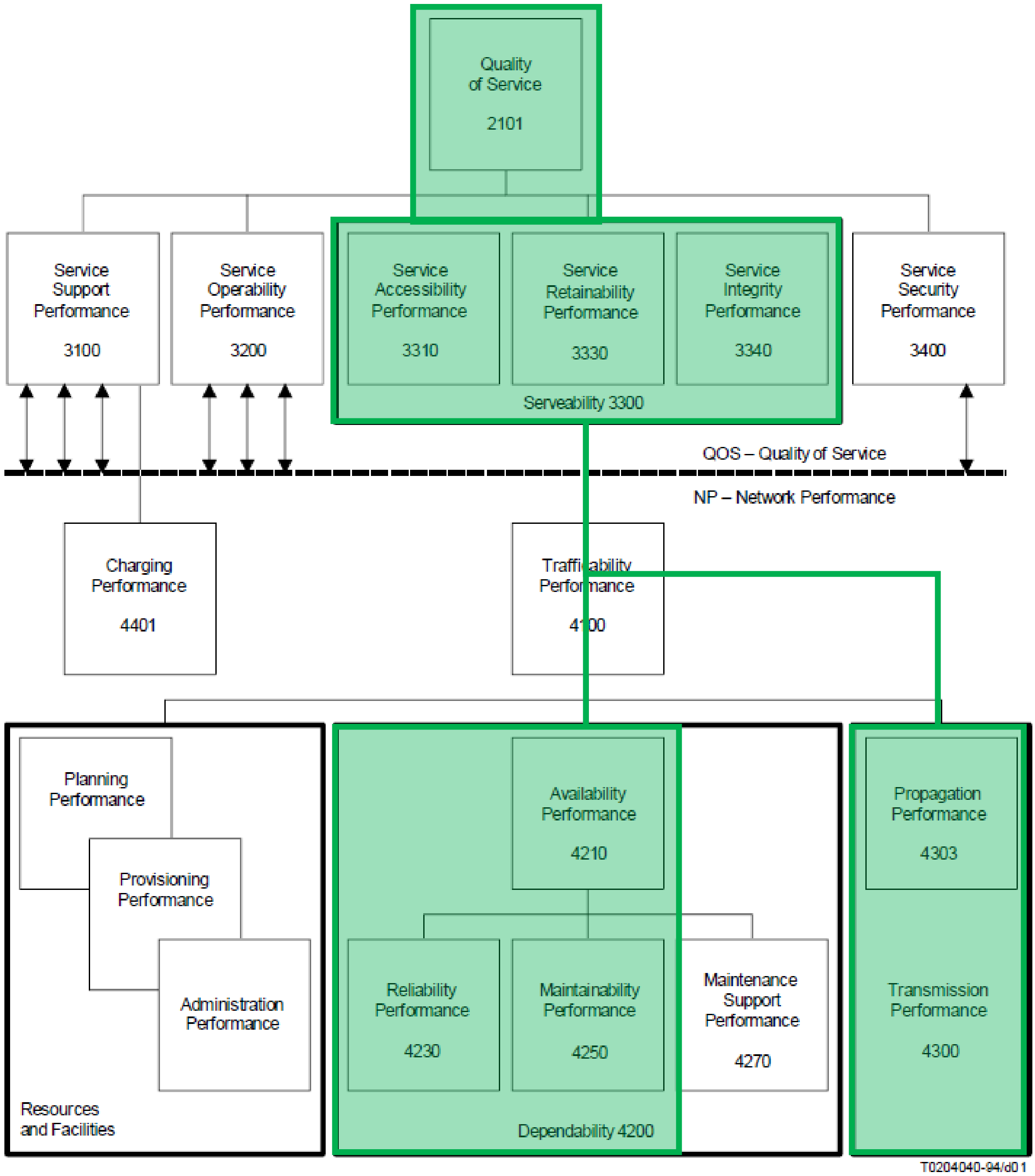


Figure 20: Performance Concepts from ITU-T E800 doc

NOTES

1. Each concept may affect the one above collectively or individually.
2. For the sake of clarity not all relationships are indicated, though they may be implied on the figure.

7.6.1 Key Quality Indicators (KQIs)

KQIs provide a measurement of a specific aspect of the performance of the product, product components (services) or service elements and draw their data from a number of sources including the KPIs. There are two main types of KQI.

- The product KQI, which is required to monitor the quality of product offered to the end-user.
- The service KQI, which is focused on monitoring the performance of individual product components (services).

Product KQIs will derive some of their data from the Service KQIs, which are obtained by aggregating multiple KPIs. A product consists of a number of services which may be either network or non-network based. Services such as Voice, SMS and WAP are network derived, while itemized billing, customer care and insurance have little dependence on network resource. Correspondingly, KQIs can be sorted to network and non-network KQIs. In this document, service KQIs are only studied in their network related aspects. The KQIs that we want to consider in the present document are the severability ones as described in ITU-T Recommendation E.800 i.e. the ones that provide the ability of a service to be obtained – within specified tolerances and other given conditions – when requested by the user and continue to be provided without excessive impairment for a requested duration.

- Accessibility: The ability of a service to be obtained, within specified tolerances and other given conditions, when requested by the user.
- Retainability: The ability of a service, once obtained, to continue to be provided under given conditions for a requested duration.
- Integrity: The degree to which a service is provided without excessive impairments, once obtained.

7.6.2 Key performance indicators (KPIs)

KPIs provide a measurement of a specific aspect of the performance of a service resource (network or non-network) or group of service resources of the same type. A KPI is restricted to a specific resource type. In this document, we are focusing on KPIs related to the above mentioned KQIs, which are the dependability ones as described in ITU-T Recommendation E.800 except for Maintenance Support Performance ones i. e. the ones that provide the ability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided. In addition, we focus Mobility as well.

- Reliability: The ability of an item to perform a required function under given conditions for a given time interval.
- Maintainability: The ability of an item under stated conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.
- Mobility: it contains the Handover related KPIs [7]

7.6.3 Relation among KPIs, KQIs and PIs from specific Technology Network Elements (NEs)

From the NEs, the network performance data is aggregated to provide KPIs that provide an indication of service resource performance. The KPIs are then used to produce the Service KQIs that are the key indicators of the service element performance. Service KQIs are then used as the primary input for management of internal or supplier/ partner SLAs that calculate actual service delivery quality against design targets or in the case of supplier/ partner, contractual agreements. Service KQIs provide the main source of data for the Product KQIs that are required to manage product quality and support the contractual SLAs with the customer. The key indicator hierarchy is illustrated in following picture. Different KPIs are defined for different technologies, which causes the need to make these indicators homogeneous for producing quality indicators for services provided through several technologies at the same time or in alternative.

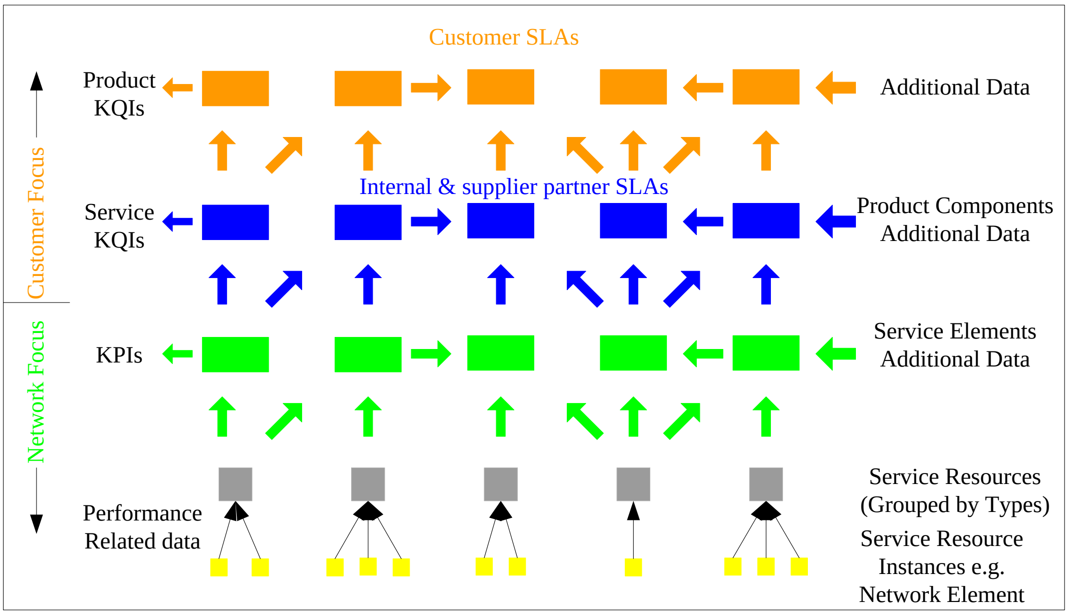


Figure 21: Key Indicator Hierarchy (see in TM Forum GB917)

NOTES

1. Performance Related data in the Figure is referred as Performance Indicators (PIs) in other part of the document.

Service and network performance are mainly indicated by KQIs and KPIs. KQIs provide a measure of specific aspect of a service and are based on a number of sources including the KPIs. KPIs provide a measurement of a specific aspect of the performance of a service resource (network or non-network) or group of service resources of the same type. These are usually computed on the basis of Performance Indicators (PIs), which are indicated by Performance Related data in the Figure above, collected from Network Elements impacted by specific service provisioning. Service Performance KQIs are user-oriented while Network Performance KPIs are network provider and technology-oriented. Network Performance KPIs together with Service Performance KQIs need to be identified to capture a more accurate picture of the customer's perception. Computation of service performance is based on network-related KPIs and non-network related KQIs. Network performance KPIs are usually defined in terms of the number and/ or intensity of network performance event occurrences during a specified time interval. The values of these KPIs can be computed from event information (e. g. counters) and reported to the customer service.

Criteria to define Network and Service performance KQIs and KPIs:

(1) Provide concrete repeatable measurements in well-defined quantities without subjective interpretation.
(2) Be useful to users and service providers in understanding the performance they experience or provide.
(3) Not exhibit a bias for services supported by one network technology as opposed to another technology.
(4) Be measurable via a process acceptable to service providers, their customers and, in some cases, outside testing agencies while avoiding including artificial performance goals.
(5) Be useful as a specification in contractual documents to help customers with high performance requirements purchase the level of service they need.
(6) Be useful for publication in datasheets.
(7) Be capable of measuring one provider independent of all others.
(8) Support a diagnostic mode that can be used to sectionalize or identify the degradation contribution in a long multi-hop, multi-provider path.

The big challenge in this study is not in the identification of the KPIs necessary to derive suitable KQI, since a great deal of work has already been performed by several SDOs, but in understanding how different technology PIs can be mixed together to provide multi-technology/ convergent KPIs and thus derive KQIs

7.6.4 Prioritization (e.g. priorities table, list, etc…)

<TbD>

7.6.5 Vendor Constraints

<TbD>

7.6.6 <Other if/where applicable>

<TbD>

7.6.7 Conclusions/Recommendations

<TbD>

7.7 Appendix 1 - STANDARDS Related to Video Communication

There are following existing standards which are related to video communication:

- 4Q '11: HDVC group defined two specifications for IMS-based point-to-point and conferencing video communication
  - UNI specification: support for several access networks: xDSL, Ethernet, LTE. Using IR.92 (VoLTE) and IR.94 (video over LTE) as a base.
  - NNI specification: built by profiling 3GPP TS 29.165 for video service.
- 3GPP is specifying the use cases and requirements for IMS-Based telepresence conference as extensions of existing IMS multi-media conference services and as applicable for different kinds of devices (mobile, fixed, etc.).
- OTTs, with WebRTC aim at deploying voice and video services through web coding. All the necessary for web conversational services will be natively integrated in web browsers, without the need for any other native application or plug-ins.
- TM Forum: GB938_Video_Over_IP_Application, describe how to define a standard way of implementing SLA for Video over IP services.
- 3GPP SA4: TR26.944 End-to-end multimedia services performance metrics.
- ETSI: TS102.250 (PartI~PartVII) Speech and multimedia Transmission Quality (STQ); QoS aspects for popular services in mobile networks.
- ITU: J.144：Objective perceptual video quality measurement techniques for digital cable television in the presence of a full reference;
  - J.241：Extended video procedures and control signals for ITU-T H.300-series terminals
  - P.MSW：Parametric non-intrusive assessment of audiovisual media streaming quality - lower resolution application area

7.8 Appendix 2 - Architectural and Framework Standards: The TMN/FCAPS Model (ITU-T)

From Ralf Wolter, “Network Management: Accounting and Performance Strategies”, Benoit Claise, CCIE® No. 2868

The ITU-T introduced the term Telecommunications Management Network (TMN) to describe a separate network that has interfaces to the telecommunication network (or production network). TMN defines interconnection points between the two networks and specifies management functionalities. The best description of how to operate a TMN is defined by the ITU-T recommendations M.3010, M.3400, and X.700.

The purpose of a framework is to describe the big picture, illustrate different functional areas, and identify how they interoperate. The focus of ITU-T M.3400 and X.700 is the specification and classification of management functionalities only. For example, it does not define whether syslog or trap messages are mandatory for event notifications. Neither does it define specific formats for storing accounting records. These details are defined in the lower-level specifications standards. In addition to the framework of M.3400, another recommendation (M.3010) defines the principles for a TMN. It includes details of a Data Communications Network (DCN) as a transport vehicle between the management applications and network elements. A DCN is also known as out-of-band-management, which separates user traffic from management traffic. Figure 3-1 illustrates the relationship between the telecommunications network, also called the service infrastructure, and the TMN.

7.8.1 TMN and Telecommunications Networks

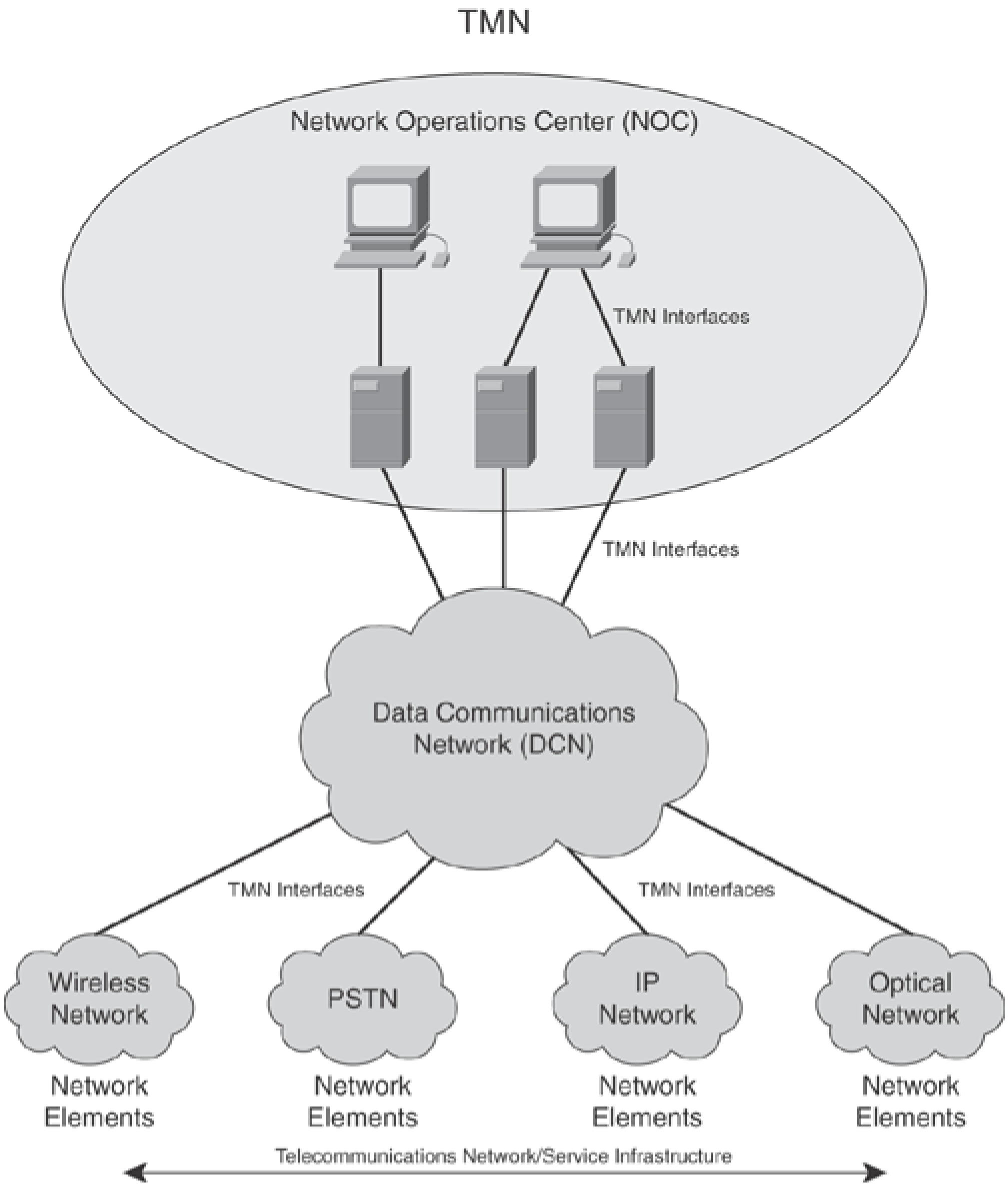


Figure 22: TMN and Telecommunications Networks

Another relevant aspect of M.3010 is the concept of layers. Network management tasks are grouped into functional areas such as FCAPS. In addition, a logical layered architecture (LLA) consists of five management layers:

- Network Element Layer (NEL) defines interfaces for the network elements, instantiating functions for device instrumentation, ideally covering all FCAPS areas.
- Element Management Layer (EML) provides management functions for network elements on an individual or group basis. It also supports an abstraction of the functions provided by the network element layer. Examples include determining equipment errors, measuring device temperatures, collecting statistical data for accounting purposes, and logging event notifications and performance statistics.

- Network Management Layer (NML) offers a holistic view of the network, between multiple pieces of equipment and independent of device types and vendors. It manages a network as supported by the element management layer. Examples include end-to-end network utilization reports, root cause analysis, and traffic engineering.
- Service Management Layer (SML) is concerned with, and responsible for, the contractual aspects of services that are being provided to customers. The main functions of this layer are service creation, order handling, service implementation, service monitoring, complaint handling, and invoicing. Examples include QoS management (delay, loss, jitter), accounting per service (VPN), and SLA monitoring and notification.
- Business Management Layer (BML) is responsible for the total enterprise. Business management can be considered a goal-setting approach: "What are the objectives, and how can the network (and network management specifically) help achieve them?"

Figure 3-2 shows the relationship between the different layers as well as the relationship with the FCAPS model. Each management layer is responsible for providing the appropriate FCAPS functionality according to the layer definition. Each layer communicates with the layers above and below it.

7.8.2 ITU-T M.3010: TMN Logical Layer Architecture

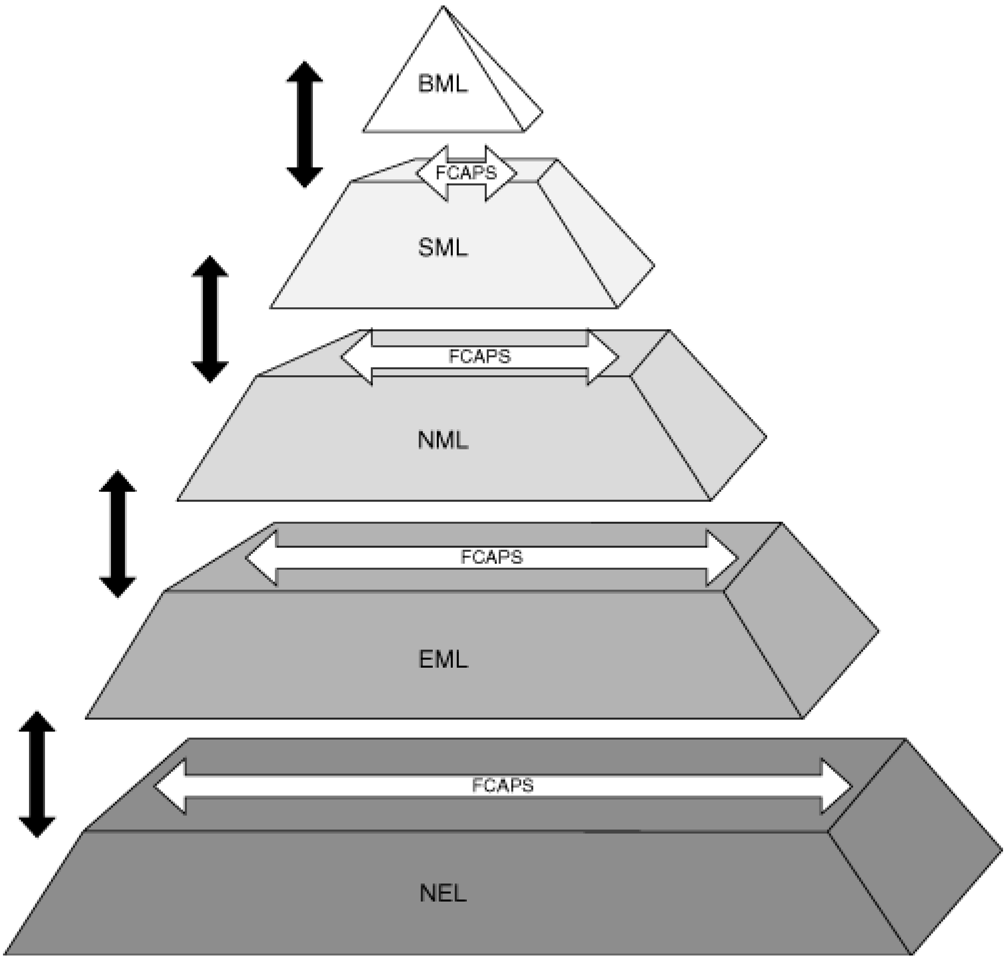


Figure 23: ITU-T M.3010: TMN Logical Layer Architecture

Now that the different layers of the TMN model have been identified, the functionality of each FCAPS area is described next. The TMN architecture has a strong relationship to Open Systems Interconnection (OSI) standards and frameworks. ISO 7498-4 defines the framework, concepts, and terminology of the OSI Management standards: "Information Processing Systems - OSI - Basic Reference Model - Part 4: Management Framework."

The ITU-T M.3400 recommendation is one document within the M series. It specifies five management functional areas (FCAPS):

- Fault management— Detect, isolate, notify, and correct faults encountered in the network.
- Configuration management— Configure aspects of network devices, such as configuration file management, inventory management, and software management.
- Accounting management— Collect usage information of network resources.
- Performance management— Monitor and measure various aspects of performance so that overall performance can be maintained at a defined level.
- Security management— Secure access to network devices, network resources, and services to authorized individuals.

The following section provides more details about each area. This chapter covers the FCAPS model extensively, because it sets the foundation for network management in general and provides a good understanding of accounting and performance management and their potential relationship to each other. Therefore, not only the accounting and performance parts of FCAPS are addressed, but the full model. Afterwards, other standards are discussed solely based on their specific relationship to accounting and performance management. Also, note that there is not an exact match between the brief FCAPS summary in Chapter 1 and the extended details for accounting and performance in this chapter. Chapter 1 provides the authors' definitions from a network element perspective, and this chapter covers FCAPS functionality from all layers of the TMN model.

7.8.2.1 Fault Management

Fault management is a set of functions that enable the detection, isolation, and correction of abnormal operation of the telecommunication network. The quality assurance measurements for fault management include component measurements for Reliability, Availability, and Survivability (RAS). Fault management consists of the following functions:

- RAS quality assurance establishes the reliability criteria that guide the design policy for redundant equipment (a responsibility of configuration management) and the policies of the other function groups in this area.
- Alarm surveillance describes the capability to monitor network element failures in Near Real Time.
- Fault localization describes where the initial failure information is insufficient for fault localization. It has to be augmented with information obtained by additional failure localization routines at the application level.
- Fault correction transfers data concerning the repair of a fault and the control of procedures that use redundant resources to replace equipment or facilities that have failed.
- Testing can be carried out in two ways. In one case, a network element analyzes equipment functions, where processing is executed entirely within the network element. Another method is active testing of external device components, such as circuits, links, and neighbor devices.
- Trouble administration transfers trouble reports originated by customers and trouble tickets originated by proactive failure-detection checks. It supports action to investigate and clear the problem and provides access to the status of services and the progress in clearing each problem.

7.8.2.2 Configuration Management

Configuration management provides functions to identify, collect configuration data from, exercise control over, and provide configuration data to network elements. Configuration management supports the following functions:

- Installing the physical equipment and logical configurations.
- Service planning and negotiation, which addresses planning for the introduction of new services, changing deployed service features, and disconnecting existing services.
- Provisioning, which consists of necessary procedures to bring equipment into service but does not include installation. As soon as the unit is ready for service, the supporting programs are initialized via the TMN. The state of the unit (in service, out of service, standby, or reserved) and selected parameters may also be controlled by provisioning functions.
- Status and control where the TMN provides the capability to monitor and control certain aspects of the network element (NE) on demand. Examples include checking or changing an NE's service state (in service, out of service, or standby) or the state of one of its subparts and initiating diagnostic tests within the NE. Normally, a status check is provided in conjunction with each control function to verify that the resulting action has taken place. When associated with failure conditions, these functions are corrective in nature (such as service restoration).
- Network planning and engineering deals with functions associated with determining the need for growth in capacity and the introduction of new technologies. Planning and engineering are examples of functions across multiple areas, because they relate to the performance section from a monitoring perspective and to the configuration section from an enforcement perspective.
-

7.8.2.3 Accounting Management

Accounting management lets you measure the use of network services and determine costs to the service provider and charges to the customer for such use. It also supports the determination of charges for services. Accounting management includes the following functions:

- Usage measurement— Consists of the following subfunctions:
    - Planning and management of the usage measurement process
    - Network and service usage aggregation, correlation, and validation
    - Usage distribution
    - Usage surveillance
    - Usage testing and error correction
    - Measurement rules identification
    - Usage short-term and long-term storage
    - Usage accumulation and validation
    - Administration of usage data collection
    - Usage generation
- Tariffing and pricing— A tariff is used to determine the amount of payment for services usage.
- Collections and finance— Functionality for administering customer accounts, informing customers of balances and payment dates, and receiving payments.
- Enterprise control— This group supports the enterprise's financial responsibilities, such as budgeting, auditing, and profitability analysis.

7.8.2.4 Performance Management

Performance management provides functions to evaluate and report on the behavior of telecommunication equipment and the effectiveness of the network or network element. Its role is to gather and analyze statistical data for the purpose of monitoring and correcting the behavior and effectiveness of the network, network elements, or other equipment, and to aid in planning, provisioning, maintenance, and quality measurement. Performance management includes the following functions:

- Performance quality assurance— Includes quality measurements, such as performance goals and assessment functions.
- Performance monitoring— This component involves the continuous collection of data concerning the performance of the network element. Acute fault conditions are detected by alarm surveillance methods. Very low rate or intermittent error conditions in multiple equipment units may interact, resulting in poor service quality, and may not be detected by alarm surveillance. Performance monitoring is designed to measure the overall quality, using monitored parameters to detect such degradation. It may also be designed to detect characteristic patterns of impairment before the quality has dropped below an acceptable level. Performance monitoring includes the following functions:
    - Performance monitoring policy
    - Network performance monitoring event correlation and filtering
    - Data aggregation and trending
    - Circuit-specific data collection
    - Traffic status
    - Threshold crossing alert processing
    - Trend analysis
    - Performance monitoring data accumulation
    - Detection, counting, storage, and reporting
- Performance management control— This group includes the setting of thresholds and data analysis algorithms and the collection of performance data. It has no direct effect on the managed network. For network traffic management and engineering, this includes functions that affect the routing and processing of traffic.
- Performance analysis— The collected performance records may require additional processing and analysis to evaluate the entity's performance level. Therefore, performance analysis includes the following functions:
    - Recommendations for performance improvement
    - Exception threshold policy
    - Traffic forecasting (trending)
    - Performance summaries (per network and service, and traffic-specific)
    - Exception analysis (per network and service, and traffic-specific)
    - Capacity analysis (per network and service, and traffic-specific)
    - Performance characterization

7.8.2.5 Security Management

Security is required for all functional areas. Security management consists of two main functions:

- Security services for communications provide authentication, access control, data confidentiality, data integrity, and nonrepudiation. These may be exercised in the course of any communications between systems and between users or customers and systems. In addition, a set of pervasive security mechanisms are defined that are applicable to any communication, such as event detection, security audit-trail management, and security recovery.
- Security event detection and reporting reports activities that may be construed as a security violation (unauthorized user, physical tampering with equipment) on higher layers of security applications.

Security management includes the following functions:

- Prevention
- Detection
- Containment and recovery
- Security administration

7.8.3 The TMN Framework

The framework shown in Figure 3-3 brings it all together. The different logical layers sit on top of each other; each layer is responsible for implementing the FCAPS functionality and passes the collected information to the next layer. From a customer's applicability perspective, after identifying and prioritizing the requirements, you can map various network management products to this matrix and identify what is required to meet your needs.

7.8.4 TMN Management Layers and FCAPS

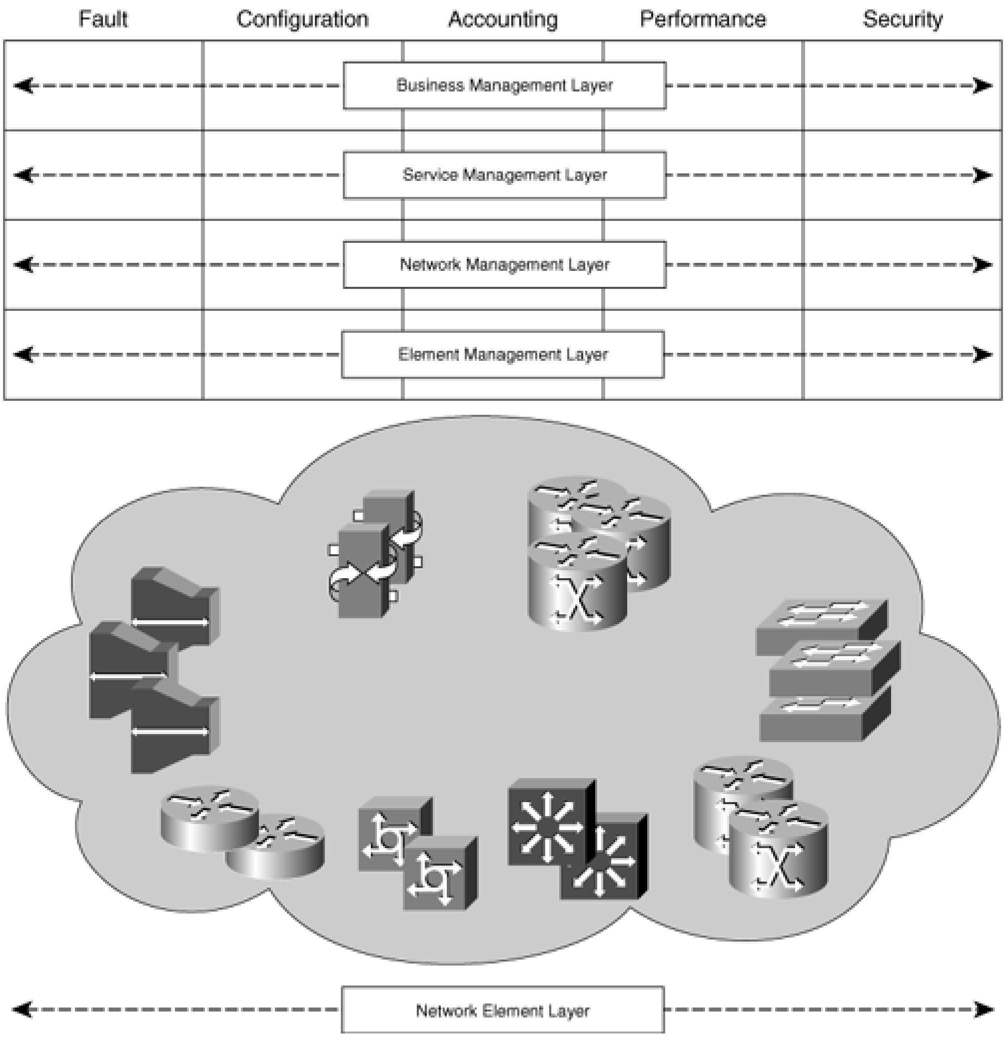


Figure 24: TMN Management Layers and FCAPS

From the perspective of this book, relevant layers of the TMN architecture are the Network Element Layer (NEL); the Element Management Layer (EML), related to similar device types; the Network Management

Layer (NML), related to mediation; and the Service Management Layer (SML), related to service monitoring and accounting. The Business Management Layer (BML) is outside the scope of this book. If you're interested, you're encouraged to study the ITU-T M series for more details.

Note that the FCAPS model describes the conceptual model of functional areas; it does not define accounting and performance standards for data collection. Therefore, a second level of standards is required for data collection. At the network element layer, it can be SNMP or IPFIX. IPDR is appropriate at the Element Management Layer.

7.9 Appendix 3 - Relationship between Service/Resource instances and KQI/KPI/PI instances

Relationship between Service/Resource instances and KQI/KPI/PI instances can be reflected by following 2 figures.

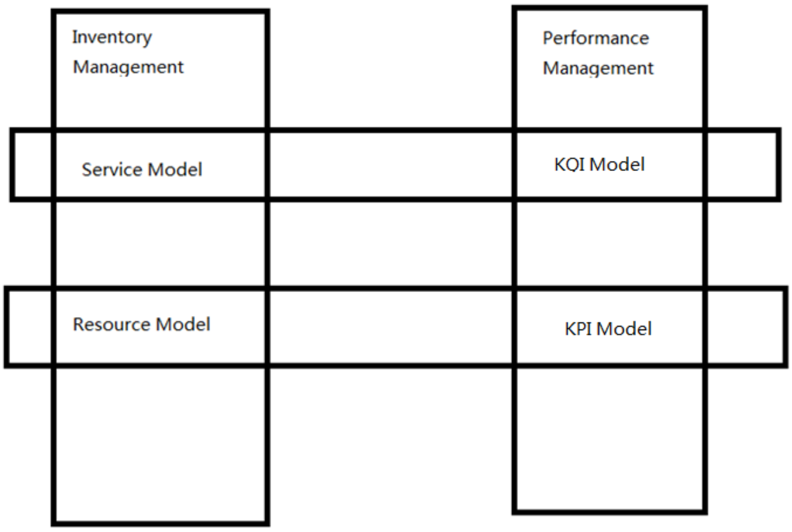


Figure 25: Relationship between Service/Resource instances and KQI/KPI/PI instances I

And

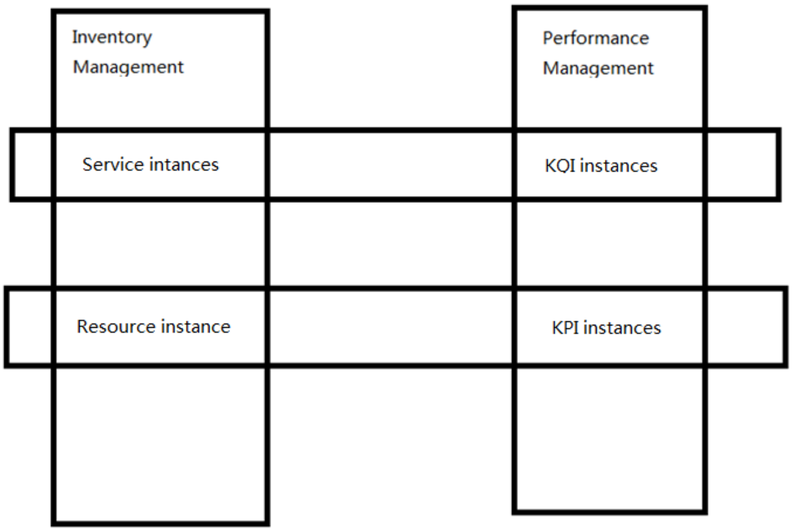


Figure 26: Relationship between Service/Resource instances and KQI/KPI/PI instances II

TM Forum SID also defined the data model of Service/Resource and their Performance generally in GB922_Addendum_1_Performance_R12-5_v1-10.

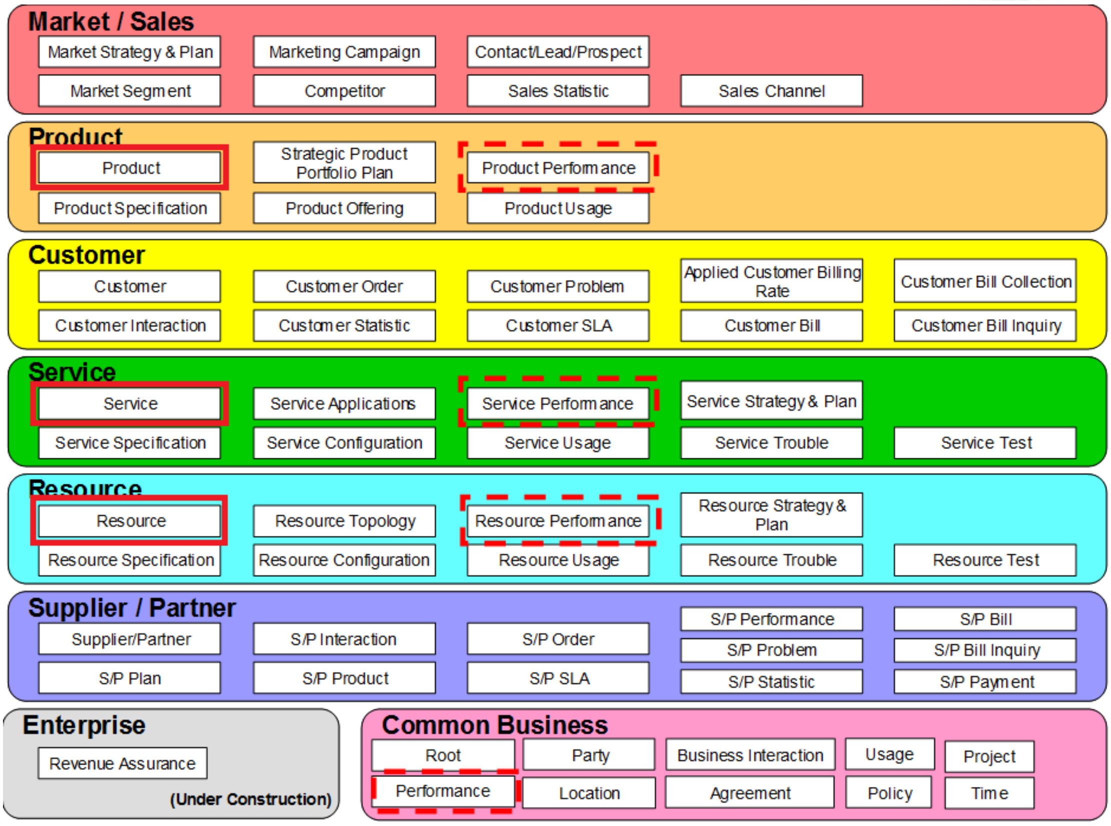


Figure 27: SID Framework Performance Entities

The Service Performance ABE collects, correlates, consolidates, and validates various performance statistics and other operational characteristics of customer and resource facing service entities. It provides a set of entities that can monitor and report on performance. Each of these entities also conducts network performance assessment against planned goals, performs various aspects of trend analysis, including error rate and cause analysis and Service degradation. Entities in this ABE also manage the traffic generated by a Service, as well as traffic trend analysis. This is important for newer technologies that separate data, control and management functions for a given Service.

The Resource Performance ABE collects, correlates, consolidates, and validates various performance statistics and other operational characteristics of Resource entities. It provides a set of entities that can monitor and report on performance. The entities in this ABE provide physical, logical, and performance information. Each of these entities also conducts network performance assessment against planned goals, performs various aspects of trend analysis, including error rate and cause analysis and Resource degradation. Entities in this ABE also manage traffic in a Resource. This includes statistics defining Resource loading, and traffic trend analysis.

Service, Resource, and Performance

The Performance ABE is an addition to the SID model's Common Business Entities domain. It represents an generalization of attributes and relationships that are common to both the SID Service Performance and Resource Performance ABEs' entities, such as performance indicators, objectives, and consequences. **Resource performance** entities is collected hop by hop (between two network elements), while **service performance** is an aggregation of multiple resource performance instances that constitute the path a service takes through a network. Two key entities that comprise the Performance ABE are PerformanceSpecification and Performance. They represent an application of the SID EntitySpecification/ Entity pattern. A PerformanceSpecification and its related specification entities provide the definition of the performance attributes, such as KPIs, dimensions, and performance objectives. The Performance entity and its related entities provide the values associated with the manner in which a service or resource is performing or has performed, such as the loss of 5K packets between two network elements.

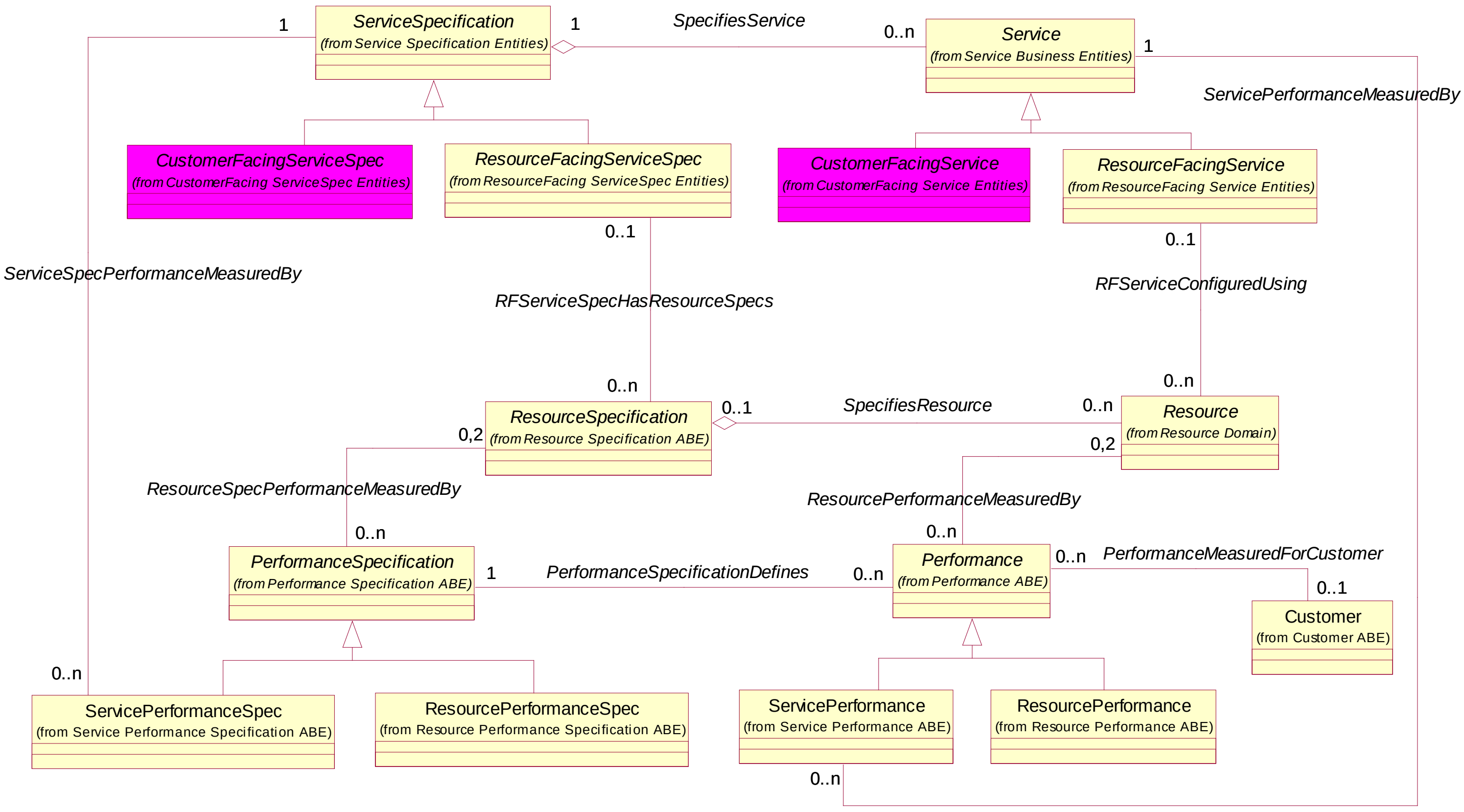


Figure 28: Service, Resource, and Performance

Figure Service, Resource, and Performance shows the associations that performance entities have with existing service and resource entities, as well as the association that the Performance entity has with the Customer entity. Note that the dark-shaded entities, CustomerFacingServiceSpecification and CustomerFacingService are not within the scope of the model as they related the Service domain with the Product domain, which is out of scope at this point in time. Also note that the ResouceSpecification is related directly to the PerformanceSpecification entity and Resource is related to the Performance entity, since both Service and Resource performance deal with Resources.

The associations with the specification entities provide part of the definition of the performance specification entities. For example, the specification of a GGSN and SGSN define the types of network elements whose performance is measured.

The cardinality of the association between ResourceSpecification and PerformanceSpecification is 0,2 because at most two types of resources' performance is defined by a PerformanceSpecification. Similarly, the association between Resource and Performance also has a cardinality of 0,2. These Resource domain entities are directly related to the respective Performance ABE entities and not to ResourcePerformanceSpec and ResourcePerformance. The reason is that Resources are used to measure both Service-related and Resource-related performance.

For the ServiceSpecification entity the cardinality is 1 because a given instance of a ServicePerformanceSpec entity measures the performance of a single ServiceSpecification entity, such as a mobile voice call. Similarly, the cardinality of the association between a Service and a Service performance is 1.

The cardinality between a Customer and Performance is 0,1 because a instance of Performance may or may not be a measure of performance for an instance of Customer.

A PM measurement job is the administrative entity defined by a client application to perform a periodic activity related to PM data. The PM activities may be production of measurements, collection of measurements or PM objective monitoring (scheduled evaluation of thresholds). The PM Measurement Job is a sub class of the PM Management Job (Management Job ABE under TIP Common ABE). The Management Job defines the attributes that may apply to any kind of a job while the Measurement Job adds the attributes that are specific to the Performance Management context.

The PM measurement job includes the following:

- A set of requested performance indicators
- A network/service scope defining a subset of the network or a subset of the service catalog
- Scheduling parameters
- Specific activity parameters, related to collection, production or objective monitoring

A measurement job must define a scope of monitored objects using the monitored objects criteria. The monitored objects criteria support two kinds of monitored objects specification, represented as two sub-entities:

- Monitored Instances criteria - Specifies a list of individual monitored instances (typed as object names).
- Monitored Class criteria - Specifies a monitored object class (a string) in conjunction with a filter object. The filter is composed of name value pairs that can be used to focus the PM collection.

The Measurement Job is shown in figure Measurement Job.

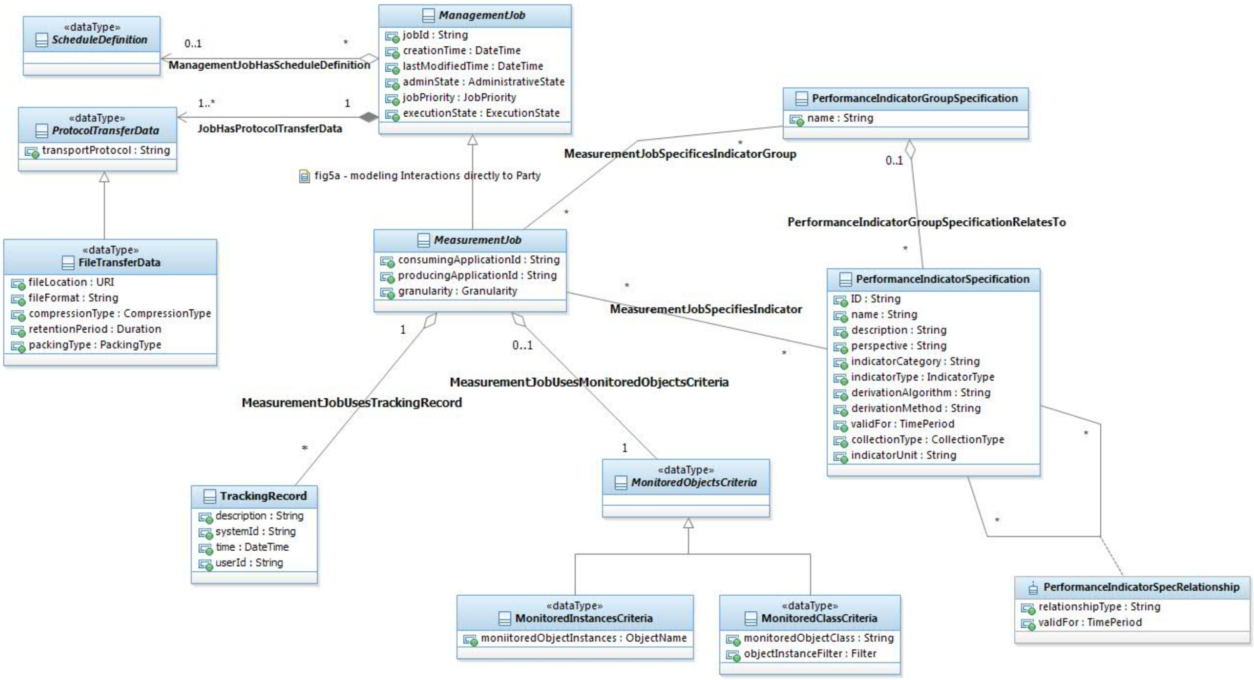


Figure 29: Measurement Job

A Measurement Collection Job is used to control the periodic collection of performance indicators, implemented as a sub-entity of the PM Measurement Job. As the Measurement Collection Job inherits from the Measurement Job, it includes all attributes and associations defined for the base measurement job entity. The Measurement Collection Job and its attributes are shown in figure PF.16 below.

Similarly, a Measurement Production Job is defined as a sub-entity of the Measurement Job. It is used to define a job for generating indicators. A Production Job may have a Collection Job associated to it. The Production Job is described is also shown in figure Performance Monitoring, Measurement Production & Collection Jobs

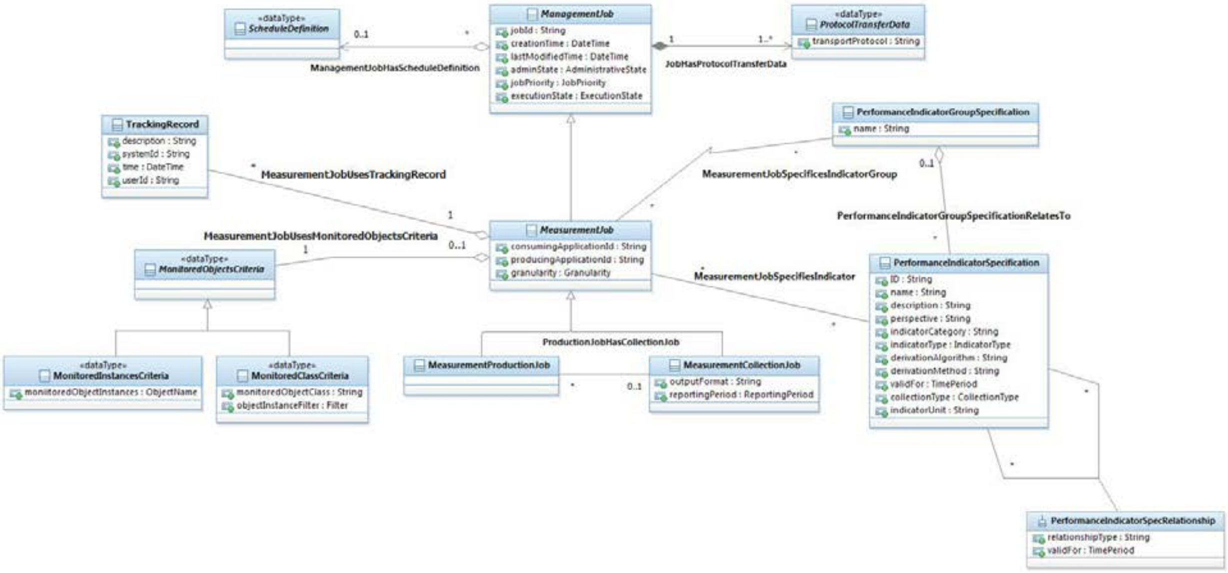


Figure 30: Performance Monitoring, Measurement Production & Collection Jobs

7.10 Appendix 4 – Sketch of Resource and Service Management Domain

From [16]

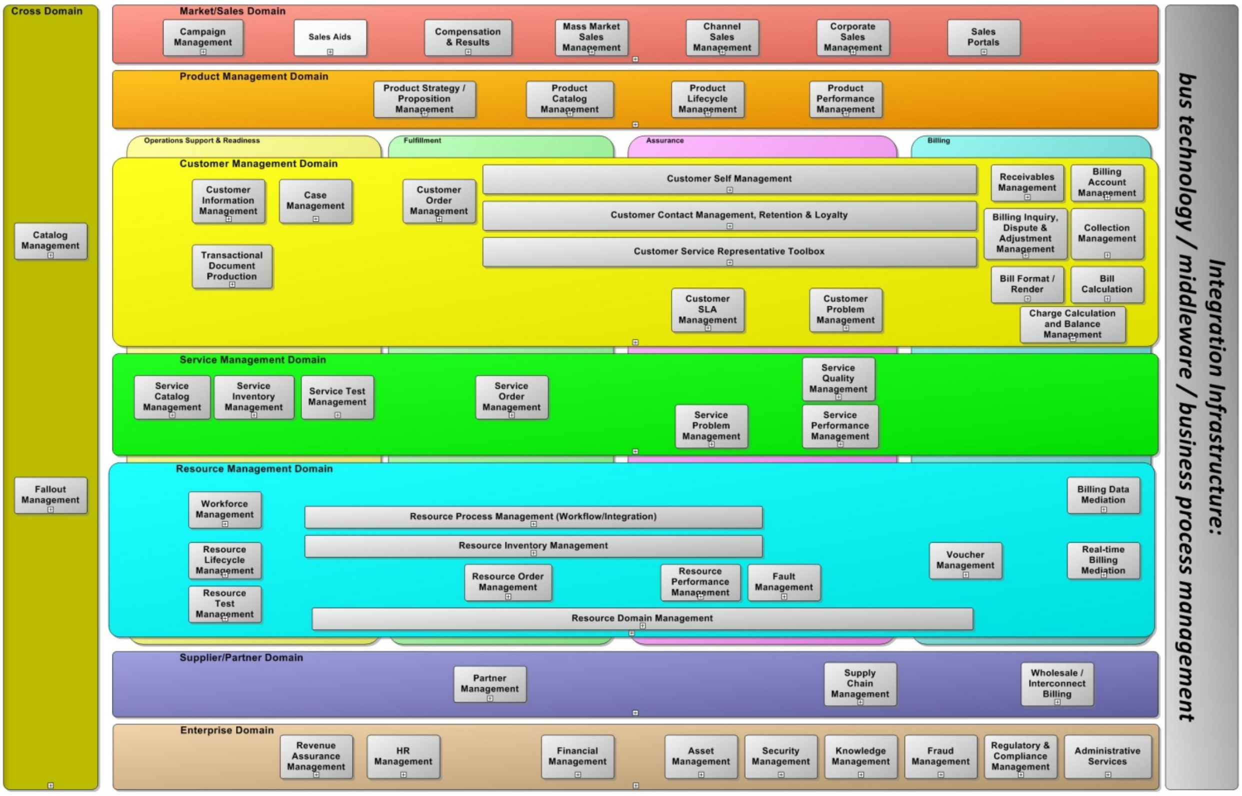


Figure 31: TM Forum Application Framework

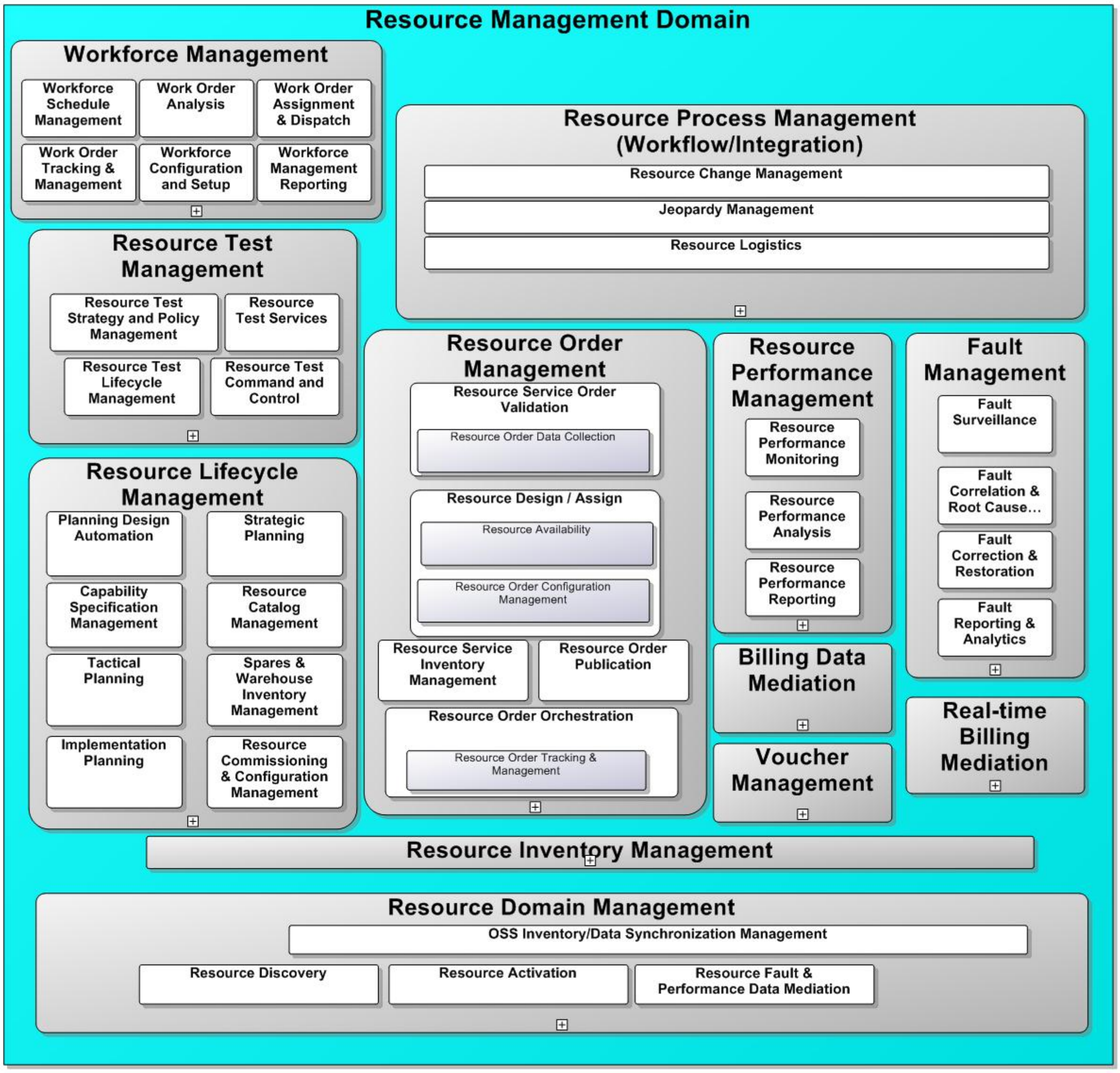


Figure 32: Resource Management Domain of TM Forum Application Framework

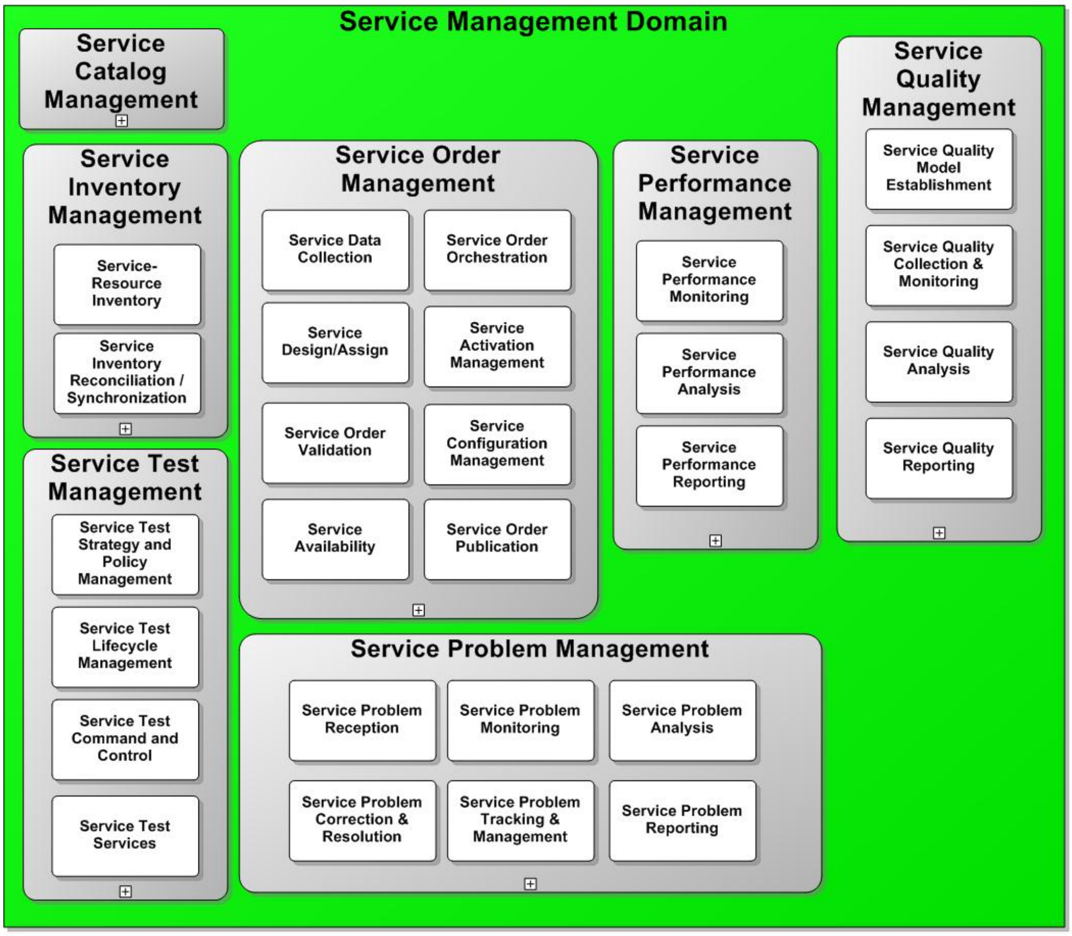


Figure 33: Service Management Domain of TM forum Application Framework

7.11 Performance Management Requirements and their Addressees

PM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-PM (1)	X		X
REQ-PM (2)	X	X	X
REQ-PM (3)	X	X	
REQ-PM (4)	X		X
REQ-PM (5)	X		X
REQ-PM (6)	X		X
REQ-PM (7)	X		X
REQ-PM (8)	X		
REQ-PM (9)	X		
REQ-PM (10)	X		
REQ-PM (11)	X		

PM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-PM (1)	X		X
REQ-PM (2)	X	X	X
REQ-PM (12)	X		
REQ-PM (13)	X		
REQ-PM (14)			X
REQ-PM (15)		X	
REQ-PM (16)			X
REQ-PM (17)	X		
REQ-PM (18)	X		
REQ-PM (19)			X
REQ-PM (20)			X
REQ-PM (21)			X
REQ-PM (22)			X
REQ-PM (23)	X		
REQ-PM (24)	X		

NGCOR

NEXT GENERATION CONVERGED OPERATIONS REQUIREMENTS

STREAM "INVENTORY MANAGEMENT"

by NGMN Alliance

Version:	**1.0**
Date:	**2013-07-22**

Version:	**1.0**
Date:	**2013-07-22**
Document Type:	
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Pekka Olli/ TeliaSonera**
Contributors:	
Approved by / Date:	**NGMN Board / 7th November 2013**

Abstract: Short introduction and purpose of document

This a deliverable from NGMN NGCOR Inventory Management sub-task. The document describes service and Resource Inventory Management requirements based on use case analysis of different processes addressing development&deployment and operations processes within operators' environments. The requiremnts are targeted to give guidance in standarzation development and inventory solution implementation.

Document History

Date	Version	Author	Changes
2012/10/10	V 0.1	Pekka Olli, TeliaSonera	1st version, based on gathering from NGCOR phase 1 InvM
2012/11/23	V 0.13	Lukasz Mendyk, Comarch SA	Chapters: 2.4.3 Scenarios and use cases related to service inventory support for infrastructure sharing business scenarios 2.4.4 Scenarios and use cases related to service inventory support for Configuration Management 2.4.5.1 Use Case: Service catalogue driven customer service order fulfilment process
2012/11/26	V 0.11	Pekka Olli, TeliaSonera	Chapters: 2.4.2.1 Use case: Deriving service specification from product specification 2.4.2.2 Use case: Modelling service reflecting the underlying technology infrastructure, (generic) 2.4.2.3 Creation and maintenance of service specification capabilities, the service meta-model 2.4.6.1 Use case: Service inventory support for service quality management
2012/12/05	V0.2	Pekka Olli, TeliaSonera	Merging previous versions V0.1, V 0.11, V0.13 to V 0.2
2012/12/31	V0.21	Pekka Olli, TeliaSonera	Enhancements , chapters 2.3, input from Michael Geipl 2.4.x added and modified use cases process pictures Some editorial
2013/01/10	V0.3	Pekka Olli, TeliaSonera	Merging previous versions to v0.3, Some editorial,
2013/01/16	V0.5	Pekka Olli TeliaSonera	Editorial update for delivery of NGCOR 2 drafts
2013/01/18	V0.6	Pekka Olli TeliaSonera	Streamlining and editorials by Yvonne Dörnhofer

2013/01/31	v0.61	Pekka Olli Teliasonera	Walkthrough comments in Beijing meeting
2013/02/25	V0.61NetCracker	NetCracker	Review comment and input
2013/01/15	V0.64	Lukasz Mendyk, Comarch	Integrating previous contribution (v.23) - REQ-InvM (15)… REQ-InvM (17)
2013/02/22	V0.64	Lukasz Mendyk, Comarch	REQ-InvM(18-19),
2013/02/27	V0.7	Pekka Olli TeliaSonera	Merging the previous vesrions v0.6xx
2013/03/05	V0.71_PO	Pekka Olli TeliaSonera	Enhancements on V0.7 various chapters
2013/03/13	V0.71	Michael Geipl,/ DT	Integrating terms/definitions for SIM in chapter 2.3.2; Inserting appendix A on service modelling
2013/03/05	V0.72	Pekka Olli TeliaSonera	Merging V0.7xx
2013/03/27	V0.73	Michael Geipl,/ DT	Correction of Service definition in chapter 2.3.2 Condensing Annex A.1 Integrating Resource terms/definitions in chapter 2.3.1
2013/04/12	V0.75	Pekka Olli TeliaSonera	Inserting NGCOR phase 1 material Organizing requirements chapters
2013/04/12	V0.75-MG	Michael Geipl,/ DT	Corrections 2.3.1, 2.3.2
2013/04/12	V0.76	Pekka Olli TeliaSonera	Enhancements
2013/04/18	V0.77	Pekka Olli TeliaSonera	Enhancements , chapter 4.3.1.3, use case and requirements templates to be used shown in use case chapter and requirements chapter
2013/05/17	V0.78-_MG	Michael Geipl,/ /DT	Additions to v0.77 Chapter A1.3 'SLA Modelling in SID' added. Consideration of TM Forum Comments (slight modifications in chapters 2, 5.1.1, 5.2.1, 5.2.2). Input to chapter 3 'Gap Analysis'. Editorial corrections in Annex A.
2013/05/20	V0.79	Pekka Olli	Cleaning V0.77 and V0.78 making acceptance of most track changes so far
2013/05/20	V0.8	Pekka Olli	Integration of new contributions after Torino meeting; - V0.78_MG - NGCOR templates for use case and reqs implemented - Merged two use cases (CFS and RFS defintions) - Reqs cleaning
2013/05/23	V0.81	Pekka Olli	Enhancements • Conversion to common templates for use cases and requirements • Identifiers of use cases and reqs (note reqs numbering changes) • Removed duplicate requirements • Included service inventory example from Necracker, chapter 6.1.1 • Additions in gap analysis (MG)

			• Chapter conclusions • Service modelling examples moved from appendix to chapter 6 • editorials
2013/05/23	V0.82	Pekka Olli	References between use cases and requirements enhanced
2013/06/03	V0.82-MG	Michael Geipl/DT	Review comments
2013/06/06	V0.85	Pekka Olli	Additions in Gap analysis (clouds etc.) Cross References between use cases and requirements SQM example from Comarch Chapter conclusion Editorial checkings MG&PO
2013/06/10	V0.9	Pekka Olli	Inventory chapter finalization for NGCOR consolidation
2013/06/14	V0.91	Yvonne Doernhofer	Editorial review
2013/06/16	V0.92	Pekka Olli	Editorial checkings/corrections
2013/06/25	V0-95	Pekka Olli	Editorial reviewing, checking/corrections in cross-referencing use cases vs requirements and inserting MSWord cross-referencing Added table to whom requirements are addressed Additional notes related to merging NGCOR phase 1 and NGCOR phase 2
2013/06/26	V0.96	Yvonne Doernhofer	Add addressees of requirements section; editorial clean-up
2013/06/27	V0.97	Pekka Olli	Editorial correction
2013/07/22	V1.0	Thomas Kulik	Version changed to V1.0 to align with other streams and showing readiness from project point of view; numeration of chapters, figures and tables changed;

8 REQUIREMENTS FOR RESOURCE AND SERVICE INVENTORY MANAGEMENT (INVM)

8.1 STREAM GENERAL OVERVIEW

Information today pervades every aspect of an organization, including reporting, marketing, product development, and resource allocation. In the last years, business reports to management and investors as well as planning decisions of a service provider have become much more dependent on information derived from various sources than ever before.

The Inventory stream of NGCOR places the Inventory Management in the focal point of view as it is understood that inventories are the key and core parts of OSS architecture of operators. The main role of inventories is to provide comprehensive and reliable data supporting efficiently different operational, planning and deployment processes when managing the infrastructure and the services. Inventories are the key OSS applications/ systems and central points of managed and structured way of information handling throughout different management layers.

A direction to harmonized inventory interfaces and information models is a must when having a growing complexity of OSS support needs. Operators still do have a lot of old legacy inventory systems. The information in these systems is not flexible to use, since it is split into many pieces and many data stores. When implementing next generation networks and services an increasing amount of new network and service data has to be managed in conjunction with the older ones. At the same time customer focused information management accelerates integration needs between BSS level and OSS level and requires inventory support. A federated view from different inventory systems is a foreseen need. Generally, inventory development projects are perceived as expensive and the answer to the question how to make migration paths cost effectively and secure way to new generation commercial-off-the shelf (COTS) inventories is of high importance for operators.

Resource inventories or traditionally 'Network inventories' are OSS systems which are managing all resource related information covering all physical and logical resources and their features i.e. all resource information needed and used to implement and operate services and products.

Service inventories are relatively new concepts in the OSS and not much experience with implementations exists yet. However operators do see them as key part of target OSS for improved and efficient service management.The purpose of service inventories is to manage and store all service definitions and common service information and data. The service inventory implements an abstraction layer between products and resources.

Product inventories are BSS systems which are managing product catalogue and keeping track of the product subscriptions. The product catalogue defines the product offering from marketing perspective and consists of a collection of product specifications.

8.2 INTRODUCTION

8.2.1 Scope

The NGCOR Inventory Management work was initiated during March - June 2011 within NGCOR phase 1 project. In the very beginning the focus was first to get a common view on Inventory Management area in broad sense: The main Inventory Management concepts, the main roles and characteristics of inventories within OSS/ BSS environment of operators.

In the continued work of NGCOR phase 1 during autumn 2011 Resource Inventory Management was the selected prioritized area and several use cases and scenarios on essential process areas were identified and related requirements were defined.

In NGCOR phase 2 Service Inventory Management area was selected to be in scope to extend Inventory Management requirements. For Service Inventory Management area also several use cases and scenarios on essential process areas were identified and related requirements were defined.

Product Inventory Management area has been out of scope of detailed use case and requirements work of NGCOR. Only high level concepts and principles of Product Inventory Management are described to show the view of all inventory layers within OSS/ BSS.

8.2.2 References

As an outlining summary of the problem space and concepts, NGCOR positions Inventory Management at the core of information management for resources, services and products within OSS/ BSS environment of operators. NGCOR shares an aligned view of TM Forum TIP Inventory harmonization study [59], i.e.

- the general acceptance that the term “Inventory” designates a repository of information (Data Base), and more precisely a repository of instance entities. Depending on the focus, this repository may contain instances of Products, Services, and Resources.
- the term “Catalogue” would be more used to designate a repository of specifications (e.g. service specifications, resource specifications). The term “Specification” is used to define the invariant characteristics and behaviour (attributes, methods, constraints, relationships, requests, associated business rules and FAB processes) of a (Managed) Resource/ Service.
- In the document we will consider Inventory Repository in the broad sense, meaning that it may contain instances and/ or specifications. The instances that may be present in an Inventory repository are instances of object classes all specified in an information model.
- Complementary to the repository (data store) view point, an Inventory system can expose services either by sending notifications to external systems or by allowing external systems to invoke operations that it exposes. The operations may be used by external systems:
    - to modify the content of the repository (we talk about updating or synchronizing processes) or
    - to query the repository in order to collect specific information that it contains.
- the notifications generated by an Inventory system are used to inform other systems of any change in the repository.

With respect to Inventory Management specified by 3GPP, NGCOR has a broader scope by addressing functionalities of Inventory Management within OSS architecture of operators and interfacing inventory with other OSS applications. NGCOR is dealing also with functionalities of NMSs and also NMS - NMS interfacing. The common problem space of 3GPP and NGCOR is interfacing towards the network, i.e. aiming at a standard northbound interface. In this context it is also to be noted that ‘network’ can have several layers or domains as detailed architecture view: access, transport, control, application, content etc. A management system, OSS/ NMS, manages all these layers. Typically today EMSs for different domains are having different northbound interfaces towards OSS/NMS and this is the specific problem space where NGCOR drives harmonization and convergence.

It is to be noted that when describing OSS architecture models, e.g. as in Figure 14, the presented architecture structures do not imply any implementation model. That means implementation models derived from the reference model can include variants. For example, the described functionalities can be implemented separately or jointly, the needed databases can be centralized or distributed.

8.2.3 Terminology and conventions

This chapter explains and analyses terminology and main conventions of concepts in the Inventory Management area. The analysis is presented in order to create a solid basis for Inventory Management requirements in the context of the NGMN NGCOR project. Also 'the full picture' of inventories is addressed spanning from BSS-level product Inventory Management to OSS with service and resource/ network layer Inventory Management.

The NGCOR project is supposed to build on previous work done in SDOs and other industry organizations. NGCOR Inventory Management uses TM Forum originated concepts (eTOM, SID and TAM) for structuring the management and the role of different kind of inventories. The scope in OSS area is for setting requirements and addressing both service management layer and resource management layer needs and seeing relations from Inventory Management perspective in a comprehensive OSS architecture context.

8.2.3.1 Resource Inventory Management terminology and conventions

This chapter clarifies terms in the area of Resource Inventory Management and addresses Resource Inventory Management as a holistic concept without any major attempt to consider possible approaches for implementations for needed applications and various data repositories.

Resources represent physical and non-physical (logical) components used to construct services which lead to the definition of physical and logical resources. This is important to build a set of reusable managed entities that can be used to model the physical and logical aspects of different types of resources. Logical and physical resources are encapsulated via resource facing services. Resources could be drawn from the application, computing and network domains, and therefore include, for example, network elements (e.g. routers), software (e.g. applications), IT systems (e.g. servers in the cloud), and further technology components.

A **Logical Resource** is a part of a service provider's infrastructure that is immaterial and can't be touched. Logical resources are hosted by physical resources; they can't live on their own. Logical Resources can be grouped in a hierarchical structure. In terms of modeling it describes different logical aspects of resources and has two main purposes: To collect common attributes and relationships for all logical resource entities, and to provide a convenient, single point where relationships with other managed objects can be defined.

A **Physical Resource** is a part of a service provider's infrastructure that physically exists in reality.
In terms of modelling it is an abstract base class for describing different types of hardware/ software. It has two main purposes: To collect common attributes and relationships for all hardware/ software, and to provide a convenient, single point where relationships with other managed objects can be defined.

A **Resource Specification** represents a generic means/ template for implementing a particular type of resource. A resource specification defines the common portions of a set of resources, while a resource defines a resource instance that is based on a particular resource specification.

A **Logical Resource Specification** is a description of the characteristics and behaviour of logical resources that are considered to be of the same kind. In terms of modelling it is an abstract base class that is used to define the invariant characteristics and behaviour (attributes, methods, constraints, and relationships) of a logical resource.

A **Physical Resource Specification** is a description of the characteristics and behaviour of physical resources that are considered to be of the same kind. In terms of modelling it is an abstract base class that is used to define the invariant characteristics and behaviour (attributes, methods, constraints, and relationships) of a physical resource.

A **Resource Inventory** as a logical component of NGCOR Resource Inventory Management is a database including instance entities of logical and physical resources including the relations between them as well as with resource facing service instances.

A **Resource Catalogue** as a logical component of NGCOR Resource Inventory Management includes the engineering view of the resources and consists of collections of resource descriptions as logical and physical resource specifications including the relations between them as well as with resource facing service specifications.

The overall function of **Resource Inventory Management** is to store and manage up-to-date information (by reconciliation and synchronization procedures) of all resource specifications (physical & logical) in the resource catalogue and resource instances (physical & logical) in the resource inventory. This information will be provided or accessed by authorized OSS/ BSS applications in order to support the efficient handling of the operators' business processes.

Figure 1 shows the functional components of NGCOR Resource Inventory Management mapped to the TM Forum Telecom Application Framework (TAM). According to TAM, the main logical capabilities and closely related functionalities of Resource Inventory Management are

- Capabilities to manage, create, maintain and provide access to information of resource specifications (resource catalogue). The resource specifications are deployed by SI&P process functions (eTOM), and the resource catalogue is initially populated by OS&R process functions (eTOM).
- Capabilities for providing and maintaining on-line resource instance information for automated and manual operation process functions. Resource instances are created based on resource specifications during fulfilment process and are updated according to the usage status of resources. All physical and logical configuration of the infrastructure including network elements, service and IT systems (end to end view: access, core, transport, control layer, application layer) and their components (SW and HW) are kept on track.
- Capabilities to provide multiple reports about resource utilization/ trend, available capacity, lifecycle status of planned, deployed, used, and retired resources. Capability to visualize network resource topology in multiple views according to function, type, domain, status, administration boundary, with navigation of hierarchy and other relationships.
- Resource instance information is kept up to date with actual resource situation by resource discovery.
- Resource instance information is synchronized with other OSS applications keeping resource information up to date throughout OSS.
- Resource domain management area is regarded to represent functionality typically existing EMS systems.

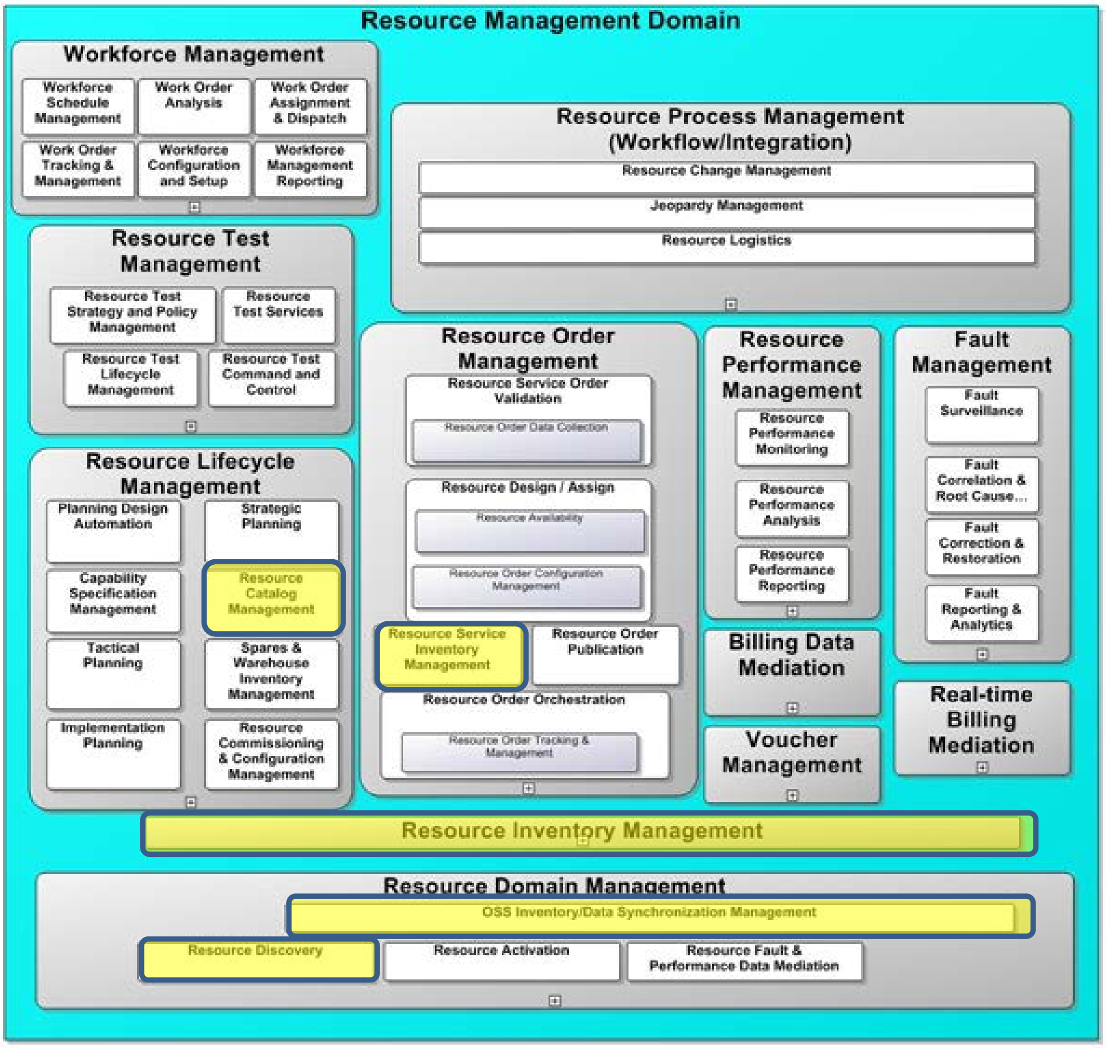


Figure 8.2-1: The constituents of NGCOR **Resource Inventory Management** reference model based on TMF TAM (v4.5) framework

In broad sense the operators' concern is of extensive and high quality **resource information management** which covers all resources and their features used to implement services and products. Fundamental principle is managing resource information in a uniform and organized way as a key part of OSS architecture. The resource information to be managed covers all physical and logical resources needed for service production including spare parts and, if applicable, extending to customer premises equipment. In service production environments implemented as cloud infrastructures or services the relevant resources need also to be modelled in the resource inventory.

Considering the role of Resource Inventory Management in management of dynamic information in the network – such as functioning of **Self Organized Network** (SON) features in the network elements, it can be generally characterized OSS and management environment needs ([1] NGMN Alliance NGMN TOP OPE Requirements):

- OSS needs to support SON implemented according to different solution scenarios; centralized, distributed and/ or hybrid solutions.

- A network element can operate with or without SON function and can easily be transferred between these two modes. The ability to suspend/ resume/ enable/ disable the SON function at determined break points shall be defined on a case by case basis.
- Degree of automation to be configurable by the operator, spanning from operator controlled (open loop) to fully autonomous (closed loop).
- OSS needs to support completely automated optimization cycle of SON.
- OSS needs to support automated import of optimized settings for SON.
- OSS should provide a general SON monitoring & control application covering policy control, history log and switch on/ off functionality. OSS shall be synchronized in real time with SON initiated network changes. Capability to monitor the specific results of each particular SON function needs to exist.

As regards to various optimization features enabled by SON (Automatic Neighbourhood Relations, Cell Physical Identiry management, cell outage compensation, load balancing, etc.) it is needed that:

- OSS should provide analysis, alarms and user friendly visualization of the optimization feature in question.
- OSS should provide the operator with resolution scenarios as suggestions for each specific optimization case which the operator can choose and select to solve the conflict resolution. Optionally these suggestions can be enabled automatically following operator policies.

As a **conclusion**, the dynamic and automatic behaviour of the network sets new requirements for both new types of OSS applications as well as keeping up-to-date information of the dynamic status of resources for Resource Inventory Management i.e. **"automatic inventory".**

8.2.3.2 Service Inventory Management terminology and conventions

This chapter clarifies terms in the area of Service Inventory Management and addresses Service Inventory Management as a holistic concept without any attempt to consider possible approaches for implementations.

A **Service** in the context of NGCOR is a collective term of all customer experiences based on technology driven functions which will be delivered by resources.

A Service represents a logical functionality/ abstraction which decouples products (owned & managed by BSS) from resources (owned & managed by OSS). That is why there are two differing points of view of a service for customers and operators. The customer point of view is related to the customer experience using the service via an offered product. The operator point of view will be focused on functionality/ services delivered by network and IT resources necessary to provide a product.
Because of the different points of view special service definitions and models are needed for the relationships between resource functionalities that will be provided by an operator and their usage by the customers. Therefore, the concept of Customer Facing Services (CFS) and Resource Facing Services (RFS) has been introduced.

A **Customer Facing Service (CFS)** is an abstraction that defines the characteristics and behaviour of a particular service as seen (perceived) by the customer. This means that a customer purchases and/ or is directly aware of the type of service, and is in direct contrast to a Resource Facing Service which supports Customer Facing Services but is not seen or purchased directly by the customer.
Related to the customer point of view the Customer Facing Services contain services, which will be used by external or internal customers of an operator. Important criteria for customer point of view could be the description of service usage (scenarios/ use cases). Customer Facing Services are directly related to products (realization of a product) and are enabled by Resource Facing Services. If needed, Customer Facing Services can be grouped in a hierarchical structure where the top CFS should always cover the end-to-end view/ usage of a service.

Examples for CFS could be:

- Voicecall, Voicemail
- Messaging (SMS, MMS, E-Mail)
- Media (IPTV, Video, Music, Games)
- Telematic (Location Based Services, Navigate)
- Payment (M-Commerce, Micro Payment, Payment/Cards, M-Wallet, Click & Buy)
- Customer Support Services (Call Centre)
- Data Access (in context of WLAN, 2/3G, LTE, DSL, VDSL, Roaming, M2M)
- Cloud Services (Hosting, Media Centre, SaaS)
- Content (Portal, Shops, Advertising)

A **Resource Facing Service (RFS)** is an abstraction that defines the characteristics of a particular service that is not directly seen or purchased by the customer, and is more directed towards physical and/or logical resources. Characteristically, their descriptions are more technical oriented compared with those of CFS. If needed, they may be grouped in a hierarchical structure.
Examples for RFS could be:

- Network Access: Permits access to the network
- Transport: Provides Connectivity (e.g. LAN, WAN)
- Service Delivery Platform: HW and SW for Service Delivery
- Gateway: Enables Access to Third Party/Partner (e.g. Access to Content, Service, Firewall, Partner Access)
- Content Delivery: Data delivery functionality (video streams, music, ...)

A **Service Specification** represents a generic means/template for implementing a particular type of service. A service specification defines the common portions of a set of services, while service defines a specific instance that is based on a particular service specification. To enable collaboration between different domains, an agreement on a common service model (service specification template) for all involved domains is essential. The service specifications are deployed by SI&P process functions (eTOM).

A **Customer Facing Service Specification (CFSS)** describes the functionality of a CFS. A CFSS is an abstraction that defines the invariant characteristics and behaviour of a particular CFS as seen by the customer. The invariant portion serves as a single common basis to build a set of variable CFS that all use this common CFSS. A CFSS hides the details of its underlying technical implementation as much as possible.
A CFSS describes a functionality that the service provider provides to a customer and that the customer can access at a well-defined interaction point, which is typically realized on an end-user device like a mobile handset or a PC.
While the product specification only contains the information needed for a buying decision and a legally binding agreement, the CFSS describes the details of the functionality that can be accessed by a customer.
CFSS are associated with product specifications, thus capturing the relationship between a service and the product that is supported by this service.

A **Resource Facing Service Specification (RFSS)** describes the functionality of a RFS. A RFSS is an abstraction that defines the invariant characteristics and behaviour of a particular RFS. It is not seen by the customer, but it is required by one or more CFSS in order for them to function correctly. The invariant portion serves as a single common basis to build a set of variable RFS that all use this common RFSS. A resource-facing service specification hides its underlying implementation through hard- and software.
A RFSS is a description of a functionality that can be exposed at a device interface (a different name for a service access point) and is made available by a service provider's infrastructure.

RFSS are associated with resource specifications, thus capturing the relationship between a service and the set of resources supporting this service.

The main function of **Service Inventory Management** is to store and manage up-to-date information (by reconciliation and synchronization procedures) of all service specifications (CFSS & RFSS) in the service catalogue and service instances (CFS & RFS) in the service inventory. This information will be provided or accessed by authorized OSS/BSS applications in order to support the efficient handling of the operators' business processes.

A **Service Inventory** as a logical component of NGCOR Service Inventory Management is a database including instance entities of Customer Facing Services (CFS) and Resource Facing Services (RFS) including the relations between them as well as with resource instances (RFS concerned) and product instances (CFS concerned).

A **Service Catalogue** as a logical component of NGCOR Service Inventory Management includes the engineering view of the service offering and consists of collections of service descriptions as Customer Facing Service Specifications (CFSS) and Resource Facing Service Specifications (RFSS) including the relations between them as well as with resource specifications (RFSS concerned) and product specifications (CFSS concerned). Furthermore, related engineering rules for provisioning and monitoring can be included, e.g. a production plan that covers the activation sequence and timing considerations which have to be ensured during instantiation, or further compatibility, dependency and eligibility issues. The service catalogue is initially populated by OS&R process functions (eTOM).

Figure 2 shows the functional components of NGCOR Service Inventory Management mapped to the TM Forum Telecom Application Framework (TAM).

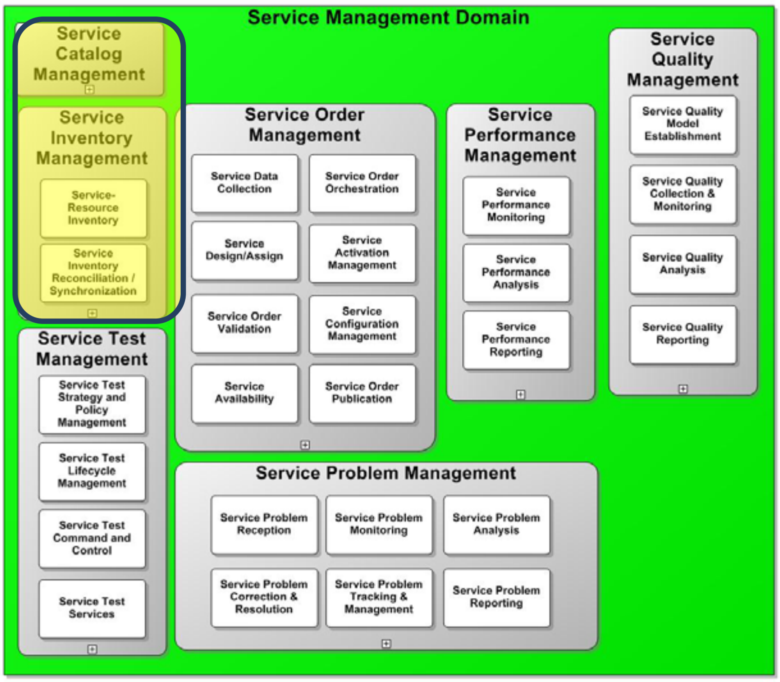


Figure 8.2-2: The constituents of NGCOR Service Inventory Management reference model based on TMF TAM (v4.5) framework

8.2.3.3 Product Inventory Management terminology and conventions

This chapter addresses product Inventory Management as a holistic concept without any attempt to consider possible approaches for implementations.

Figure 8.2-3: The constituents of NGCOR Product Inventory Management reference model based on TMF TAM (v4.5) framework

The main responsibility of the **product inventory** is to manage the **product catalogue** and keep track of the product subscriptions. The product catalogue defines the product offering from marketing perspective and consists of a collection of **product specifications**. Each product specification describes a **product type**. Several product specifications may be defined for the same product type. Product specifications are associated with service specifications, stored in the service catalogue, thus capturing the relationship between a product and the set of services bundled by this product.

Each subscription is captured in the Product Inventory through a product instance associated with the corresponding specification in the catalogue. The product instance is also associated with the subscriber of the product and the related subscriber account information, as well as the supporting CFS.

Product Inventory Interfacing with other BSS/ OSS Applications/ Functions concerns:

- Customer SLA Management, Service Problem Management/ Trouble Ticketing, and Billing and Customer Order Management use the information stored in the Product Inventory.
- Customer Order Management function stores in the Product Inventory customer details, order and product detail, and account information acquired when a new order is created. Customer Order Management also retrieves product specifications from the product catalogue in order to create product instances and to decompose the product orders.
- Service Problem Management/ Trouble Ticketing function may access the product inventory to correlate a subscriber to a service, and to retrieve details about the subscriber, when creating a trouble ticket.
- Customer SLA Management retrieves subscribers for given products and the subscriber contact information, using the product inventory.
- Service Inventory Management retrieves product inventory information for capturing the relationship between a service and the product that is supported by this service.

8.3 GAP ANALYSIS

The following **existing and ongoing standardization activities** are mainly relevant to the Inventory Management activities in NGCOR:

8.3.1 TM Forum TIP Inventory Management

The original motivation for these activities was the existence of several existing Inventory interfaces that have been developed independently from each other (OSSJ, MTOSI, 3GPP). The objective derived from this motivation is the design of a new Inventory interface for several network technologies (wireline, wireless, cloud) that is agile in order to be applicable to different Inventory domains (Resource, Service, Product) and to be compatible with different kinds of information models (TM Forum SID, 3GPP NRM, JWG MA UIM) using the TIP tool chain.

Current activities concern the design of generic task centric interface patterns that can be exposed by different OSS Systems (not limited to Inventory). This work includes interface specifications for generic Query, Update, Notification and Import/Export interfaces and their allocation to specific inventory domains. Up to now considered Inventory domains investigated in TIP have been resources. The work in future phases will also cover services and resources. As a first step SID will be used as information model.

8.3.2 TM Forum Catalogue Management

The Catalogue Management Feature Description Document (FDD) includes fundamental definitions, concepts and principles of catalogue management. The purpose of the document is to provide a set of guidelines for catalogue practices, from which particular needs/ requirements can be leveraged. It introduces a series of use cases that utilize Frameworx including Information Framework definitions for product, service, resource and business interactions in the context of catalogue management.

Besides general use cases that can apply to products, services or resources there are specific use cases for service and resource catalogues, for example:

- Managing service catalogue and catalogue items lifecycle
- Creating service catalogue items
- Querying the service catalogue items
- Publishing service catalogue items to product catalogue and service fulfillment
- Publish resource catalogue Item
- Service catalogue to resource catalogue synchronization

As a summary it can be seen that catalogues are defined as essential parts of the general Frameworx architecture. However, e.g. the details concerning interfaces between catalogues and other components in the architecture (e.g. inventories) and catalogue information is not defined.

8.3.3 3GPP SA5 Inventory Management

In 3GPP SA5 a set of specifications on Inventory Management exist which covers requirements and information modelling in UML and as XML schema. These standards are related to the Northbound Interface of Resource Inventories for mobile networks and are based on the 3GPP SA5 Network Resource Model (NRM). The area of Service Inventory is out of scope in 3GPP SA5. During the last years only minor corrections have been incorporated. Currently there is no related work item running.

8.3.4 Multi-SDO JWG on Model Alignment (MA)

The Multi SDO JWG on Model Alignment is a joint activity between 3GPP, TM Forum and NGMN (as well as potentially other interested organizations) which takes the NGMN NGCOR requirements into account. In phase 1 the work on an Umbrella Information Model (UIM) has been started. This will be continued in phase 2 enriched by further activities e.g. on an Umbrella Operations Model (UOM).
Concerning inventories in phase 1 some studies on comparison between TM Forum MTOSI and SID with 3GPP Inventory definitions and information modeling have been done. In phase 2 UIM Inventory definitions (in accordance with NGCOR, 3GPP and TMF requirements) will be addressed. This work must include definitions of inventory data to identify common views, and agreement on UIM inventory related objects, attributes and relationships.

8.3.5 TM Forum's and ETSI's work regarding service management and modeling of clouds based services and virtualization aspects

The business and operational model for cloud adoption and deployment is still an emerging topic both for the cloud services providers and buyers. The business of ensuring that cloud service creation and delivery produces highly reliable, predictable and massively scalable services, while keeping feasible operating costs and end-end control of all of the assets in the service delivery chain is very challenging for service providers. Cloud applications may rely upon virtualized computing and virtualized network resources that can both dynamically change their configurations in response to external policies and load conditions - there are both physical resources and logical resources involved. TM Forum focuses in on cloud service management aspects and more widely management of digital services in several of its programs, from which some relevant issues are referred below. (References [74], [75], [76], [77], [78]). A short outlook concerning Network function virtualization work in ETSI ISG and continuation is also given.

To address these issues, the approach taken by the TM Forum is aimed at solving that problem by exposing a common core of basic management information at the 'point of touch' between digital services. TM Forum's approach concentrates on following areas for specifications of management interfaces:

- The Frameworx Simple Management API (SM-API) which defines a design pattern for an API that reveals how to manage any given service from a Provisioning, Assurance and Usage/ Charging perspective.
- The Frameworx Service Lifecycle Management (SLM) defines best practices and requirements for establishing a role based software/services factory and a Lifecycle Management Meta Data model. This is aligned to the rest of Frameworx and ITIL.
- The key concepts for creating e2e SLA management in based on the more technical and rigorous definitions in the core TM Forum Frameworx assets.
- A step by step process called PaDIOM (Partner, Design, Integrate, Operate, Monetize) for going from concept to operational SLA Guaranteed service.

Specific concerns on cloud service resource management and challenges of virtualization
There are significant resource management challenges associated with cloud services. In particular, the virtualization at the elastic compute and elastic network layers is complicated to manage while multiple clouds and multiple enterprise domains that are increasingly involved in the delivery of cloud services further complicate the management problem. Cloud service and application management entails supporting the management of virtual and physical computing, storage, and network resources. Effective Cloud resource management is a core technical issue of cloud services and the difficulties encountered when dealing with this issue is limiting their mainstream adoption.

It is useful to look at cloud resource management from the point of view of the lifecycle management of a cloud service. Each service must be acted upon by traditional business processes associated with Provisioning/

Configuration, Service Assurance, and Charging/ Billing/ Settlement as it passes through its lifecycle. The dotted lines in Figure 4 depict the active coordinated relationship that must be maintained between resources at each layer. There must be a mechanism to maintain awareness as to which logical and physical resources are actually relevant to a specific instance of a specific application at any given point in time.

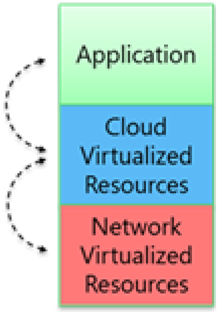


Figure 9-1: Lifecycle management of a cloud service

Another issue that arises is the division of responsibility between an internal cloud virtualization management layer (IaaS and PaaS) and an external OSS. Although the cloud virtualization layer can typically manage its own physical and logical resource allocations for supported applications, an external OSS may be required to dynamically reallocate resources in a coordinated fashion across all three layers or to track and have knowledge of those changing relationships.

To support multi-cloud end-to-end service management, management capabilities must also be exposed as interfaces between management systems. These simple service/ resource management APIs need to be able to expose the capability to manage the relevant underlying resources in a coordinated manner transparent to whatever external systems are interacting with the simple service/resource management APIs.

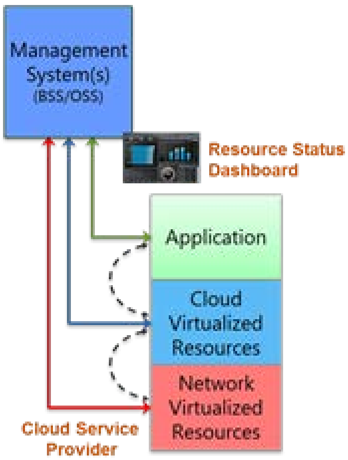


Figure 9-2: Cloud services application management

Each digital service provider is able to maintain information on the status of their own services as well as the services on which their services depend. All stakeholders are now able to subscribe to and collect event information from the services that are relevant to the end user's experience. In fact, Management as a Service becomes a new potential type of premium service.

- The provisioning interfaces described become very important in multi-cloud, syndicated scenario. Using a standard and reusable SM-API for provisioning eliminates the need for a custom integration effort to launch a new service syndication partner.
- For the Service Assurance SM-API, the ultimate test of whether the correct metrics are being collected and evaluated or not is simply whether the dashboards accurately display the status of the composite service. If the dashboards are green and the customer has a complaint then the metrics being collected are missing something important and need to be adjusted to more accurately reflect reality from a customer's viewpoint. The SM-API design template makes it feasible to iterate on this until dashboards sufficiently reflect customer reality.

Addressing modelling aspects

Cloud services are very diverse in terms of different components. To overcome this situation a unified resource representation is needed and a comprehensive cloud ontology to support the needs of cloud providers, as well as of the application developers. In order to have such a "common description language" for cloud resources, the development of specific or overall ontologies for these layers is necessary. The Frameworx Information Framework (SID) offers very extensive and mature resource models and binding that can be easily applied to cloud resource. Such models can be adapted within other ontology languages making all both platform and vendor agnostic.
The Information Framework is currently supported by off-the-shelf tools, and provides a recognized information model, which controls complexity and allows for the definition of standardized integration points. Given the popularity and adoption of Frameworx in the communications and defence industries, the availability and scope of Frameworx based ontologies is constantly increasing and is growing to support the needs of Cloud Services

From oncept and terminology pint of view several definitions of "Service Model" can be introduced, each defined with its specific context in mind, such as Cloud Service Model vs. the traditional service model of, say VPN service. There are also some key requirements from the end user perspective and from service designer and provider perspectives around the concept of a "Service Template".

The TM Forum SID takes an information model view, the fundmental concept of SID service model is built upon the Product-Service-Resource relationship and the concept of CustomerFacingService (e.g. APIs exposed to external parties) and ResourceFacingService (e.g. interface that is usually internal and supporting the interaction with its depending resources).

A standardized service template is essential to record service characteristics in a consistent and machine readable form. This template should also help to record information that is intrisic to the service based on the context of business objectives and service objectives such as service dependencies and SLA metrics. TM Forum recognizes also harmonizing the work among OASIS/ TOSCA and recommends harmonization, TM Forum SID and SES to meet these requirements. Quoting from TOSCA draft spec: The TOSCA Service Templates (the model) has to be linked to deployment artifacts for creating actual cloud service instances

Use of catalogues to facilitate SLA management

At the most basic level, a service catalogue provides a portfolio of services that are available to the customer. To drive automated product offering/bounding from various service capabilities in near real time, the Active Catalogue concept (TMF867) has been used that models the same approach as Computer Aided Design (CAD) and Computer Aided Manufacturing (CAM) from the manufacturing business. The key concept is to remove the service and product dependencies from the system, and model them in the catalogue via well-defined ProductSpecification, ServiceSpecification and ResourceSpecifications and their dependencies.

Service catalogue and federated catalogue management are essential to handle the complexity of SLA management for Cloud. Although there is some work being done in the TM Forum, but more synergy in the industry is required to derive consistent methods for Service Templates, management metadata coordination, and management interfaces to be included for all Cloud services.

ETSI Network function virtualization, [81]
To accelerate progress on network functions virtualization a group of operators have been working a joint white paper. A new network operator-led Industry Specification Group (ISG) with open membership is being setup under the auspices of ETSI to work through the technical challenges for network functions Vvrtualisation as outlined in the white paper.

Regarding management and orchestration following statement is made: A consistent management and orchestration architecture is required. Network functions virtualisation presents an opportunity, through the flexibility afforded by software network appliances operating in an open and standardised infrastructure, to rapidly align management and orchestration North Bound Interfaces to well defined standards and abstract specifications. This will greatly reduce the cost and time to integrate new virtual appliances into a network operator's operating environment. Software Defined Networking (SDN) further extends this to streamlining the integration of packet and optical switches into the system e.g. a virtual appliance or network functions virtualisation orchestration system may control the forwarding behaviours of physical switches using SDN.

8.3.6 Analysis recommendations

Based on an analysis of the current activities in standardization organizations on Inventory Management the following **recommendations addressing the NGCOR needs** are given concerning future activities:

- **TM Forum:**
  - The work on TIP generic patterns with information model independent concepts should be continued. In the context of NGCOR an application of these patterns to resource and service inventory domains has turned out to be important. The usage of SID is a good choice for the first step. As soon as inventory definitions are provided by the JWG on MA, the generic TIP patterns can also be applied to this joint model.
  - The work on catalogue management interfaces should be continued. Especially the interfaces between service and resource catalogues with resource and service inventories including information modelling, in line with the work of TIP Inventory, are of interest in the context of NGCOR.
  - In the TAM specification [52] there are some parts to be added concerning catalogue and Inventory Management: Functionality and supported business services for Service Catalogue Management and Resource Catalogue Management, and supported business services for Resource Inventory Management.
  - TM Forum is expected to continue its wide prorams on e2e multi-cloud management area for further detailed specifications of cloud service management interfaces. Especially unform service and resource modeling is seen a key issue from Inventory Management point of view.

- **3GPP SA5:**
  - In 3GPP SA5 the MSDO Model Alignment work on UIM inventory definitions should be considered in furure Inventory specifications as soon as they are available.

- **Multi-SDO JWG on Model Alignment (MA):**

    - o Inventory related objects, attributes and relationships should be defined in the Umbrella Information Model (UIM) according to the requirements from NGCOR, 3GPP and TM Forum.

- **ETSI ISG for NFV**
    - o In the work starting up in ETST ISG a consistent management and orchestration architecture is required to be worked on. To rapidly align management and orchestration north bound interfaces to well defined standards and abstract specifications is of key importance.

8.4 SCENARIOS AND USE CASES FOR ENHANCED INVENTORY MANAGEMENT

8.4.1 Process management approach to the design and implementation of Inventory Management

Within the information-driven business of a service provider the approach to the design and implementation of a future multi-vendor, multi technology resource and service inventory solution has to include the implementation of an **information governance process**. This is one of the key success factors.

A process driven approach to the design and implementation of a future multi-vendor, multi technology resource and service inventory solution is another key success factor. This implies to start with process analysis and use case definitions as well as with the analysis of information needs & consumption for the process groups: Operations (fulfilment and assurance processes) and operations support and readiness as well as lifecycle management processes incl. planning and deployment from the eTOM.

From process and use case definitions requirements towards the information model, the connectivity needs and architectural requirements can be derived.

Dominated by the process view, an Inventory Management system becomes a dynamically changing system presenting current, past and future states of the network and services. Inventory becomes a real heart of the OSS, loosely coupled with OSS applications in the eTOM-domains of product/ service/ resource life cycle management, fulfilment and assurance.

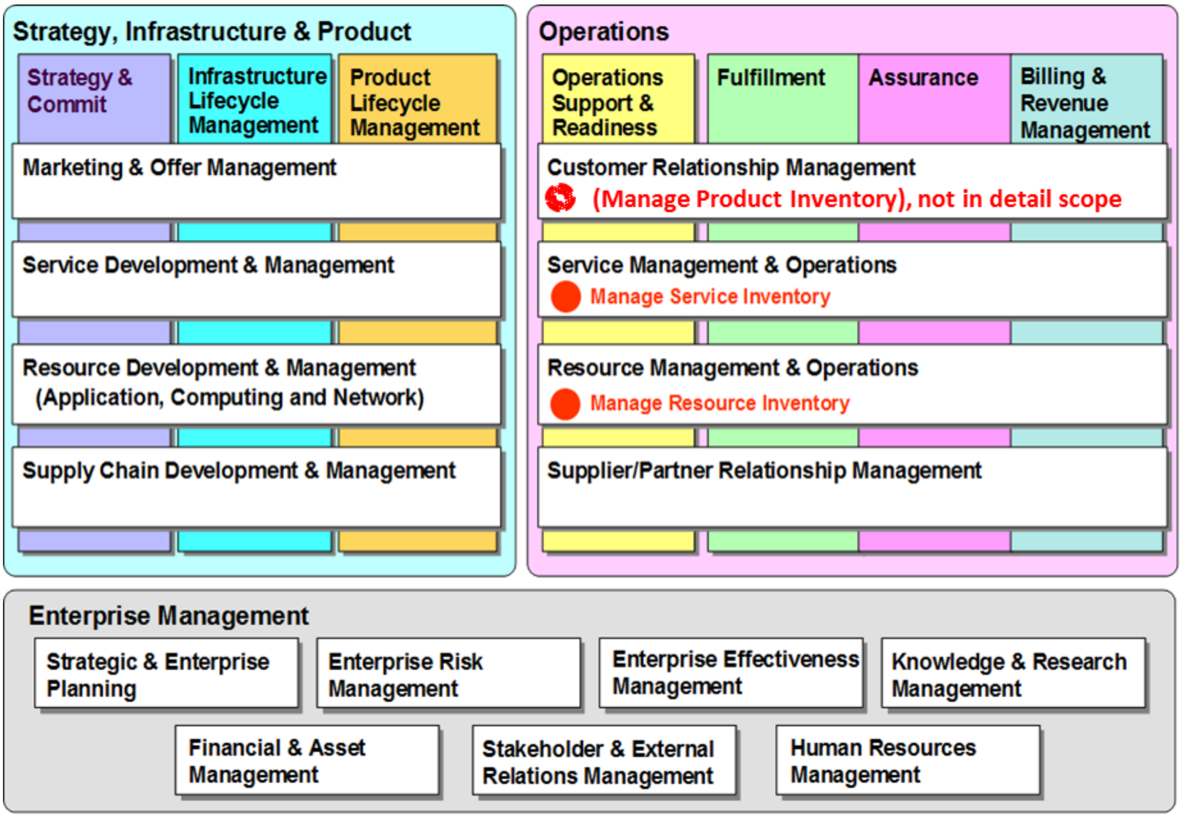


Figure 10-1: Key scope of InvM stream in the eTOM framework (i.e. Product Inventory Management is out of detailed scope)

In the layered structure of eTOM it regards especially

- The service management layer where Service Inventory Management provides benefits by
  - Managing all service related data.
  - Providing abstraction layer on top resource management layer and via that enabling modular and componentized usage of resources as support of different services offered by the operator.
  - Enabling flexible and componentized customer product offerings composed of different service entities and via that reducing time to market in new product launches or product offering changes.
- The resource management layer where Resource Inventory Management provides benefits by
  - Managing all resource related data.
  - Provides accurate view of actual status of resources.
  - Enabling flexible and componentized usage of resources as support for different services.

Inventory Management will be essential to support Next Generation technologies enabling automation. Many operators are also developing international operations cross affiliates and cross countries which requires consolidation and harmonization of inventory data. Many of the desired improvements in efficiency from NGMN automation will not be achievable due to current inconsistent end-to-end management of inventory data.

To run the operations business of a service provider efficiently, the organization relies on accurate information provided in the form needed to do the work. The common data managed by inventories and respective processes have to ensure that the data providing that information is:

- Managed according business requirements.
- Unique - there should be only one master copy.

- Correct and up to date.
- Of high integrity.
- Delivered in the form needed.
- Be configurable to adapt inexpensively to new requirements from new business model, government and corporate policy/ governance, and technologies

These goals will not be reachable without harmonizing current practices and processes for Inventory Management across the different parts of the technology organization to reflect the full information life cycle. Lack of a harmonized Inventory Management would mean:

- Not knowing what data to hold.
- Not having all the required data.
- Data is inconsistently held in multiple systems.
- Data is missing or inaccurate.
- Data is not really "owned".
- Data is not shared.

8.4.2 Overview scenario on process flows concerning Service Inventory and Resource Inventory Management support for development, implementation and operations processes – Generic use case – UC-Gen-SIM-RIM-1

This chapter analyses an overview of process flows within the operators' environment envisioning the role of Service Inventory Management and Resource Inventory Management for different processes. The related processes span from product development and their implementation to different operations processes.

UC-Gen-SIM-RIM-1 This overall scenario is presented as a generic use case for all Inventory Management (identifier UC-Gen-SIM-RIM-1) and is related to and addressing the whole requirements suite.

The more detailed specific use cases in the following chapters are detailing further the analysis of selected process and sub-processes. The process flows are described using TM Forum eTOM concepts and principles.

The capability for launching, offering and marketing competitive products at the marketplace is the key element of success from operator business perspective. Product development and design processes develop new products or services and product or service enhancements and new features, ready for implementation by the operations processes. Product development and design addresses also major product and service updates and enhancements as well as withdrawal of product from the marketplace.As a result detailed product specifications are documented and captured in an appropriate enterprise repository, called product catalogue. In the product and customer domain various other inventories may exist, for example offering inventory, sales inventory, customer inventory.
Product specifications include e.g.:

- Detailed product-related technical, performance and operational specifications.
- Customer manuals.
- Required product features.
- The specific service and resource requirements and selections.
- Specific performance and operational requirements.
- Support activities.

* Any product specific data required for the systems and network infrastructure.

Further on, service development and design processes use product specifications as input for development of new or enhanced service types and service components. Service development also addresses process and procedure implementation, systems changes and customer documentation as well as rollout and testing of the service type and capacity management. The detailed service specifications are documented and captured in an appropriate enterprise repository, called service catalogue. Service specifications include e.g.:

* Detailed service-related technical and operational specifications.
* Customer manuals.
* Required service features.
* Specific underpinning resource requirements and selections.
* Specific operational and quality requirements.
* Support activities.
* Any service specific data required for the systems and network infrastructure.
* Specifications and tools (SDK) for product developers, including 3rd parties.

Resource development and design processes develop new, or enhance existing technologies and associated resource types, so that new products are available to be sold to customers. These processes also retire or remove technology and associated resource types, which are no longer required or used. Within resource development and planning it is considered whether to acquire resources from outside, taking into account the overall business policy in that respect. Resource types may be built, or in some cases leased from other SPs or suppliers. To ensure the most efficient and effective solution can be used, negotiations on network level agreements with suppliers or partners are paramount for both building and leasing.

The detailed resource specifications are developed using detailed service specifications as input. Resource development and design processes ensures that all detailed resource specifications are produced and appropriately documented and captured in an appropriate enterprise repository, called resource catalogue. Resource specifications include e.g.:

* Detailed resource-related technical, performance and operational specifications.
* Specific technology requirements.
* Selections required for the systems and network infrastructure.
* Support activities.
* Any resource specific data required for the systems and network infrastructure required for the systems and network infrastructure.
* Necessary manuals.

Information provided by catalogues, product catalogue, service catalogue and resource catalogue can be accessed by authorized OSS/ BSS applications in order to support the efficient handling of the operators' business processes. Moreover important for modular and componentized products is the modeling of relations between products, their service components and underlying resource components.

* For automated **fulfillment,** process service and resource catalogue can provide defined rules for execution of provisioning logic and for creation of corresponding service instances and resource instances according the defined service models and resource models. In the use case analysis an example of catalogue driven fulfillment is presented (see chapter 4.3.4.1) and respective requirements in chapter 5.
* The information held in catalogues (specifications) and inventories (instances) respectively is utilized widely in **assurance** processes. The benefits are gained by having all information related to service infrastructure and resource infrastructure in a uniform and structured way; for example all service models, all physical and logical resources of a converged infrastructure, their naming, interrelations and

topologies, performace and quality measuring characteristics etc. Assurance processes and their users don't need to manage and administrate all service and resource information; they only need to have relevant information which is needed in its tasks e.g. for processing the alarms or securing the quality or performance (see chapters 4.3.5 and 4.4.1).

Like stated above, this overview process flow, usage and role of service and resource inventory management represent generic use case – UC-Gen-SIM-RIM-1. As a consequence of the generic nature of UC-Gen-SIM-RIM-1 the whole requirements set described in chapter 5 can be regarded as resulting requirements from UC-Gen-SIM-RIM-1. However to be noted when reading use case templates and requirements templates NGCOR does not refer UC-Gen-SIM-RIM-1 when there is a more specific use case defined and resulting detailed requirements.

Figure 7 shows the overview of process flows concerning Service Inventory and Resource Inventory Management support product and service development main phases, implementation and operations processes.

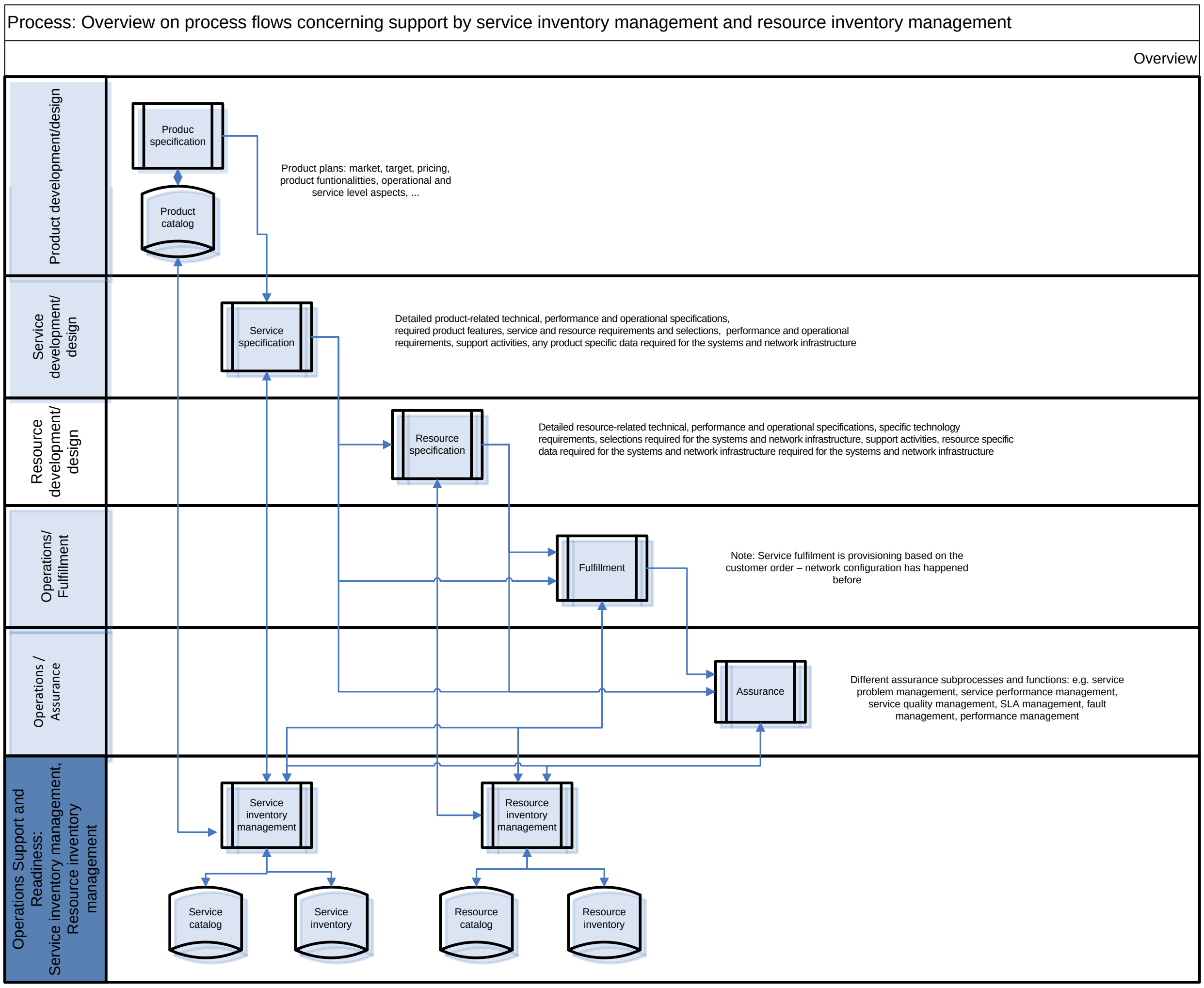


Figure 10-2: Overview scenario on process flows concerning Service Inventory Management and Resource Inventory Management support for different process from development to operation

8.4.3 Scenarios and use cases related to support of Service Inventory Management

In this chapter various scenarios and use cases related to Service Inventory Management are presented. Those are highlighting the benefits to have all service related information managed in a uniform and structured way in support for different processes in operator's business.

NGCOR realizes the big challenge to achieve unanimous understanding about concept of 'service'. Within the whole 'communication ecosystem' there exists enormous amount of alternatives for determining what a service depending on the context is. Having operators' business and product offerings as the starting point for service modeling leads to various considerations of for example; what is business logic and operator's role in the value chain, which tangible assets or intangible things are objects for product offerings, which part of value chain the service addresses (e.g. providing network services, providing content services, providing different forms of cloud services etc). In principle service information modeling should be generic and applicable to all kind of services and different business models.

It is to be understood that there are possibilities to consider tens or hundreds process use cases and various levels of details of them. The viewpoint of NGCOR has been to analyze a selected set of use cases, which is regarded to give comprehensive rationale for Service Inventory Management overall with main principles, usage, concepts and benefits of it.

8.4.3.1 Scenarios and use cases related to Service Inventory Management support for product and service development and planning

First process area analyzed is Service Inventory Management support for product and service development processes.

The related use cases are addressing:

- Analyzing product specifications from customer perception and customer usage point of view for defining appropriate service information models to represent the product within service management. Typically the analysis contains: positioning of the service in the full service portfolio and hierarchy, analysis if product or product parts are addressing similar or new service or service components, analyzing of detailed product features and characteristics – These models are definitions of customer facing services (CFSs).
- Analyzing product specifications from production and technology point of view for defining appropriate service information models representing the product within service management .Typically the analysis contains: analyzing which kind of technology is needed for implementation of product features, structuring and mapping the technology needs for concrete network and IT platforms, analyzing the detailed operational and performance aspects needed from each technology platform to fulfill the product features – These models are definitions of resource facing services (RFSs).
- Analyzing service models details from system architecture design process point of view:
    - Structures, hierarchies, relations and associations (CFS and RFS structures).
    - Models for control and guidance of order fulfillment and provisioning.
    - Models to support SLA, support of aggregation, calculation of KQI/KPI
    - Models to support service impact analysis.

8.4.3.1.1 Use case: Deriving service specifications from product specification and modeling service reflecting the underlying technology infrastructure (generic) – Use case UC-SIM-1

This use case presents specifically how service development and design processes further on use product specifications as input for development of new or enhanced service types and service components, determined as customer facing services (CFSs). Then secondly this use case presents how service development and design processes further on use customer facing service specifications as input to analyze and identify the technology infrastructure components needed to implement the specified products, the technology infrastructure components determined as resource facing services (RFSs).

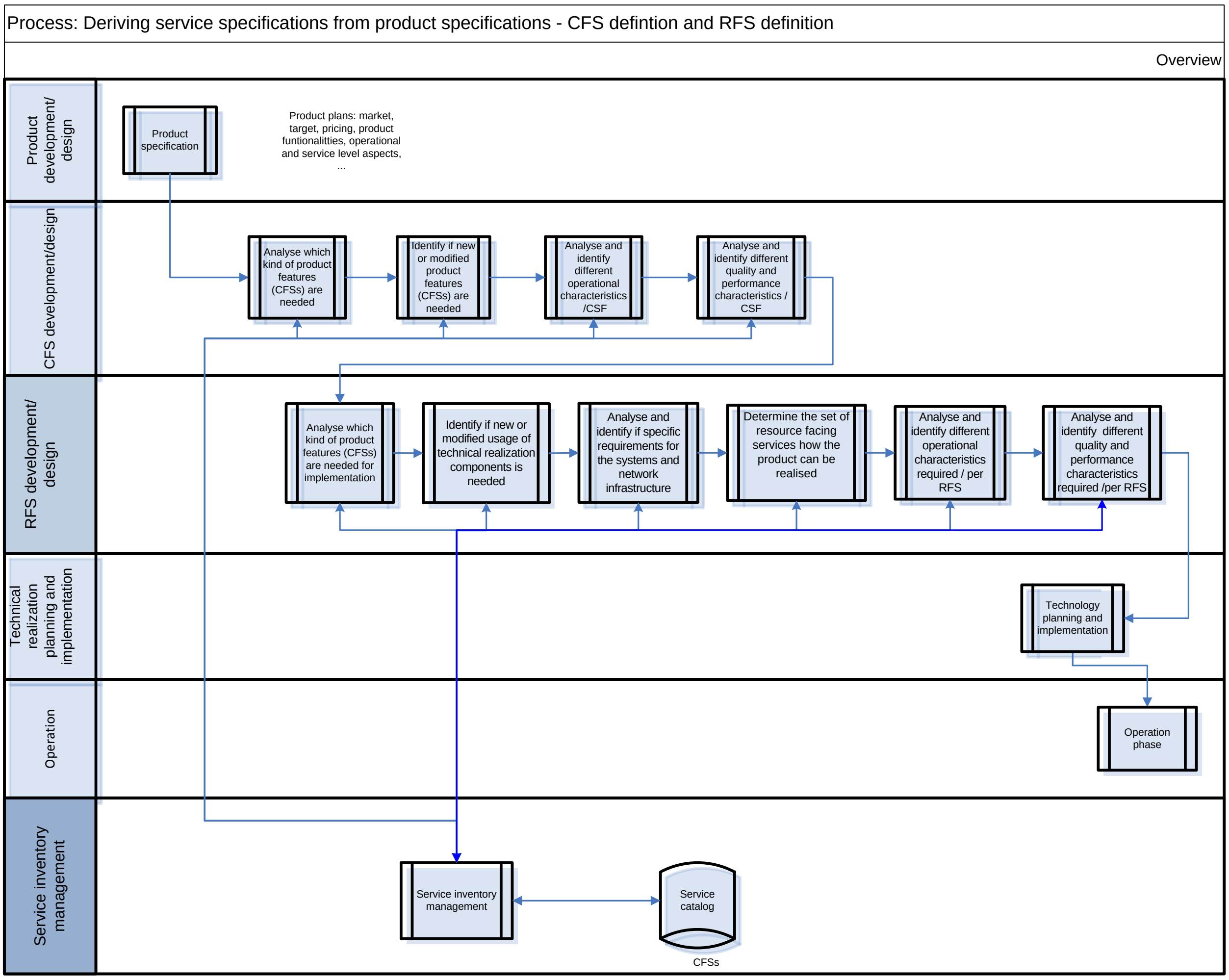


Figure 10-3: Deriving service specifications from product specifications, CFS definition and RFS definition

UC-SIM-1

Identifier: Deriving service specifications from product specifications	**Use Case Id: UC-SIM-1**
Originating Process : Product development and design	**Actor role:** Service developer/designer, Technical implementation developer/designer

Precondition(s) and Dependencies:	
Precondition(s) and Dependencies: As part of product development and design, service specification needs to be detailed to reflect the product offering upwards and the needed underlying technical infrastructure resources Product specification is planned and created Product specification repository, Service specification repository and Resource specification repository capabilities are existing embodied by respective catalogues	
Scenario description: **CFS definition** • Service developer/designer enters to analysis of product specification • Analyse and identify different product features available for customer usage (Customer facing services) • Identify if new or modified products/product features are specified • Analyse and identify different operational characteristics required / per CFS • Analyse and identify different quality and performance characteristics required /per CFS • All product features are analysed to form a viable customer facing service specification • Customer facing services are defined **RFS defintion** • Service developer/designer enters to technical realization analysis of product specification, assisted by technical implementation developer/designer • Analyse and identify different customer facing services needed for implementation • Identify if new or modified usage of technical realization components is needed for products/product features • Analyse and identify if specific requirements for the systems and network infrastructure exist • Determine the set of resource facing services how the product can be realised • Analyse and identify different operational characteristics required / per RFS • Analyse and identify different quality and performance characteristics required /per RFS • All product features are analysed to form a viable resource facing service specification • Resource facing services are defined	
The resulting requirements / capabilities: REQ-InvM (1), REQ-InvM (2), REQ-InvM (3), REQ-InvM (4), REQ-InvM (5), REQ-InvM (6), REQ-InvM (7), REQ-InvM (8), REQ-InvM (9), REQ-InvM (10), REQ-InvM (11), REQ-InvM (12), REQ-InvM (13), REQ-InvM (14), REQ-InvM (15), REQ-InvM (16), REQ-InvM (17), REQ-InvM (18), REQ-InvM (19), REQ-InvM (20), REQ-InvM (21), REQ-InvM (22)	
Justification (Business benefits/Impact if not Implemented): All service related information managed in a uniform and structured way in support for different processes in operator's businesses	
Miscellaneous Comments / Useful hints:	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date :** **NGMN NGCOR /June 2013**

8.4.3.1.2 Use case: Analyzing service models details from system architecture design process point of view - the service meta-model – Use case UC-SIM-2

The purpose of this use case is to analyze high level design process and principles from service modeling point of view – i.e. concerning product and service development from IT system architecting point of view. The use case attempts to describe and envision which kind of service information and service information model parts need to be specified and considered to be suitable and concrete enough for applying in various real service scenarios and their management. This generic modeling principles can be regarded as basis for service meta model. The intention is to analyze and identify for example what kind of service data has to be defined and managed in the Service Inventory ManagementService Inventory Management context and for what kind operations and interactions the service data is object to when taking into account various processes supported by OSS architecture. The intention is not to try to reach detailed information model specification level, e.g. UML modeling, but instead to identify the requirements on rather high level for service modeling. These service modeling principles apply to a layered management architecture where different layers (product management, service management and resource management) have separate concern of each layer's model but these models in each layer are highly dependent on each other.

The purpose of service modeling is to produce service specifications and templates to embody service information model structure and details. The following service information model design aspects are seen the main features of the design. This use case relates to various Service Inventory Management requirements:

UC-SIM-2

Identifier: Analyzing service models details from system architecture design process point of view - the service meta-model	**Use Case Id: UC-SIM-2**
Originating Process: Product development and design	**Actor role:** IT system architect
Precondition(s) and Dependencies: Product specification is planned and created Product specification repository, Service specification repository and Resource specification repository capabilities existing embodied by respective catalogues	
Scenario description: • At first stage it is relevant to identify building blocks from which products and product offerings on upper layer can be constructed in a flexible way. Technical realization aspects identified from product descriptions representing technology infrastructure constitute another set of structure blocks. This analysis produces service information model entities which typically can be visualized as tree structure where associations between product, service and resource layer entities are shown. Within service information model structures additional modularity can be achieved via composition of lower core level entities (in TMF SID terms defining CFS, RFSs and resources - logical and physical). Service information model details in terms of attributes are defined based on required product feature characteristics. Technical realization capabilities represented by respective service model entities constitute another set of attributes of entities to make a consistent modeling vertically through layers. As an overall goal in design is to allow utmost flexibility and dynamics in modification of services and service structures to enable rapid product launches and new technology introductions as part of products. General good design practices such as modularity, reuse of previous definitions, entity composition analysis from core entities etc. is promoted to be applied. The design process can also be iterative and checking top-down and bottom-up. • Service information models need to be designed to include capabilities to support for automatic fulfillment and provisioning. In this perspective service information model needs to include e.g.: o Information for mapping product order parameters to service order parameters	

- Feasibility checking and validation information of parameters - Service fulfillment execution and orchestration rules and related information for responses and exception handling - Mapping the service order parameters to meaningful set of resource activation parameters for delegation to resource management layer below • The common service information models design needs to take into account also capabilities to support for service assurance. In this perspective service information model needs to include e.g.: - Information on mapping of the customer SLA agreement parameters to service level KQIs/KPIs - Information on calculation and aggregation of customer SLA based service level KQI/KPIs - Values for thresholds and time dependencies of SLA parameters and respective service level KQIs/KPIs - Mapping information from SLA requirements to resource KPIs which have their specific measurement capabilities - Establishment of KQI/KPI calculation and aggregation hierarchy derived from service/resource information model structure - Information on consequences if service quality or service performance targets are not met - Information for support of service impact analysis needs utilizing the information from service/resource information model structure
The resulting requirements / capabilities: REQ-InvM (1), REQ-InvM (2), REQ-InvM (3), REQ-InvM (4), REQ-InvM (5), REQ-InvM (6), REQ-InvM (7), REQ-InvM (8), REQ-InvM (9), REQ-InvM (10), REQ-InvM (11), REQ-InvM (12), REQ-InvM (13), REQ-InvM (14), REQ-InvM (15), REQ-InvM (16), REQ-InvM (17), REQ-InvM (18), REQ-InvM (19), REQ-InvM (20), REQ-InvM (21), REQ-InvM (22)
Justification (Business benefits/Impact if not Implemented): All service related information managed in a uniform and structured way in support for different processes in operator's business
Miscellaneous Comments / Useful hints:
Required timeline (link to roadmap) / Priority: — **Requirement Owner / Date:** NGMN NGCOR /June 2013

8.4.3.2 Scenarios and use cases related to Service Inventory Management support for infrastructure sharing business scenarios

The scenarios defined in this chapter are to identify the use cases where service inventory, service model or broadly speaking the service centric approach for network management can help to realize the infrastructure sharing business scenarios. The intension is also to identify the area of collaboration between the streams of NGCOR project: Service Inventory and Business Scenarios for Converged Operations.

8.4.3.2.1 Use Case: Requesting a Capacity reservation from the shared RAN to be able to support mobile customers – Use case UC-SIM-3

UC-SIM-3

Identifier: **Requesting a service level capacity reservation from the shared RAN to be able to support mobile customers**	**Use Case Id: UC-SIM-3**
Originating Process : Desing if shared RAN	**Actor role:** MasterOperator – an operator managing the shared RAN (including CELL sharing) SharingOperator1 – a first operator which uses (shares) the RAN managed by the MasterOperator SharingOperator2 – a second operator which uses (shares) the RAN managed by the MasterOperator

Precondition(s) and Dependencies:

SharingOperator1, SharingOperator2 and MasterOperator has signed the agreement specifying the rules of managing and using the shared RAN – "shared RAN agreement"

SharingOperator1 has re-assessed its mobile customer demand and customer experience metrics relevant to the shared RAN

Scenario description:

- SharingOperator1 decides that it needs to increase the service level provided by the shared RAN to improve the customer experience of its mobile customers
- Or: Master operator notifies Sharing Operators that the utilization of its RAN capacity pools for certain service types exceed certain threshold
- SharingOperator1 defines new characteristics of the Resource Facing Service (RFS) RAN which is used to model the service provided by the RAN
- SharingOperator1 issues the service order using the RFS RAN service as an argument of the order. The order is passed to the MasterOperator
- MasterOperator using its expertise to translate the service requirements received from SharingOperator1 into the requirements towards the RAN configuration. Doing that MasterOperator takes into account the limited resources of the managed RAN, the service level which was previously requested by SharingOperator2 and the "shared RAN agreement" policy
- MasterOperator modifies the configuration of the shared RAN in a way that the requirements specified by the SharingOperator1 are satisfied
- The shared RAN has been reconfigured by the Master Operator in a way that satisfies the service order issued by the SharingOperator1
- The SharingOperator1 now can have the customer experience of its mobile customers improved

The resulting requirements / capabilities:

REQ-InvM (10), REQ-InvM (11), REQ-InvM (12)

Justification (Business benefits/Impact if not Implemented):

- To define the requirements towards the shared RAN to be able to provide the adequate service level to support mobile customers
- To manage the RAN as "a black box" service rather than manage directly configuration of the RAN

• To delegate the Configuration Management expertise (low level technical expertise) to the operator of the shared network • To avoid "overwriting" the configuration of the RAN by operators sharing the same RAN • To enable sharing operators to define their requirements towards the shared RAN in a way they can be "fairly" treated by the operator managing the shared RAN
Miscellaneous Comments / Useful hints: If the service level requested by SharingOperator1 can't be satisfied due to the limited resources (without violating the SharingOperator2 service level requirements), MasterOperator reports the problem to the SharingOperator1 specifying what the maximum level of service can be provided (using the RFS RAN service model to formally define what can be requested by the SharingOperator1)

Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.3.3 Scenarios and use cases related to Service Inventory Management support for Configuration Management

The scenarios defined in this chapter are to identify the use cases where service inventory, service model or broadly speaking the service centric approach for network management can help realize the Configuration Management scenarios. The intention is also to identify the area of collaboration between the streams of NGCOR project: Service Inventory and Configuration Management.

8.4.3.3.1 Use Case: Requesting a capacity reservation from the RAN to be able to support mobile customers – Use case UC-SIM-4

This use case is somehow similar to the use case in chapter 4.3.2.1. It can be considered as more generic one as it can be applied not only for shared infrastructure scenarios but also to the scenarios where an operator decides to outsource Configuration Management or even without outsourcing Configuration Management, but with the intention to seamlessly integrate a department which analyses the needs from service perspective with a network Configuration Management department.

UC-SIM-4

Identifier: **Requesting a capacity reservation from the RAN to be able to support mobile customers**	**Use Case Id: UC-SIM-4**
Originating Process : Desing of RAN management and configuration	**Actor role:** CMDepartment – a department (or third party to which CM is outsourced to) managing the configuration of the RAN ServiceDepartment – a department which manages the service domain of an

	mobile operator
Precondition(s) and Dependencies: ServiceDepartment has re-assessed its mobile customer demand and customer experience metrics relevant to the RAN	
Scenario description: • ServiceDepartment decides that it needs to increase the service level provided by the RAN to improve the customer experience of its mobile customers • ServiceDepartment defines new characteristics of the Resource Facing (RFS) Service RAN which is used to model the service provided by the RAN • ServiceDepartment issues the service order using the RFS RAN service as an argument of the order. The order is passed to the CMDepartment • CMDepartment using its expertise translates the service requirements received from ServiceDepartment into the requirements towards the RAN configuration. CMDepartment translates the characteristics of the RAN Service into the configuration parameters and potentially using the template mechanism • CMDepartment modifies the configuration of the RAN in a way that the requirements specified by the ServiceDepartment are satisfied • If the service level requested by ServiceDepartment can't be satisfied due to the limited resources , CMDepartment reports the problem to the ServiceDepartment specifying what the maximum level of service can be provided (using the RFS RAN service model to formally define what can be requested by the ServiceDepartment) • The RAN has been reconfigured by the CMDepartment in a way that satisfies the service order issued by the ServiceDepartment. • The ServiceDepartment now can have the customer experience of its mobile customers improved	
The resulting requirements / capabilities: REQ-InvM (10), REQ-InvM (11), REQ-InvM (12)	
Justification (Business benefits/Impact if not Implemented): • To define the requirements towards the RAN to be able to provide the adequate service level to support mobile customers. • To managed the RAN as "a black box" service rather than manage directly configuration of the RAN • To delegate the Configuration Management expertise (low level technical expertise) to the network Configuration Management department	
Miscellaneous Comments / Useful hints:	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.3.4 Scenarios and use cases related to Service Inventory Management support for Service Fulfilment

The scenarios on this area highlight the usage and management of service catalogue/ service inventory information during service fulfillment.

8.4.3.4.1 Use Case: Service catalogue driven customer service order fulfilment process – Use case UC-SIM-5

This use case demonstrates the idea of data (catalogue) driven fulfillment process which is a complementary concept to “process driven inventory”. This concept aims at significantly reducing time-to-market by treating the service design done in the service catalogue as the model enabling to drive the automated order fulfillment process (high level execution plan). This is to be achieved by leveraging a meta-model describing the service structure capable of driving the fulfillment process.

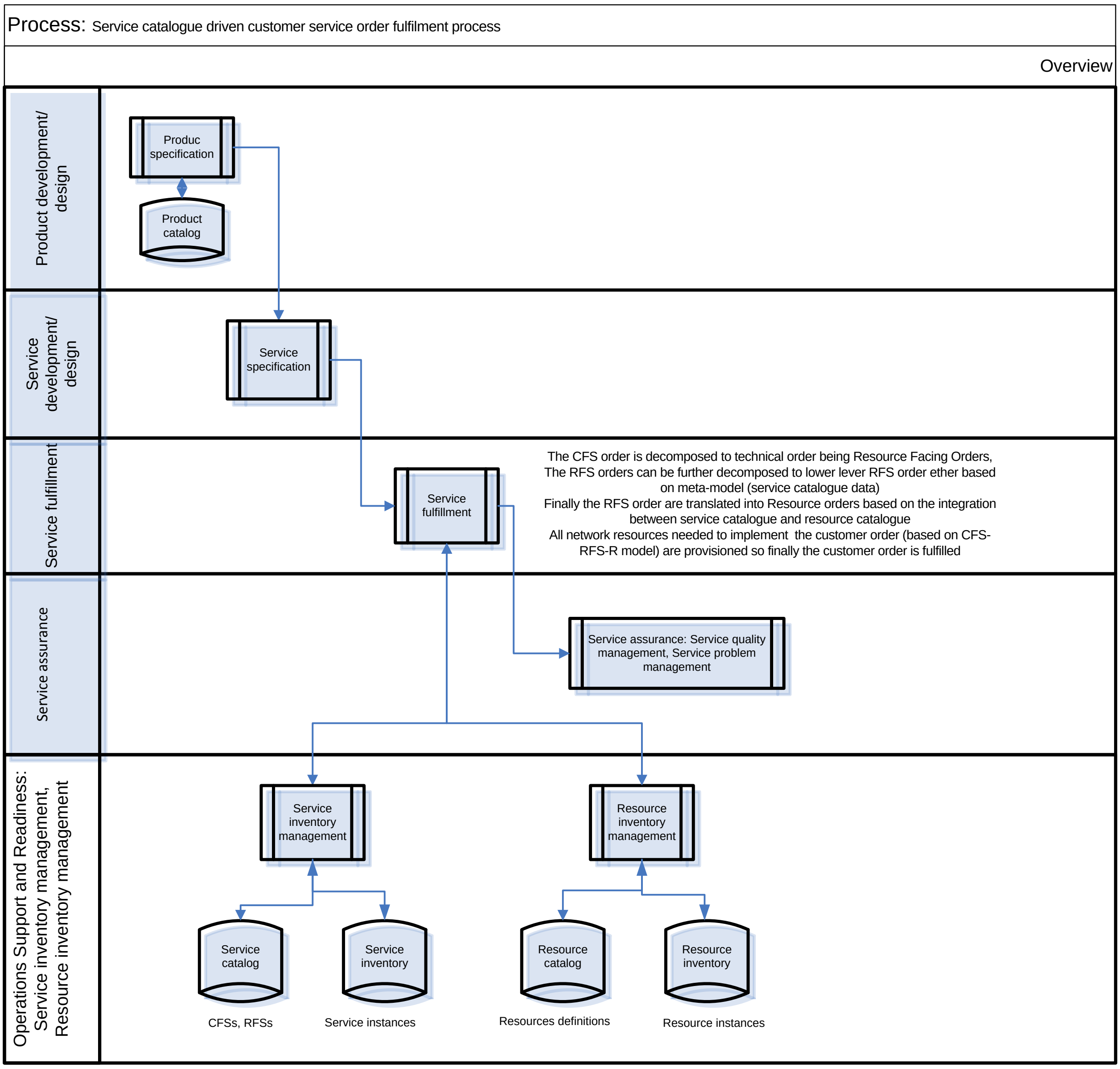


Figure 10-4: Service catalogue driven customer service order fulfilment process

UC-SIM-5

Identifier:	**Use Case Id: UC-SIM-5**

<table>
<tr><td>Service catalogue driven customer service order fulfilment process</td><td></td></tr>
<tr><td>Originating Process :
Customer order mangement for delivery of a service requested by the customer</td><td>Actor role:
A customer, service fulfilment system</td></tr>
<tr><td colspan="2">Precondition(s) and Dependencies:
A new product has been designed comprising the full product model spanning Product-Service-Resource model</td></tr>
<tr><td colspan="2">Scenario description:
• During the order capture a customer has ordered the product, his order is materialised as the Customer Facing Service (CFS) instance with characteristics having values (For example Broadband Internet speed characteristic value = 10Mbit/s)
• The CFS order has been sent to the fulfilment system which validates the order based on a service specification definition retrieved from a service catalogue
• The CFS order is decomposed to technical order being Resource Facing Service Orders. This generates the high level execution plan which steps include the RFS orders invocation. The flow of orders (the execution plan flow) is calculated based on meta-model extending the CFS-RFS Specification of TMF SID model
• The RFS orders can be further decomposed to lower lever RFS order either based on meta-model (service catalogue data) or can trigger the low lever execution plan which was designed for the RFS
• Finally the RFS orders are translated into Resource orders based on the integration between service catalogue and resource catalogue (this includes also integration of service and resource inventories)
• All network resources needed to implement the customer order (based on CFS-RFS-R model) are provisioned so finally the customer order is fulfilled
• Customer has the service delivered, the service inventory has a complete description of the service being delivered in a form of service instances (both CFS-RFS-(R) instances)</td></tr>
<tr><td colspan="2">The resulting requirements / capabilities:
REQ-InvM (1), REQ-InvM (2), REQ-InvM (3), REQ-InvM (4), REQ-InvM (5), REQ-InvM (6), REQ-InvM (7), REQ-InvM (8), REQ-InvM (9), REQ-InvM (13), REQ-InvM (44)</td></tr>
<tr><td colspan="2">Justification (Business benefits/Impact if not Implemented):
• To automate the process as much as possible
• Use the service design done in the Service Catalogue as a driving model for the process
• Reduce time-to-market by basing the fulfilment process on the service catalogue data</td></tr>
<tr><td colspan="2">Miscellaneous Comments / Useful hints:</td></tr>
<tr><td>Required timeline (link to roadmap) / Priority:</td><td>Requirement Owner / Date:
NGMN NGCOR /June 2013</td></tr>
</table>

8.4.3.5 Scenarios and use cases related to Service Inventory Management support for Service Assurance

The scenarios in this area highlight the usage and management of service catalogue/ service inventory and resource catalogue/resource inventory information during service assurance. These use cases exemplify the benefits of having well-structured, consistent, and in a unified way modeled information about services and resources for different usage in service assurance processes and applications.

The common service inventory data can be used for example by:

- Service quality management (use case presented)
- Service performance management.
- SLA management.
- Service problem management/ trouble ticketing (use case presented).
- Providing service inventory data for different queries from operations systems and its users.

The following process flow presents the main interaction between service assurance (e.g. service quality management, service problem management), and Service Inventory Management and Resource Inventory Management.

The use cases presented can be regarded as examples to represent relationship and interaction between Inventory Management and Service aAssurance. Other use cases for support of further assurance functional areas can be defined in later work.

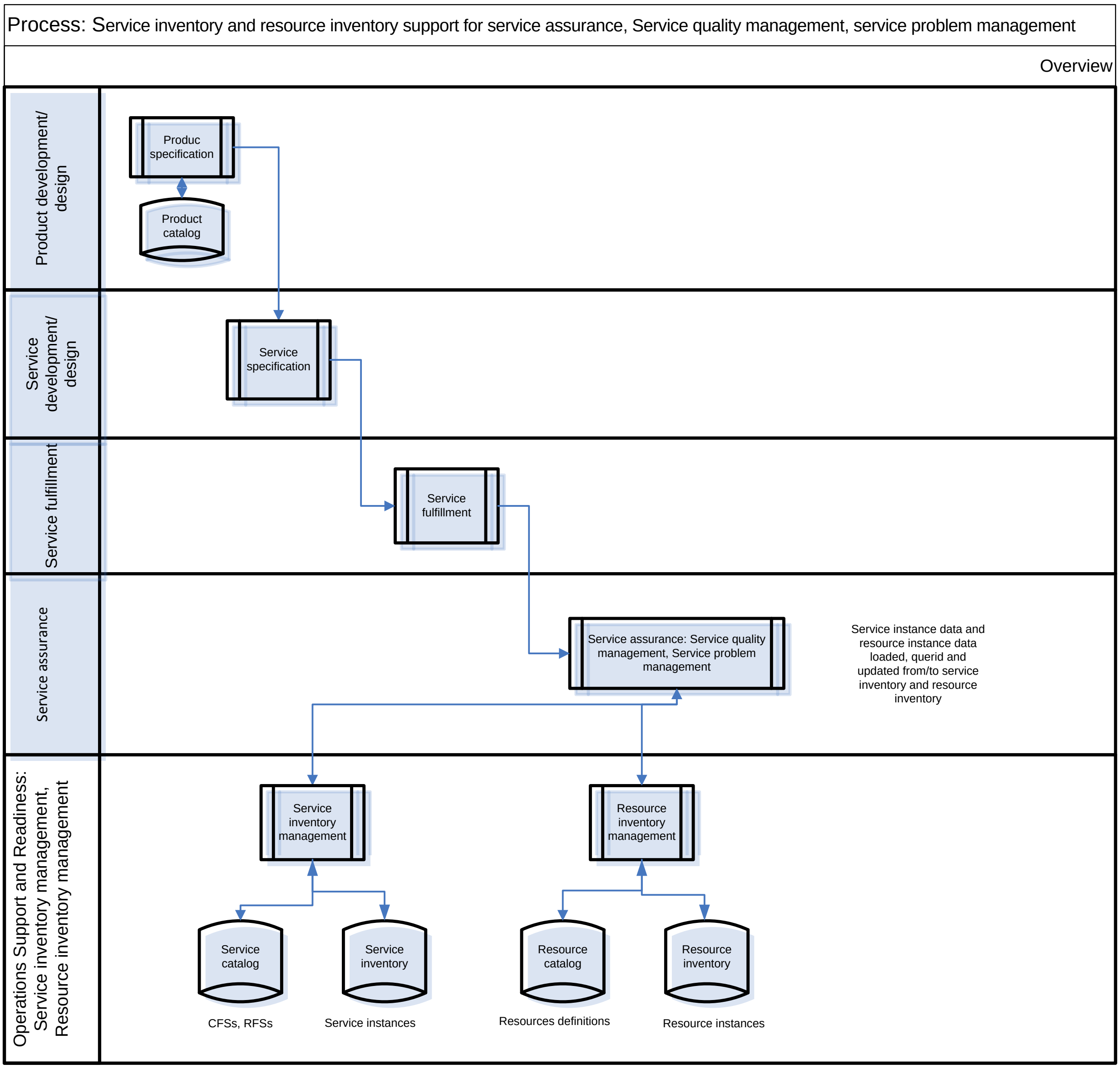


Figure 10-5: The main interaction between service assurance (e. g. service quality management, service problem management) and Service Inventory Management and Resource Inventory Management.

8.4.3.5.1 Use case: Service Inventory Management support for Service Quality Management – Use case UC-SIM-6

UC-SIM-6

Identifier: **Service Inventory management support for service quality management**	**Use Case Id: UC-SIM-6**
Originating Process : Continuous service quality surveillance or specific service quality reporting request	**Actor role:** Operation quality manager Service inventory mgmt Resource inventory mgmt Service quality management system
Precondition(s) and Dependencies: A service has been designed comprising the full service model spanning Product-Service-Resource model layers Service Inventory Management and Service quality management systems are ready for co-operation and interaction Services are 1) provisioned for operation and 2) launched and in production	
Scenario description: • OSS system environment concerning Service Inventory Management and service quality managment interaction starts with Service Inventory Management enabling service quality management by providing relevant service model data. The provided service model data contains: produt-service-resource entity model, KQI definitions of service entities including mapping to the corresponding product SLA metrics and resource KPI defintitions, KQI calculation and aggregation principles from lower layer KPIs as well as support for SLA fulfillment calculations, KQI thresholds and potential timing parameters • SQM system may instanciate relevant part of service model and KQI model for its internal funtioning • Service Inventory Management provides updated service and KQI model information to service quality management whenever service model is changed or quality management requirements are changed	
The resulting requirements / capabilities: REQ-InvM (1), REQ-InvM (2), REQ-InvM (3), REQ-InvM (4), REQ-InvM (5), REQ-InvM (6), REQ-InvM (7), REQ-InvM (8), REQ-InvM (9), REQ-InvM (15), REQ-InvM (16), REQ-InvM (47),	
Justification (Business benefits/Impact if not Implemented): Service inventory provides a well-structured and consistent service model for service quality management processes and applications. Service inventory provides to Service Quality Manager all service information to allow correct monitoring of Quality of Service (QoS) according to specific rules defined. Data model contributes to required data aggregation (on SQM) for quality analysis and to manage and end-to-end service mapping.	
Miscellaneous Comments / Useful hints:	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date :** **NGMN NGCOR /June 2013**

8.4.3.5.2 Use case: Service Inventory Management support for Service Problem Management: Impact analysis and root cause analysis – Use case UC-SIM-7

UC-SIM-7

Identifier: **Service inventory Management support for Service Problem Management: Impact analysis and root cause analysis**	**Use Case Id:** **Use Case Id: UC-SIM-7**
Originating Process : Continuous service problem management process or specific service problem reporting request	**Actor role:** Operation quality manager Product Inventory mgmt Service inventory mgmt Resource Inventory mgmt Service Problem management system
Precondition(s) and Dependencies: Services are 1) provisioned for operation 2) launched and in production	
Scenario description: • Service/network operation center identifies a troubled resource • Service/network operation center creates Resource Trouble ticket • and sends it to Service Problem Management • Service Problem management receives Resource Trouble ticket • Resource Inventory is queried to find what service (s) (by ID or references) is consuming the resources • Service Problem Management checks if there is already Service Trouble Ticket (s) associated with the Resource. • If not, create Service trouble ticket (s), associate it with Resource trouble ticket and send it to appropriate system • Service inventory is queried to find the associated Product (s) • Product inventory is queried to find the associated Customer (s) • Service Problem Management checks if there are already customer product trouble tickets related to the services • If yes, associate the service TT(s) to the customer product TT(s) • If not, create Customer Product TT(s) with associated Service TT(s) • and send to appropriate systems (like CRM) • The impacted customer product (s) are identified, and there are associated Product Trouble tickets	
The resulting requirements / capabilities: REQ-InvM (1), REQ-InvM (2), REQ-InvM (3), REQ-InvM (4), REQ-InvM (5), REQ-InvM (6), REQ-InvM (7), REQ-InvM (8), REQ-InvM (9), REQ-InvM (14), REQ-InvM (46)	
Justification (Business benefits/Impact if not Implemented): Service Inventory Management provides a well-structured and consistent service model for service problem management processes and applications. Service Inventory Management provides to Service Problem Manager all service information, including the other consumed Services, Resources, as well as association to Product and to	

Customer. Such relationship can help to identify impacted services and customers in case of resource failure, or planned maintenance activities, to correlate with or supress customer trouble tickets. On the other direction, such relationship can support root cause analysis to indentify troubled resource for given problematic service(s).	
Miscellaneous Comments / Useful hints:	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date :** **NGMN NGCOR /June 2013**

8.4.4 Scenarios and use cases related to support of Resource Inventory Management

In this chapter several scenarios and use cases are presented to exemplify how Inventory Management can support effectively some key operational and lifecycle processes.

The scenarios and use cases deal with Resource Inventory Management support and show benefits to have uniform and well-structured Information Management for all resources throughout the full lifecycle of resources. From each use case more detailed requirements are then derived.

The use cases which are presented can be regarded as examples to represent relationship and interaction between Inventory Management and service assurance. Other use cases for support of other assurance functional areas can be defined in later work.

8.4.4.1 Scenarios and use cases related to Resource Inventory Management support for Fault Management

In this scenario focus is on interrelation and interaction between Resource Inventory Management and Fault Management, with Fault Management being one of key and basic applications within OSS. This scenario highlights the benefits to have all information related to resource infrastructure (e.g. all physical and logical resources of a converged infrastructure, their naming, interrelations and topologies formed etc.) managed in a uniform and structured way. Fault Management and its users don't need to manage and administrate all resource information, they only have to know relevant information which is needed in its tasks e.g. for processing the alarms, enriching the alarm information, correlating single alarm in relation to whole topology and visualizing alarms to users.

The following use cases are described:

- Alarm handling capabilities: how Resource Inventory Management supports Fault Management to get initial resource information (it is assumed that all possible domains of converged infrastructure are present and included in the models).
- Enrichment of Alarm information & alarm prioritization: how resource inventory information provided supports enriching single alarm message information for prioritization and visualization & presentations purposes (it is assumed that alarm message content includes which resource instance is the source of alarm and not every alarm causes a query to Resource Inventory Management).

- Alarm correlation and root cause analysis: how resource inventory information is used to analyze a group of simultaneous alarms, correlating between those and searching the root cause. How resource data included in Fault Management is synchronized with the master data in Resource Inventory Management.
- How the potential conflicts between resource instance information included in the alarm message content and information stored in the Fault Management are solved assisted by Resource Inventory

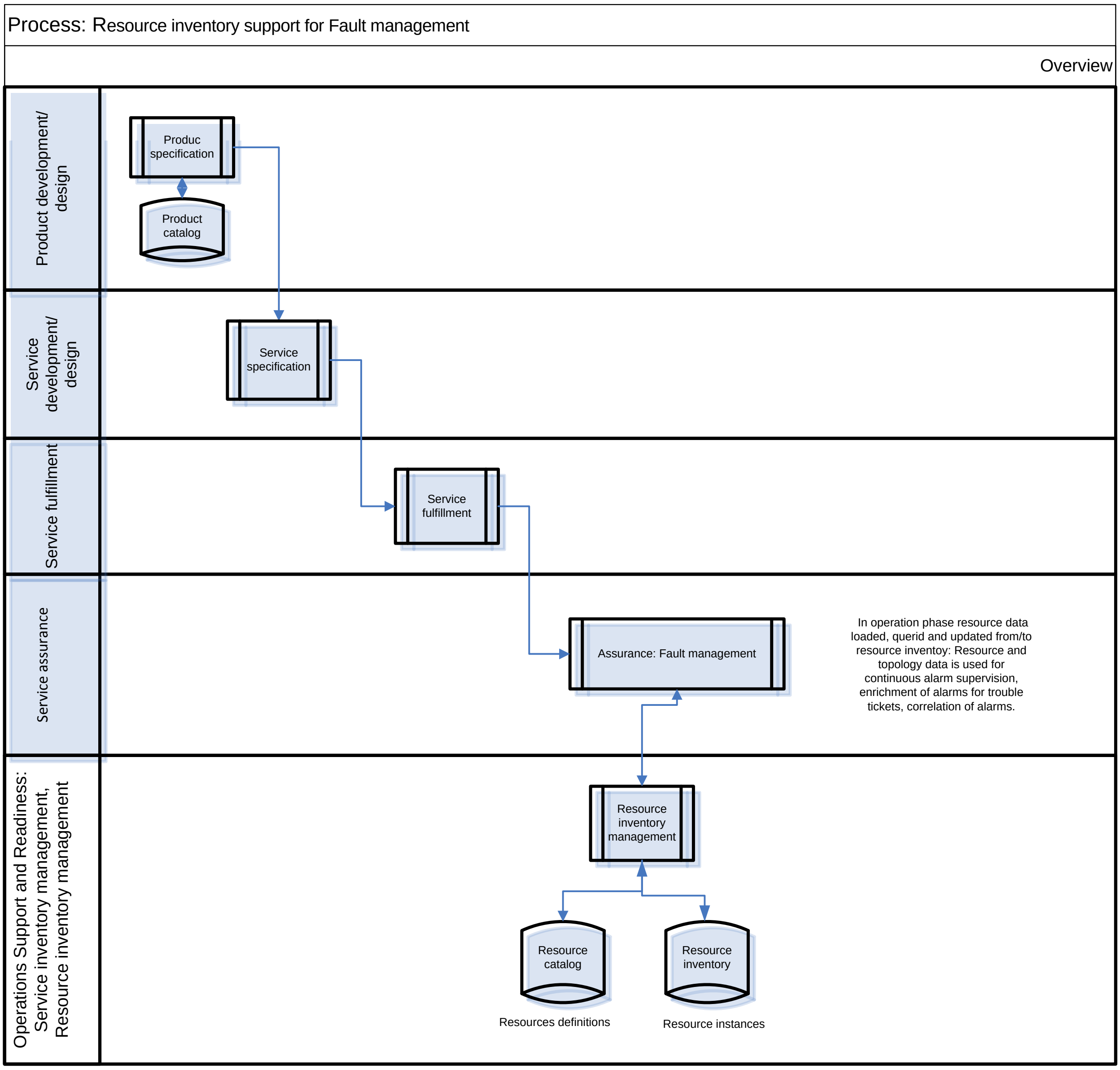


Figure 10-6: Process flow related to Resource Inventory Management support for Fault Management

8.4.4.1.1 Use case: Alarm handling capabilities – Use case UC-RIM-1

UC-RIM-1

Identifier: **Alarm handling capabilities**		**Use Case Id:** **Use case UC-RIM-1**
Originating Process : Continuous alarm supervision and Fault Management		**Actor role:** Typically staff in network operation centres
Precondition(s) and Dependencies: Network and service production is operational Operational OSS system environment including Resource Inventory Management and Fault Management system For efficiency gains and cost reduction it is recommended to have a harmonized interface between the EMS level and the NMS level where discovery & reconciliation functionality is placed		
Scenario description: • This scenario creates functional readiness for Fault Management to use common and centralized resource data • Resource instance information is created or updated in the resource inventory, after which they can be provided to Fault Management application • Fault Management application is provided with an up to date resource information and it is ready for operation		
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (28), REQ-InvM (29), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (37), REQ-InvM (39), REQ-InvM (41), REQ-InvM (42), REQ-InvM (45), REQ-InvM (66)**		
Justification (Business benefits/Impact if not Implemented): Saving operational costs and increasing service quality through fast fault clearance is essential for operation of the NGMN network. All alarms from all NEs in the Access-, Core-, and Transmission network and IT resources need to be received, diagnosed, solved and managed efficiently		
Miscellaneous Comments / Useful hints:		
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date :** **NGMN NGCOR /June 2013**	

8.4.4.1.2 Use case: Enrichment of Alarm info & Alarm – Use case UC-RIM-2

UC-RIM-2

Identifier: **Enrichment of Alarm info & Alarm Prioritisation**		Use Case Id: **Use case UC-RIM-2**
Originating Process : Continuous alarm supervision and Fault Management		**Actor role:** Typically staff in network operation centres
Precondition(s) and Dependencies: Network and service production is operational Operational OSS system environment including Resource Inventory Management and Fault Management (FM) system Information input during the planning phase, during the deployment phase and during the operation phase of the NE lifecycle has to deliver a Resource Inventory Management with high data quality. Network Elements have unique identifiers		
Scenario description: • Alarm record concerning a specific NE is received by FM Application • Resource Inventory Management provides the topology information of the network to FM • Alarm record is enriched and categorized according its priority class • Incident-Ticket is populated with relevant information		
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (28), REQ-InvM (29), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (37), REQ-InvM (39), REQ-InvM (45), REQ-InvM (66)**		
Justification (Business benefits/Impact if not Implemented): Reduction of high of work expenses in the Fault Management process caused by manual work. (Resource and cost perspective as well as data quality issue) When having high number of alarms it is essential to prioritize incoming alarms based on their business impact. Incident-Tickets for IP-hardware-components (e.g. router, server, switches, and storages etc.) have to be enriched during the incident detection & recording phase In many cases alarm priorities from 1 to n are derived from the combination of a network element classification and the criticality of the alarm.		
Miscellaneous Comments / Useful hints: For up to date topology Resource Inventory Management needs to support agreed data model and enable data entry (manual as well as via discovery & reconciliation)		
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**	

8.4.4.1.3 Use case: Alarm correlation and root cause analysis– Use case UC-RIM-3

UC-RIM-3

Identifier: **Alarm correlation and root cause analysis**	Use Case Id: **Use case UC-RIM-3**

Originating Process : Continuous alarm supervision and Fault Management	Actor role: Typically staff in network operation centres
Precondition(s) and Dependencies: Network and service production is operational Operational OSS system environment including resource inventory and Fault Management (FM) systems Further design work is required to detail correlations rules and logic	
Scenario description: • Alarm record or group of alarms are received by FM application • Resource Inventory Management provides the topology information of the network to FM • Alarm information is processed according to correlation criteria • Root cause is identified • Incident tickets are created and populated with information from alarms and Resource Inventory Management	
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (28), REQ-InvM (29), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (37), REQ-InvM (39), REQ-InvM (45), REQ-InvM (66)**	
Justification (Business benefits/Impact if not Implemented): Quick resolution of root cause of for a group of simultaneous alarms	
Miscellaneous Comments / Useful hints: Near real-time data synchronization via these interfaces has to be performed Further design work is required to detail these correlations In most cases topology information provided by Resource Inventory Management systems will be required	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.2 Scenarios and use cases related to Resource Inventory Management Support for Configuration Management

In this scenario focus is on interrelation and interaction between Resource Inventory Management and Configuration ManagementConfiguration Management. This scenario highlights the benefits to have all information related to resource infrastructure, its configuration and its detailed features closely related to each other and centrally managed in a uniform and structured way. In the architecture model the concept of Resource Inventory Management includes not only the resources, but also the configuration structure information of resources i.e. the parts and also configuration parameter information. The architecture model does not imply any directives or proposals of detailed technical implementations; the different data storages and databases may be implemented as distributed or centralized ones.

The following use cases are described:

- Initial configuration of parameter settings after first deployment of resources. This capability has to span over a wide set of converged infrastructure, actual parameters differ from resource to resource.

- Managing configuration and parameter setting changes as a result of SON function, with example on self-configuration.
- Self-Test & Automatic Inventory, with example for eNodeB.

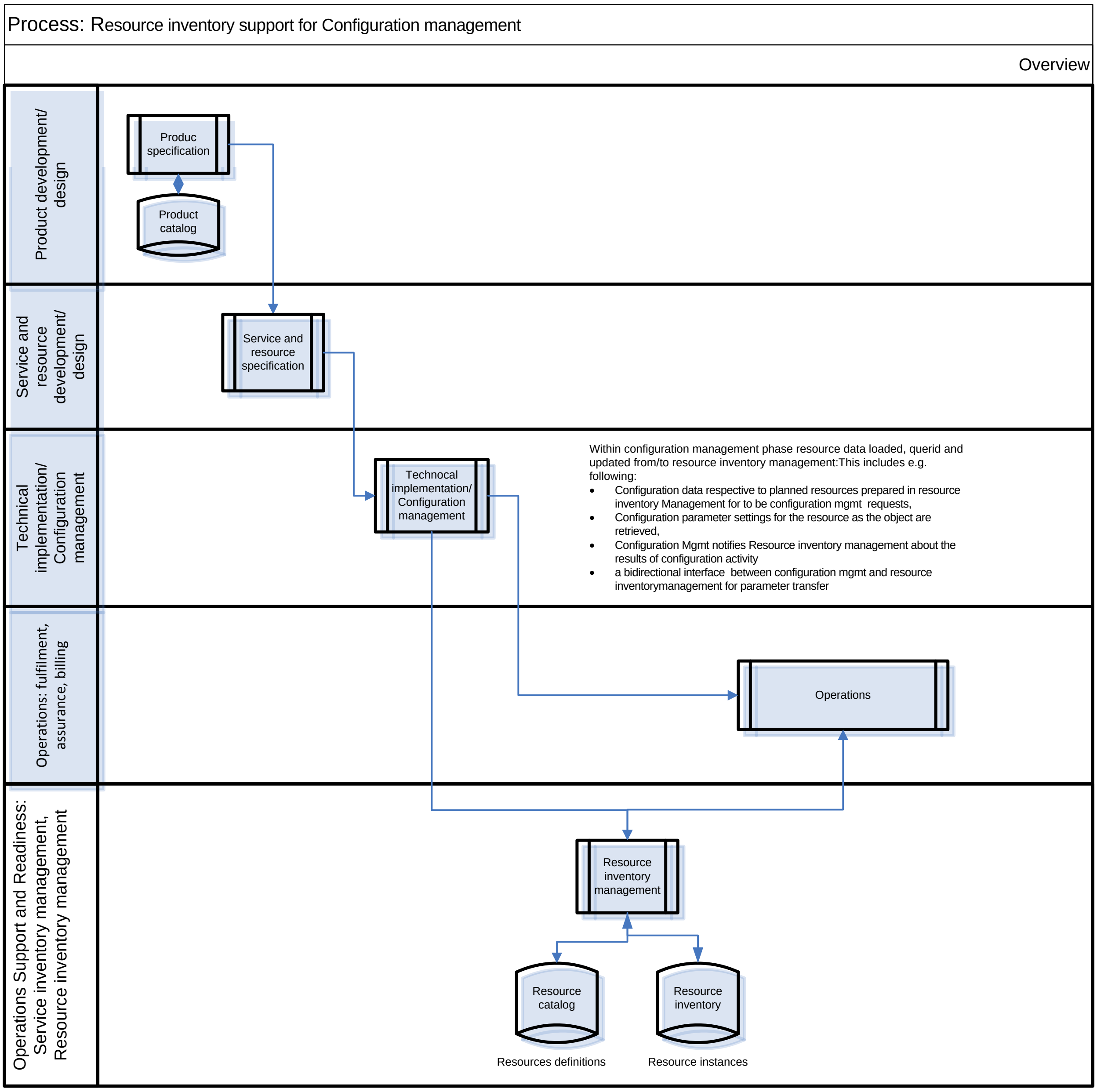


Figure 10-7: Process flow related to Resource Inventory Management support for Configuration Management

8.4.4.2.1 Use case: Initial configuration – Use case UC-RIM-4

UC-RIM-4

Identifier: Initial configuration	Use Case Id: Use case UC-RIM-4
Originating Process : **Resource configuration initiated after planning phase**	**Actor role:** Typically staff in network operation center or dedicated network implementation staff

Precondition(s) and Dependencies:

- Network and service production environment under preparation for Operational phase
- Operational OSS system environment including resource inventory and Configuration Management systems are operational and interconnected
- Resources and their initial parameter settings are planned by planning and respective information instantiated in resource inventory
- Resources are deployed and connected to OSS

Scenario description:

- Human operator determines the object(s) for configuration and initiates configuration phase after planning and deployment
- Configuration parameter settings for the resource as the object are retrieved from Resource Inventory Management
- Configuration Management sends the configuration parameters to the resource
- Configuration Management notifies Resource Inventory Management about the results of configuration
- The resource(s) as object for parameter setting have all been configured
- New parameter settings in the resources are ready for operational use

The resulting requirements / capabilities:
REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (50), REQ-InvM (51), REQ-InvM (55), REQ-InvM (56), REQ-InvM (57), REQ-InvM (66)

Justification (Business benefits/Impact if not Implemented):
Minimizing separate phases for manual entering of resource information by providing automated flow of usage of resource information produced by planning & deployment from Resource Inventory Management to Configuration Management

Miscellaneous Comments / Useful hints:

Required timeline (link to roadmap) / Priority:	Requirement Owner / Date: NGMN NGCOR /June 2013

8.4.4.2.2 Use case: Support for Plug&Play Self Configuration, eNodeB – Use case UC-RIM-5

UC-RIM-5

Identifier: Support for Plug&Play Self Configuration, eNodeB	Use Case Id: Use case UC-RIM-5

Originating Process : Resource configuration initiated after planning phase	**Actor role:** Typically staff in network operation center or dedicated network implementation staff

Precondition(s) and Dependencies:

- Network and service production environment under preparation for operational phase
- OSS system environment including resource inventory and Configuration Management systems are operational and interconnected
- The initial assignment of address, OSS and x-GWs, for a dedicated eNodeB is assumed to be a planning activity. Initial Data will be set up in the planning tools
- The eNodeB is physically installed and all physical connectors are plugged in. A unique eNodeB identifier has been transferred into the eNodeB by appropriate medium latest during the on site installation phase. It has a temporary IP address assigned and has established secure end-to-end connections to the security servers and the element manager
- There shall be no need to pre-configure the eNodeB by the vendor or the operator. The configuration data maybe aggregated as a specific configuration file

Scenario description:

- Configuration data respective to planned resources, eNodeBs, is prepared in Resource Inventory Management ready for Configuration Management requests
- ENodeB initiates the self-configuration, configuaration requests sent to Configuration Management
- Configuration Management requestes planned parameter transfer from Resource Inventory Management
- Configuration data is transferred to eNodeBs (in accordance with the northbound interface specification)
- eNodeB has established its operational parameter settings

The resulting requirements / capabilities:
REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (50), REQ-InvM (51), REQ-InvM (55), REQ-InvM (56), REQ-InvM (57), REQ-InvM (66)

Justification (Business benefits/Impact if not Implemented):
New eNodeBs have plug and play self-configuration capabilities. This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB. This saves overall commissioning costs.
Based on information delivered by the DHCP server/Configuration Server the eNodeB starts to establish a bidirectional, stable and secure end-to-end connection during its plug&play deployment phase.

Miscellaneous Comments / Useful hints:
The eNodeB requests the configuration data from Configuration Management. The configuration data matching with the same characteristics as the requesting eNodeB (unique eNodeB identifier is used to bind a configuration data with the actual eNodeB HW), is retrieved as the planned parameter set dedicated to the requesting eNodeB. This parameter set, consisting of dedicated radio- and IP-parameters plus a set of default parameters may have been aggregated into a configuration file based on policy or other selection criteria. This file is delivered back to the requesting eNodeB. The eNodeB reconfigures itself and comes up with its final IP addresses and a radio configuration.

Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.2.3 Use case: Self Test & Automatic Inventory, eNodeB – Use case UC-RIM-6

UC-RIM-6

Identifier: Self Test & Automatic Inventory, eNodeB	Use Case Id: Use case UC-RIM-6
Originating Process : Resource configuration initiated after planning phase	**Actor role:** Typically staff in network operation center or dedicated network implementation staff
Precondition(s) and Dependencies: • Network and service production environment under preparation for operational phase • OSS system environment including resource inventory and Configuration Management systems are operational and interconnected • The eNodeB is physically installed and all physical connectors are plugged in. It has an IP Address assigned and has retrieved its configuration data / parameter set from Resource Inventory	
Scenario description: • ENodeB has set up its confirmation and is ready for testing before put into operation • Resource Inventory Management enables to discover/upload eNodeB data and to reconciliate (between planned data and uploaded data) • Resource Inventory accesses eNodeB's parameter sets on request (via Itf-N in accordance with the northbound interface specification) • Resource and its configuration data has been updated in the Resource Inventory Management	
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (50), REQ-InvM (51), REQ-InvM (55), REQ-InvM (56), REQ-InvM (57), REQ-InvM (66)**	
Justification (Business benefits/Impact if not Implemented): Self-testing of nodes supported by automatic status reporting saves specialized personnel from visiting the installation site and performing a manual report of the eNodeB characteristics. Following the final self-test the eNodeB delivers • a state change notification • details on its configuration which is used to update information in Resource Inventory Management for the respective resource	
Miscellaneous Comments / Useful hints: Reconciliation (between planned data and uploaded data) to be done in real-time and respectively at dedicated intervals (<= 24h).	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.3 Scenarios and use cases related to Resource Inventory Management support for planning and deployment

In this scenario focus is on interrelation and interaction between Resource Inventory Management and planning & deployment. Planning and deployment is a vast area where very often both operator's own staff and as well as external contractors are co-operating and using variety of OSS systems. The scenario highlights the benefits to have all information related to resource infrastructure managed in a uniform and structured way. Planning & deployment systems and users of them don't need to maintain and administrate common resource information which is centrally stored can accessed via interaction with Resource Inventory Management. The main purpose for Resource Inventory Management support for planning and deployment is for technical issues, not for financial aspects of those.

Following use cases are described

- Planning of new resources or extending capacity and utilizing Resource Inventory Management providing the existing resource information; resource topology, geography, location, capacity etc.
- Planning providing initial technical parameter configurations settings e.g. radio parameters or transmission equipment parameters to be used in technical configuration
- Resource deployment support; Resource Inventory Management providing resource information for various phases of deployment (network construction, implementation and changes), e.g. for roll-out work implementation planning, managing spare part stores and information on them, infra site acquisition and management, network technical implementation etc. as well as deployment providing updated or status information on executed work on resources indicating readiness for operation
- IP address management and planning/ implementation support

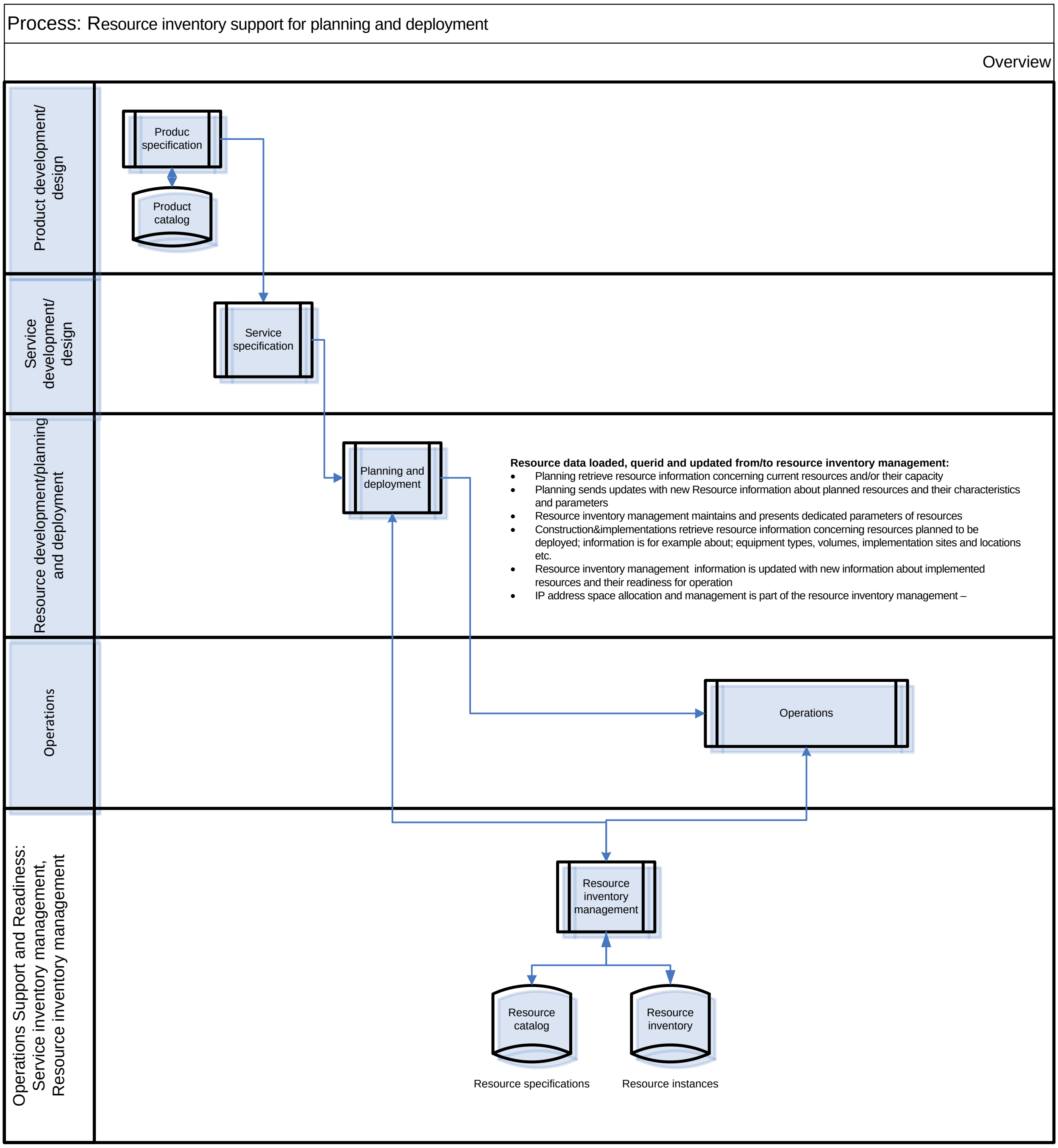


Figure 10-8: Process flow related to Resource Inventory Management support for resource lifecycle management

8.4.4.3.1 Use case: Planning of resources – Use case UC-RIM-7

UC-RIM-7

Identifier: Planning of resources	Use Case Id: Use case UC-RIM-7

Originating Process : **Network planning**	**Actor role:** Planning staff
Precondition(s) and Dependencies: • Network production environment under planning (new or changes) for operational phase • OSS system environment including Resource Inventory Management and planning & deployment systems are implemented, operational and interconnected	
Scenario description: • Planning of new resource is initiated • Planning systems retrieve resource information from Resource Inventory Management concerning current resources and/or their capacity • Planning systems update resource inventory with new information about planned resources and their characteristics and parameters • Planning of new resources is considered completed • New resource information successfully updated to Resource Inventory Management and available for further phase in deployment and operation	
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (30), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (40), REQ-InvM (52), REQ-InvM (59), REQ-InvM (60), REQ-InvM (61), REQ-InvM (62), REQ-InvM (63), REQ-InvM (64) , REQ-InvM (65)**	
Justification (Business benefits/Impact if not Implemented): Saving when utilizing and updating of common Resource Inventory Management information when planning new resources or extending capacity	
Miscellaneous Comments / Useful hints:	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.3.2 Use case: Planning of basic (eNodeB) parameters for Plug&Play – Use case UC-RIM-8

UC-RIM-8

Identifier: **Planning of basic (eNodeB) parameters for Plug&Play**	**Use Case Id:** **Use case UC-RIM-8**
Originating Process : Network planning	**Actor role:** Planning staff
Precondition(s) and Dependencies: • Network production environment under planning (new or changes) for operational phase	

• OSS system environment including Resource Inventory Management and planning & deployment systems are implemented, operational and interconnected • It is assumed that IP address and address range planning is internationally coordinated
Scenario description: • Planning of new resource is initiated including the detailed parameters • The Planning tool allows a consistent planning of all resource parameter values, maintain them in its database • Planning tool provides parameter transfer to Resource Inventory Management • Resource Inventory Management allows maintaining and presenting the dedicated set of parameters of the resource (including e.g. ANR specific values for each planned eNodeB) • Resource inventory managment is updated with new resource parameter information
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (30), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (40), REQ-InvM (52), REQ-InvM (59), REQ-InvM (60), REQ-InvM (61), REQ-InvM (62), REQ-InvM (63), REQ-InvM (64) , REQ-InvM (65)**
Justification (Business benefits/Impact if not Implemented): Basic node parameters have to be provided as a pre-deployment activity. This allows to minimize detailed manual planning of neighbour relations, frequencies etc. This saves specialized personnel from visiting the installation site and performing a manual set up of the eNodeB.
Miscellaneous Comments / Useful hints: During the installation and commissioning phase each eNodeB has to be provided with a set of configuration data, this configuration data consist of the elements: • Site specific eNodeB parameters • dummy cell parameters • standard cell specific parameters having a generic, net wide nature and underlying a change from time to time • SP specific transport parameters having a generic, net wide nature

Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.3.3 Use case: Resource deployment (construction and implementation) support UC-RIM-9

UC-RIM-9

Identifier: **Resource deployment (construction and implementation)support**	**Use Case Id:** **Use case UC-RIM-9**
Originating Process : Network planning	**Actor role:** Implementation and constructions staff, may include operator's own staff and sub-contractors

Precondition(s) and Dependencies: • Network production environment under implementation and deployment (new or changes) for operational phase • OSS system environment including Resource Inventory Management and planning & deployment systems are implemented, operational and interconnected	
Scenario description: • Deployment of the planned resources is initiated • Construction and implementations support systems need to retrieve resource information from Resource Inventory Management concerning resources planned to be deployed; information is for example about equipment types, volumes, implementation sites and locations etc. • Resource Inventory information is updated with new information about implemented resources and their readiness for operation • Resources are deployed ready for operational use	
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (30), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (40), REQ-InvM (52), REQ-InvM (59), REQ-InvM (60), REQ-InvM (61), REQ-InvM (62), REQ-InvM (63), REQ-InvM (64) , REQ-InvM (65)**	
Justification (Business benefits/Impact if not Implemented): Efficient resource construction and implementation by utilization and having up to date Resource Inventory Management information when building or changing resources or capacity	
Miscellaneous Comments / Useful hints: Specific concerns about security and access control mechanisms for external sub-contractors	
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**

8.4.4.3.4 Use case: IP address management and planning / implementation support – Use case UC-RIM-10

Most SP and enterprise organizations will obtain public IP address space from their national or regional Internet Registry and RIPE. After a block of public IP address space has been obtained, it can then be allocated to address pools and from there be assigned to locations, subnets, devices and ports across the network. Similarly, private IP address space will be allocated in that way.

During planning of IP addresses allocation - whether private or public ones - planners and administrators must forecast the IP address capacity requirements in each subnet on the network. This is typically based on the number of devices and ports located at each site, or the number of dynamically active users or mobile users expected at the site (DHCP), and the number of IP addresses required on average for each end user of a service. Another aspect is, for example, routers in the backbone that need to be configured to provide priority processing on VoIP packets versus best-effort data packets.

Address planning and assignment is best performed using a centralized Resource Inventory Management containing the IP addresses as logical resources. A centralized Resource Inventory Management provides a holistic view of the entire address space deployed over a number of sites and with address pools deployed on multiple DHCP and DNS servers throughout the network.

UC-RIM-10

Identifier: **IP address management and planning/ implementation support**		**Use Case Id:** **Use case UC-RIM-10**
Originating Process : **Network planning**		**Actor role:** Planning and deployment staff, may include operator's own staff and sub-contractors
Precondition(s) and Dependencies: • Network production environment under implementation and deployment (new or changes) for operational phase • OSS system environment including Resource Inventory Management with IP address pools as logical resources and planning & deployment systems are implemented, operational and interconnected		
Scenario description: • Obtaining IP address space from Registry • Deposit IP addresses in the Resource Inventory Management IP address pool • IP addresses are assigned to resources • IP addresses are reconciled between the network and the Resource Inventory Management • The set of IP addresses assigned to resources + the set of IP addresses assigned to DHCP servers + the set of IP addresses remaining in the IP address pool is id to the IP address space obtained from Registry		
The resulting requirements / capabilities: **REQ-InvM (23), REQ-InvM (24), REQ-InvM (25), REQ-InvM (26), REQ-InvM (27), REQ-InvM (30), REQ-InvM (31), REQ-InvM (32), REQ-InvM (33), REQ-InvM (34), REQ-InvM (36), REQ-InvM (38), REQ-InvM (39), REQ-InvM (40), REQ-InvM (41), REQ-InvM (42), REQ-InvM (52), REQ-InvM (59), REQ-InvM (60), REQ-InvM (61), REQ-InvM (62), REQ-InvM (63), REQ-InvM (64) , REQ-InvM (65)**		
Justification (Business benefits/Impact if not Implemented): Efficient, consistent and centralized handling of the IP address space by having up to date Resource Inventory information when building or changing resources and assigning / reassigning IP addresses.		
Miscellaneous Comments / Useful hints:		
Required timeline (link to roadmap) / Priority:	**Requirement Owner / Date:** **NGMN NGCOR /June 2013**	

8.5 REQUIREMENTS

8.5.1 Service Inventory Management requirements

Based on Service Inventory Management use cases are following set of requirements derived and described. The requirements are categorized as a) functional, b) modelling and c) interfacing requirements. To be noted regarding the related use cases of requirements that NGCOR has not analysed specific use cases for all possible areas covering processes from development to operations. Instead, the generic use case – UC-Gen-SIM-RIM-1 represent overview process flow, usgage and role of service and resource inventory management. As a consequence in cases where the specific detail use case is not analysed UC-Gen-SIM-RIM-1 is referred as the related use case.

8.5.1.1 Service Inventory Management functional requirements

REQ-InvM (1)

Identifier: REQ-InvM (1)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7	Priority:
Title : **Capability to manage service models of different domains and areas for converged fixed-mobile services.**		
Description: In order to be able to act in a centric role in managing and storing service data in a converged fixed-mobile environment it shall be possible to model and manage all different kinds of services.		
Rationale: Consistent and harrmonized service information models throughout fixed-mobile services result in cost-efficient information management and integration.		

REQ-InvM (2)

Identifier: REQ-InvM (2)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7	Priority:
Title : **Capability to offer and maintain service data to/with the different applications supporting planning & implementation, fulfilment, assurance and billing (generally SI&P, OSR, FAB).**		
Description: Service Inventory shall store and manage common data for other OSS applications.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile services result in cost-efficient information management and integration.		

.

REQ-InvM (3)

Identifier: REQ-InvM (3)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-	Priority:

	1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7	
Title : **Capability to organize and offer ownership of service information/data among organization functions and processes.**		
Description: Mechanisms to restrict the capabilities of a Service Inventory system that are offered to other systems. Mechanisms to create, read, update and delete Service Inventory data.		
Rationale: Well-organized information management provides cost-efficiency in development and maintenance.		

REQ-InvM (4)

Identifier: REQ-InvM (4)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7**	**Priority:**
Title : **Capability to ensure high quality of Inventory data identification, control, status accounting & reporting, verification and audit.**		
Description: Mechanisms to ensure that inventory data is consistent and of high quality throughout all data lifecycles including e.g. the following: Resource & Service specifications will be agreed based on the respective SP business needs and the infrastructure technical needs; Inventory data storage and usage is controlled and authorized; Inventory data can be reported and traced; Inventory data can be verified and audited.		
Rationale: Well-organized lifecycle management of information management provides cost-efficiency in development and maintenance.		

8.5.1.2 Service Inventory Management information modeling requirements

REQ-InvM (5)

Identifier: REQ-InvM (5)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7**	**Priority:**
Title : **A common harmonized and consistent service information model covering different services of converged fixed – mobile environment.**		

Description: It is crucial that the data managed centrally in the Service Inventory is comprehensive covering all different services of a converged fixed-mobile environment and modelled in consistent way. Service modelling characteristics and extensive details has been presented in the "Modelling and Tooling" stream of NGCOR.
Rationale: Consistent and harmonized service information models throughout fixed-mobile services result in cost-efficient information management and integration.

REQ-InvM (6)

Identifier: REQ-InvM (6)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7	Priority:
Title : **A common, harmonized and consistent service information model agreed between interworking OSS/BSS applications/areas for service management.**		
Description: Service Inventory manages and stores centrally common information for various other OSS applications. The other OSS applications producing or consuming Service Inventory data shall have a common information model with Service Inventory. Service modelling characteristics and extensive details has been presented in the Modelling and Tooling stream of NGCOR.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile services result in cost-efficient information management and integration.		

REQ-InvM (7)

Identifier: REQ-InvM (7)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7	Priority:
Title : **Vertical service information model, which contains the relationship of services to resource/product/customer – layers.**		
Description: Service Inventory manages and stores the relationship of services downwards to the resources they are built upon, and upwards to the products and customer which make use of these services. This is a prerequisite e.g. for the impact analysis capability of the service management functions.		

Rationale: Modular design and structures when composing services based on underlying resources, and products based on underlying service components facilitates fast development and time to market. Modular structure is utilized by many interfacing OSS applications. A structured and comprehensive impact analysis through different management layers is enabled as well as automated fulfilment.

REQ-InvM (8)

Identifier: REQ-InvM (8)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7**	**Priority:**
Title : **Meta-model CFS-RFS-R decomposition.**		
Description: The meta-model of the Service Inventory (Service Catalogue) should enable to describe the relations between CFS-RFS and Resource specifications which enable to perform the service order decomposition. For example it should enable to decompose a customer order (CFS order) into technical orders (RFS order) and finally Resource orders based on service catalogue data (see also REQ-InvM (13)).		
Rationale: Modular design and structures when composing services based on underlying resources, and products based on underlying service components facilitates fast development and time to market. Modular structure is utilized by many interfacing OSS applications. A structured and comprehensive impact analysis through different management layers is enabled as well as automated fulfilment.		

REQ-InvM (9)

Identifier: REQ-InvM (9)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5, UC-SIM-6, UC-SIM-7**	**Priority:**
Title : **Meta-model CFS-RFS-R characteristic mapping.**		
Description: The meta-model of the Service Inventory (Service Catalogue) should enable to describe the relations between characteristics of CFS-RFS and Resource specifications (a characteristic mapping). The goal of the characteristic mapping is to enable to translate the customer order parameters (based on CFS characteristic values) into technical order parameters (based on RFS Resource characteristic values) (see also REQ-InvM (13)).		
Rationale: Modular design and structures when composing services based on underlying resources, and products based on underlying service components facilitates fast development and time to market. Specification /defintions regarding attributes and parameters needs to be consistent through vertial layers. Modular structure is utilized by many interfacing OSS applications. A structured and comprehensive impact analysis through different management layers is enabled as		

well as automated fulfilment. Cost efficient and automated fulfillment process including mapping of all characteristics between management layers is achieved.

REQ-InvM (10)

Identifier: REQ-InvM (10)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-3, UC-SIM-4	Priority:
Title : **RFS RAN service definition.**		
Description: This requirement is to support the Use Case: Requesting a Capacity reservation from the shared RAN to be able to support mobile customers in chapter 4.3.2.1. The specification of RAN service (a Resource Facing Service) is to be defined in RAN vendor independent way. The service must capture the characteristics of service provided by the RAN service in a way that it enables to define the requirements towards a particular RAN from the perspective of being able to support mobile customers (Customer Facing Service) but without imposing any particular configuration of the RAN service. Instead after defining the RFS RAN service instance to be provided by the instance of RAN (in the sense of resource), a master operator (an operator which manages the configuration of the RAN) should be able to design the configuration that suites the requirements materialised in RFS RAN instance (see also REQ-InvM (55)). The relation between RFS RAN and RAN (resource) should be defined according the REQ-InvM (7). The definition of RFS RAN specification should enable to describe the many-to-one relation with the Resource RAN (one Resource RAN should be able to support many RFS RAN).		
Rationale: • To define the requirements towards the shared RAN to be able to provide the adequate service level to support mobile customers. • To manage the RAN as "a black box" service rather than manage directly configuration of the RAN. • To delegate the Configuration Management expertise (low level technical expertise) to the operator of the shared network. • To avoid "overwriting" the configuration of the RAN by operators sharing the same RAN.		

REQ-InvM (11)

Identifier: REQ-InvM (11)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-3, UC-SIM-4	Priority:
Title : **RFS RAN service definition – access technology agnostic.**		
Description: The RFS RAN service definition (the RFS RAN specification) should be envisioned in the way that it identifies the characteristic which can be used to define the access service properties no matter of the underlying technology. The rationale for that is to enable to treat the RAN network as a black box comparable for fixed based access network from the service point of view. The similar (if not the same) requirements (captured in RFS RAN specification) should be applicable to fixed based access network. The recommended approach to this requirement is to elaborate RFS Access specification from which the RFS RAN specification and RFS Fixed-Access specification can inherit. The RFS RAN		

specification may extend RFS Access specification for only radio specific characteristics which can't be shared with RFS Fixed-Access specification (if really needed). The intension is to avoid having technology specific characteristics at service level unless it is absolutely necessary.
Rationale: Reduce development time and improved time to market by applying modular design principles.

REQ-InvM (12)

Identifier: REQ-InvM (12)	**Rel. Use case id :** UC-SIM-1, UC-SIM-2, UC-SIM-3, UC-SIM-4	**Priority:**
Title : **RFS RAN service definition vs. "capacity".**		
Description: The REQ-InvM (10) defines that "RFS RAN … enables to define the requirements towards a particular RAN from the perspective of being able to support mobile customers (Customer Facing Service).". This definition is the most "generic" one. When elaborating the RFS Specification it may be helpful to understand it as a way of defining the requirements in the form of "service capacity". The word "service" is used here to enable to distinguish between "resource capacity" which sometimes is understood as low level capacity (for example availability of time slots). The "service capacity" can be understood as capacity to provide customer service like voice, data (with appropriate QoS depending of the data service profile). It is however not unlikely that the "service capacity" is (and should be) in the relation of "resource capacity" following general rule of RFS-Resource mapping (service – resource relation). As described in the use cases in chapters 4.3.2.1 and 4.3.3.1 the RFS RAN service specification should enable to translate the customer service oriented requirements finally to the technical requirements towards the network.		
Rationale: Reduce development time and improved time to market by applying modular design principles.		

8.5.1.3 Service Inventory Management interfacing requirements

In the following requirements the purpose of interfacing/integration of Service Inventory with different other OSS applications is explained. TMF TAM is used as a generic model to present various applications/application areas of OSS environment.

REQ-InvM (13)

Identifier: REQ-InvM (13)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-5**	**Priority:**
Title : **Service Inventory Management interfacing with fulfilment.**		

Description: Fulfilment creates the service instances based on BSS requests. It creates updates and stores specific engineering properties, e.g. a production plan that covers the activation sequence and timing considerations, which have to be ensured during instantiation of services. It implements information brokering towards BSS on service related matters. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.
Rationale: A cost efficient and automated fulfillment process is achieved. Use the service design done in the Service Catalogue as a driving model for the process. Reduce time-to-market by basing the fulfilment process on the service catalogue data.

REQ-InvM (14)

Identifier: REQ-InvM (14)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-7**	**Priority:**
Title : **Service Inventory Management interfacing with service problem management / trouble ticketing.**		
Description: Service Problem Management (including service monitoring functions) / trouble ticketing retrieves service instance information, and navigates the Service Inventory for impact analysis. The information provided from service inventory and assisted bý resource inventory enables analysing the full CFS-RFS-Resource hierachcy structure and to localize the physical resources affected by event and impacted CSFs and RFSs. By provides information on SLA metrics and SLA level associated with service type or service instance is severity assessment of the issue enabled. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.		
Rationale: Service Inventory Management provides a well-structured and consistent service model for service problem management processes and applications. Service Inventory Management provides to Service Problem Manager all service information, including the other consumed Services, Resources, as well as associations to Product and to Customer. Such relationship can help to identify impacted services and customers in case of resource failure, or planned maintenance activities, to correlate with or supress customer trouble tickets. On the other direction, such relationship can support root cause analysis to indentify troubled resource for given problematic service(s).		

REQ-InvM (15)

Identifier: REQ-InvM (15)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-6**	**Priority:**
Title : **Service Inventory Management interfacing with service quality management.**		
Description: Service Quality Management reads the service specification and service tree, and uses the information to set the KQI/KPI		

calculation rules and principles and desired monitoring thresholds. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.
Rationale: Service Inventory Management provides a well-structured and consistent service model for service quality management processes and applications. Service Inventory Management provides to Service Quality Manager all service information to allow to correct monitoring of Quality of Service (QoS) according specific rules defined. Data model contributes to required data aggregation (on SQM) for quality analysis and to manage and end-to-end service mapping.

REQ-InvM (16)

Identifier: REQ-InvM (16)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2, UC-SIM-6, UC-SIM-7**	**Priority:**
Title : **Service Inventory Management interfacing with SLA management.**		
Description: SLA management reads the service specification and service tree, and uses the information to set the desired SLA thresholds. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.		
Rationale: Service Inventory Management provides a well-structured and consistent service model for SLA management. Service inventory data is complemented with customer data for caluculation and aggregating metrics and crietiria needed in indivual customer SLA fufillment.		

REQ-InvM (17)

Identifier: REQ-InvM (17)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,**	**Priority:**
Title : **Service Inventory Management interfacing with test & diagnostics.**		
Description: Test & diagnostics retrieves service instance information, reads the test plans, and stores test results. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.		
Rationale: Service Inventory Management provides a well-structured and consistent service model for testing and diagnosis purposes.		

REQ-InvM (18)

Identifier: REQ-InvM (18)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,	Priority:
Title : **Service Inventory Management interfacing with billing mediation.**		
Description: Billing mediation accesses to information in the Service Inventory for proper grouping of the CDR as they are forwarded to BSS, using standardized formats and protocols. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.		
Rationale: Service Inventory Management provides a well-structured and consistent service model used for assigning the service context for the charging mediation events.		

REQ-InvM (19)

Identifier: REQ-InvM (19))	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,	Priority:
Title : **Service Inventory Management interfacing with service discovery.**		
Description: Service discovery checks services (service instances), which have been discovered, against the Service Inventory to validate data quality, and to trigger the reconciliation process in case of discrepancy. This interface is represented by Interface group A in the Figure 14: OSS reference architecture emphasizing Inventory Management and is an object for standardization.		
Rationale: Continuous service discovery capability thorughout of the network and service infrastructure secures up-to-date service inventory information.		

REQ-InvM (20)

Identifier: REQ-InvM (20)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,	Priority:
Title : **Service Inventory Management interfacing with Resource Inventory Management.**		
Description:		

Resource Inventory Management implements together with the Service Inventory Management the complete linkage between resources and services needed for the fulfilment, assurance, and mediation functions (OSS). This interface is represented by Interface group C in the Figure 14: OSS reference architecture emphasizing Inventory Management Service and Resource information models are objects for standardization, but if a communication interface between Service Inventory Management and Resource Inventory Management will be needed it is dependent on how Resource Inventory/Service Inventory combined concept is implemented.
Rationale: Modular design and structures when composing services based on underlying resources is facilitated by smooth interworking between Resource Inventory Management and Service Inventory Management

REQ-InvM (21)

Identifier: REQ-InvM (21)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,**	**Priority:**
Title : **Service Inventory Management interfacing with product / customer inventory.**		
Description: Service Inventory implements, together with the product / customer inventory, the complete linkage between services and products and customers, needed for the fulfilment and assurance functions (OSS). This interface is represented by Interface group C in the Figure 14: OSS reference architecture emphasizing Inventory Management Service and Product/Customer information models are objects for standardization, but if a communication interface between Service Inventory Management and Product Inventory Management will be needed it is dependent on how Service Inventory/Product inventory combined concept is implemented.		
Rationale: Modular product structures when composing products based on underlying service components is facilitated by smooth interworking between service Inventory Management and product Inventory Management		

REQ-InvM (22)

Identifier: REQ-InvM (22)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-1, UC-SIM-2,**	**Priority:**
Title : **Service Inventory Management interfacing with catalogue management.**		
Description: Service catalogue is a subset of general cross-domain catalogue management. Service catalogue deploys and stores service specifications as basis for Service Inventory information model definitions supporting full lifecycle of services including e.g. test plans. This interface is internal within Inventory Management area. Information models used are objects for standardization.		

Rationale: Service catalogue is a relevant piece of strucured and well-managed service information management and modelling.

8.5.2 Resource Inventory Management requirements

8.5.2.1.1

Based on Resource Inventory Management use cases the following set of requirements are derived and described. The requirements are categorized as a) functional, b) modelling and c) interfacing requirements. To be noted regarding the related use cases of requirements that NGCOR has not analysed specific use cases for all possible areas covering processes from development to operations. Instead, the generic use case – UC-Gen-SIM-RIM-1 represent overview process flow, usgage and role of service and resource inventory management. As a consequence in cases where the specific detail use case is not analysed, UC-Gen-SIM-RIM-1is referred as the related use case.

8.5.2.1.2 Resource Inventory Management functional requirements

REQ-InvM (23)

Identifier: REQ-InvM (23)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Capability to manage resource models of variety of technology infrastructure domains and areas of converged fixed-mobile environment.**		
Description: In order to be able to act in a centric role in managing and storing resource data in a converged fixed-mobile environment it shall be possible to manage all different resources models from e2e management perspective.		
Rationale: Consistent and harrmonized resource information models throughout fixed-mobile infrastructure result in cost-efficient information management and integration**.**		

REQ-InvM (24)

Identifier: REQ-InvM (24)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Capability to offer and maintain resource data to/with the different applications supporting planning & implementation, fulfilment, assurance and billing (generally SI&P, OSR, FAB), and with resource infrastructure.**		

Description: Resource Inventory Management shall store and manage common data for other OSS applications and synchronize and reconcile with actual resource data.
Rationale: Consistent and harmonized resource information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration**.**

REQ-InvM (25)

Identifier: REQ-InvM (25)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Capability to organize and offer ownership of resource information/data among applications, functions and processes.**		
Description: Mechanisms to restrict the capabilities of a Resource Inventory system that are offered to other systems. Mechanisms to create, read, update and delete Resource Inventory data.		
Rationale: Well-organized information management provides cost-efficiency in development and maintenance.		

REQ-InvM (26)

Identifier: REQ-InvM (26)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Capability to model and document the horizontal relationship (on physical and logical level) between resources, spanning all types of resource – technologies.**		
Description: Mechanisms to organize the horizontal relationship between resources. It must be possible to analyse the interworking of resources which delivers the E2E network service. The logical layer is needed to understand the ability of the network which delivers the E2E network service as a prerequisite for the Impact Analysis function in service management capabilities. The physical layer (including the documentation of redundancy) is a prerequisite for the impact analysis (e.g. to understand the impact of an outage on the E2E network service), and for root cause analysis in NMS as well.		
Rationale:		

A structured impact analysis covering different technology domains is enabled.

REQ-InvM (27)

Identifier: REQ-InvM (27)	**Rel. Use case id : UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Updates of resource information after changes**		
Description: Resource Inventory Management shall provide actual resource information within agreed time period after changes happened in the configuration (for example not later than N hours after a change of a configuration has occured to the Fault Management).		
Rationale: Information management within overall OSS environment is preferred to approach real-time to improve customer satisfaction.		

REQ-InvM (28)

Identifier: REQ-InvM (28)	**Rel. Use case id : UC-RIM-1, UC-RIM-2, UC-RIM-3**	**Priority:**
Title : **Configurable attibutes for support of enrichment related applications.**		
Description: It should be configurable which attributes will be available for enrichment and which ones are synchronized between Resource Inventory Management and the related applications.		
Rationale: Configurability facilitates flexibility and reduced implementation times and reduced time to market.		

REQ-InvM (29)

Identifier: REQ-InvM (29)	**Rel. Use case id : : UC-RIM-1, UC-RIM-2, UC-RIM-3**	**Priority:**
Title : **Configurable attibutes for support of synchronization related applications.**		
Description: It should be configurable which attributes will be available in the Resource Inventory Management and which ones are synchronized between Resource Inventory Management and related applications (e.g. Fault Management.).		

Rationale: Configurability facilitates flexibility and reduced implementation times and reduced time to market.

REQ-InvM (30)

Identifier: REQ-InvM (30)	Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10	Priority:
Title : **Security for external sub-contractor interfacing.**		
Description: Specific security and access control mechanisms have to be established for external sub-contractors.		
Rationale: Securing confidentiality and avoiding misuse of information is of key importance.		

8.5.2.2 Resource Inventory Management information modelling requirements

REQ-InvM (31)

Identifier: REQ-InvM (31)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10	Priority:
Title : **Capability to model and document the life cycle & usage state of network resources in line with ITU-T Recommendation X.731 – Amendment 2.**		
Description: Inventoried resources shall have a life cycle attribute so that their deployment can be planned, tracked, and managed. Logical resources, e.g. connections, are also inventoried such that their deployment can be planned, tracked, and managed using a lifecycle state attribute.		
Rationale: It is important to align with standard information models to make cost-efficiently system development and integration possible.		

REQ-InvM (32)

Identifier: REQ-InvM (32)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-	Priority:

	RIM-10	
Title : **A common harmonized and consistent resource information model covering different infrastructure domains of converged fixed-mobile environment.**		
Description: It is crucial that the data managed centrally in the resource inventory is comprehensive covering all different resources of a converged fixed-mobile environment and modelled in consistent way. Resource modelling characteristics and extensive details has been presented in the "Modelling and Tooling" stream of NGCOR.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (33)

Identifier: REQ-InvM (33)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Resource information of elements and topology**		
Description: Resource Inventory Management shall model the resource information of the elements and the topology.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover network wide views.		

REQ-InvM (34)

Identifier: REQ-InvM (34)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **A common, harmonized and consistent resource information model agreed between interworking OSS applications/areas for resource management.**		
Description: Resource Inventory Management manages and stores centrally common information for various other OSS applications. The other OSS applications producing or consuming resource inventory data shall have a common information model with Resource Inventory. Resource modelling characteristics and extensive details has been		

presented in the "Modelling and Tooling" stream of NGCOR. The identification of object instances in the Resource Inventory shall be consistent with the network resource models used for all involved applications throughout OSS.
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.

REQ-InvM (35)

Identifier: REQ-InvM (35)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title : **Configuration data preparing for CM requests**		
Description: Configuration data respective to planned resources, eNodeBs, has to be prepared in Resource Inventory Management to be addressed by Configuration Management requests. Configuration data may be aggregated as configuration files.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details of characteristics of resources.		

REQ-InvM (36)

Identifier: REQ-InvM (36)	**Rel. Use case id : UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-7**	**Priority:**
Title : **IP-Hardware components data in Resource Inventory Management**		
Description: Enrichment of Incident-Tickets for IP-Hardware-Components (e.g. Router, Server, Switches and Storages etc.) needs well documented and actual information in the Resource Inventory Management.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details of characteristics of resources.		

REQ-InvM (37)

Identifier: REQ-InvM (37)	**Rel. Use case id : UC-RIM-1, UC-RIM-2, UC-RIM-3**	**Priority:**

Title : **Complementary information attributes from Resource Inventory Management for incident-ticekets**
Description: Incident-Tickets, created from an initiating alarm, are to be populated with information (attributes: 1, 2, 3) from this initiating alarm and also with information (attributes: a, b, c) from the Resource Inventory (Examples for a, b, c: location, responsible person, accessibility).
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details of characteristicsof resources.

REQ-InvM (38)

Identifier: REQ-InvM (38)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **Maintaining and presenting dedicated radio parameters.**		
Description: The Resource Inventory Management shall allow maintaining and presenting the radio parameters including ANR specific values for each planned eNodeB (normally prepared by the planning processes).		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details of characteristics of resources.		

REQ-InvM (39)

Identifier: REQ-InvM (39)	**Rel. Use case id: UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title: **Data modelling and data entry.**		
Description: Resource Inventory Management shall support the required data modeling and data entry (manual as well as via discovery & reconciliation).		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-		

efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristics of resources.

REQ-InvM (40)

Identifier: REQ-InvM (40)	**Rel. Use case id : UC-RIM-6, UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title : **IP address space support.**		
Description: IP address space (logical resources) is part of the Resource Inventory Management – Resource Inventory Management provides capabilities for obtaining and defining public and private IP address space, and allocating parts of that address space to locations, subnets, devices, ports and address pools.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristics of resources.		

REQ-InvM (41)

Identifier: REQ-InvM (41)	**Rel. Use case id : UC-RIM-1, UC-RIM-10**	**Priority:**
Title : **Capabilities for modelling subnets and VLAN.**		
Description: Resource Inventory provides capabilities for defining subnets and VLANs.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristics of resources.		

REQ-InvM (42)

Identifier: REQ-InvM (42)	**Rel. Use case id : UC-RIM-1, UC-RIM-10**	**Priority:**
Title : **Recording IP address allocations.**		
Description:		

IP address allocations (whether manual or automatic) have to be recorded in a log file and as attribute of the target object.
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristics of resources.

8.5.2.3 Resource Inventory Management interfacing requirements

In the following requirements the purpose of interfacing of Resource Inventory with different other OSS applications are explained. TMF TAM is used as a generic model to present various applications/application areas of OSS environment.

REQ-InvM (43)

Identifier: REQ-InvM (43)	**Rel. Use case id : UC-Gen-SIM-RIM-1**	**Priority:**
Title: **Resource Inventory Management interfacing with Service Inventory Management.**		
Description: The Resource Inventory Management stores information on available capacity of logical and physical resources which needs to be accessible for Service Inventory Management in order to design a service. This interface is represented by Interface group C in Figure 14: OSS reference architecture emphasizing Inventory Management. Resource information models used are objects for standardization, but if a communication interface will be needed it is dependent on how Resource Inventory/Service Inventory combined concept is implemented.		
Rationale: Modular structures when composing services based on underlying resources is facilitated by smooth interworking between Resource Inventory Management and Service Inventory Management.		

REQ-InvM (44)

Identifier: REQ-InvM (44)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-5**	**Priority:**
Title: **Resource Inventory Management interfacing with resource order management.**		
Description: The Resource Order Management retrieves equipment and connectivity details from the Resource Inventory Management as well as provisioning rules and logic information in order to create requests to provision the network. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		

Rationale: A cost efficient and automated fulfillment process is achieved. Use of the service /resource design done in the service/resource catalogue as a driving model for the process. Reduced time-to-market by basing the fulfilment process on the service/resource catalogue data.

REQ-InvM (45)

Identifier: REQ-InvM (45)	**Rel. Use case id : UC-RIM-1, UC-RIM-2, UC-RIM-3**	**Priority:**
Title: **Resource Inventory Management interfacing with Fault Management.**		
Description: Fault Management retrieves information from Resource Inventory in order to correlate resource faults with resource topology information. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Consistent and harmonized resource information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration. For example common topology information is passed over to Fault Management.		

REQ-InvM (46)

Identifier: REQ-InvM (46)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-7**	**Priority:**
Title: **Resource Inventory Management interfacing with service problem management.**		
Description: Service Problem Management retrieves information from Resource Inventory to correlate service problems with resource topology information. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Consistent and harmonized resource information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration. For example common topology information is passed over to service problem management		

REQ-InvM (47)

Identifier: REQ-InvM (47)	Rel. Use case id : UC-Gen-SIM-RIM-1, UC-SIM-6	Priority:
Title: **Resource Inventory Management interfacing with service quality management.**		
Description: Service Quality Management retrieves information from Resource Inventory Management to correlate service quality with resource topology information. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization		
Rationale: Consistent and harmonized resource information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration. For example common topology information and KPI/KQI aggregation rules are passed over to service quality management.		

REQ-InvM (48)

Identifier: REQ-InvM (48)	Rel. Use case id : UC-Gen-SIM-RIM-1	Priority:
Title: **Resource Inventory Management interfacing with performance management.**		
Description: Performance Management accesses the Resource Inventory for having topology information to identify the appropriate performance data collection points. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Consistent and harmonized resource information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration. For example common topology information and KPI/KQI aggregation rules are passed over to performance management.		

REQ-InvM (49)

Identifier: REQ-InvM (49)	Rel. Use case id : UC-Gen-SIM-RIM-1	Priority:
Title: **Resource Inventory Management interfacing with resource discovery.**		
Description: Resource discovery function provides means to upload and reconcile the Resource Inventory information with the actual network element information. The interface is either provided via element management systems or in some cases directly		

to network elements. Resource discovery interfaces towards network is represented by Interface group B in the Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.
Rationale: Continuous resource discovery capability throughout the network infrastructure secures up-to-date resource inventory information.

REQ-InvM (50)

Identifier: REQ-InvM (50)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **Discovery and reconciliation of eNodeB data.**		
Description: Resource Inventory Management shall enable to discover/upload eNodeB data and reconciliate (between planned data and uploaded data) in real-time and respectively at dedicated intervals (<= 24h). Concerned data are the resource data for each installed eNodeB and the configuration data for each installed eNodeB.		
Rationale: Continuous resource discovery capability throughout the network infrastructure secures up-to-date resource inventory information.		

REQ-InvM (51)

Identifier: REQ-InvM (51)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **N-Itf support.**		
Description: Resource Inventory Management shall have access to configuration parameter sets on request via Itf-N in accordance with the northbound interface specification.		
Rationale: Standard interfaces reduce development time and costs.		

REQ-InvM (52)

Identifier: REQ-InvM (52)	**Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**

Title: **Periodical reconciliation of IP-related data.**		
Description: A periodical reconciliation of actual IP-related data from the network with the Resource Inventory Management has to be performed. Resource inventory information can be updated with information about assigned IP addresses and planning & design faults in the network can be recognized.		
Rationale: Continuous resource discovery capability throughout the network infrastructure secures up-to-date resource inventory information.		

REQ-InvM (53)

Identifier: REQ-InvM (53)	**Rel. Use case id : UC-Gen-SIM-RIM-1**	**Priority:**
Title: **Resource inventory synchronization.**		
Description: Resource inventory synchronizing function provides a common inventory view across the OSS management applications and ensures that resource inventory data generated in each application is available to other applications as required. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Consistent and harrmonized resource information models throughout fixed-mobile service production which uptodate based synchronization capability result cost-efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristicsof resources.		

REQ-InvM (54)

Identifier: REQ-InvM (54)	**Rel. Use case id : UC-Gen-SIM-RIM-1**	**Priority:**
Title: **Resource Inventory Management interfacing with billing mediation.**		
Description: Billing mediation accesses the resource inventory in order to retrieve topology information to identify the appropriate usage data collection points using standardized formats and protocols. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Resource Inventory Management provides a well-structured and consistent resource model to be used for associating		

the resources and topology with charging mediation events.

REQ-InvM (55)

Identifier: REQ-InvM (55)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **Resource Inventory Management interfacing with Configuration Management.**		
Description: Configuration Management performs the equipment configuration to bring resources into operation. It performs initial equipment configurations triggered by SI&P processes, and keeps the configuration data up-to-date. Configuration Management interface towards network is represented by Interface group B in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: All information related to resource infrastructure, configuration of it and its detailed features are closely related to each other and centrally managed in a uniform and structured way to reduce development and integration costs.		

REQ-InvM (56)

Identifier: REQ-InvM (56)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **Retrieval of configuration parameter settings.**		
Description: Configuration parameter settings for the resource object are retrieved from Resource Inventory Management by Configuration Management.		
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information models need to cover necessary details in terms of wideness in scope and characteristics of resources.		

REQ-InvM (57)

Identifier: REQ-InvM (57)	**Rel. Use case id : UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **Configuration notifications.**		

Description: Configuration Management notifies Resource Inventory Management about the results of configuration activity (successful or not).
Rationale: Consistent and harmonized resource information models throughout fixed-mobile service production result in cost-efficient information management and integration. The information and operation models need to cover necessary details in terms of wideness in scope and characteristicsof resources.

REQ-InvM (58)

Identifier: REQ-InvM (58)	**Rel. Use case id : UC-Gen-SIM-RIM-1**	**Priority:**
Title: **Resource Inventory Management interfacing with resource testing.**		
Description: Resource test management accesses Resource Inventory Management for obtaining the resource information under testing. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization		
Rationale: Resource Inventory Management provides a well-structured and consistent resource model for testing and diagnosis purposes.		

REQ-InvM (59)

Identifier: REQ-InvM (59)	**Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title: **Resource Inventory Management interfacing with other Resource Lifecycle Management.**		
Description: Resource Lifecycle Management applications/functions such as Resource Planning, Resource Change Management and Resource Catalogue Management produce and consume Resource Inventory data. This interface is represented by Interface group A in Figure 14: OSS reference architecture emphasizing Inventory Management It is an object for standardization.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (60)

Identifier: REQ-InvM (60)	Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10	Priority:
Title: **Providing current resources to planning.**		
Description: Planning systems need to retrieve resource information from Resource Inventory Management concerning current resources and/or their capacity.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (61)

Identifier: REQ-InvM (61)	Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10	Priority:
Title: **Update of planned resources.**		
Description: Planning systems need to update Resource Inventory Management with new information about planned resources and their characteristics and parameters.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (62)

Identifier: REQ-InvM (62)	Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10	Priority:
Title: **Planned parameters values transfer to Resource inventory.**		
Description: The Planning tool shall allow a consistent planning of all these parameter values, maintain them in its database and provide an interface to the resource inventory for parameter transfer.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service		

production result in cost-efficient information management and integration.

REQ-InvM (63)

Identifier: REQ-InvM (63)	**Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title: **Basic parameter transfer to resource inventory.**		
Description: Resource inventory shall provide an interface to the planning tools for parameter transfer (Basic set of parameters is defined by the planning tool (IP addresses, location, HW, transmission...)).		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (64)

Identifier: REQ-InvM (64)	**Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title: **Resource information to construction and implementation support systems.**		
Description: Construction and implementations support systems need to retrieve resource information from Resource Inventory concerning resources planned to be deployed. Information is for example about equipment types, volumes, implementation sites and locations etc.		
Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.		

REQ-InvM (65)

Identifier: REQ-InvM (65)	**Rel. Use case id : UC-RIM-7, UC-RIM-8, UC-RIM-9, UC-RIM-10**	**Priority:**
Title: **Update on new information of implented resources**		
Description: Resource inventory information is updated with new information about implemented resources and their readiness for operation.		

Rationale: Consistent and harmonized service information models between OSS applications throughout fixed-mobile service production result in cost-efficient information management and integration.

General interfacing

REQ-InvM (66)

Identifier: REQ-InvM (66)	**Rel. Use case id : UC-Gen-SIM-RIM-1, UC-RIM-1, UC-RIM-2, UC-RIM-3, UC-RIM-4, UC-RIM-5, UC-RIM-6**	**Priority:**
Title: **Near real-time interface between Service and Resource Inventory Management and OSS applications.**		
Description: Near real-time interface for data synchronization between Service and Resource Inventory Management and relevant OSS applications has to be implemented.		
Rationale: Information management within overall OSS environment is preferred to approach real-time to improve customer satisfaction. For example between service inventory/ resource inventory and assurance applications.		

8.5.3 OSS Architecture reference model, emphasizing Inventory Management

In the following figure a common OSS architecture reference model is presented emphasizing the central role of Inventory Management within OSS. The model is aligned with and adapted from TAM v4.5 focusing on the key features of Inventory Management and related applications.

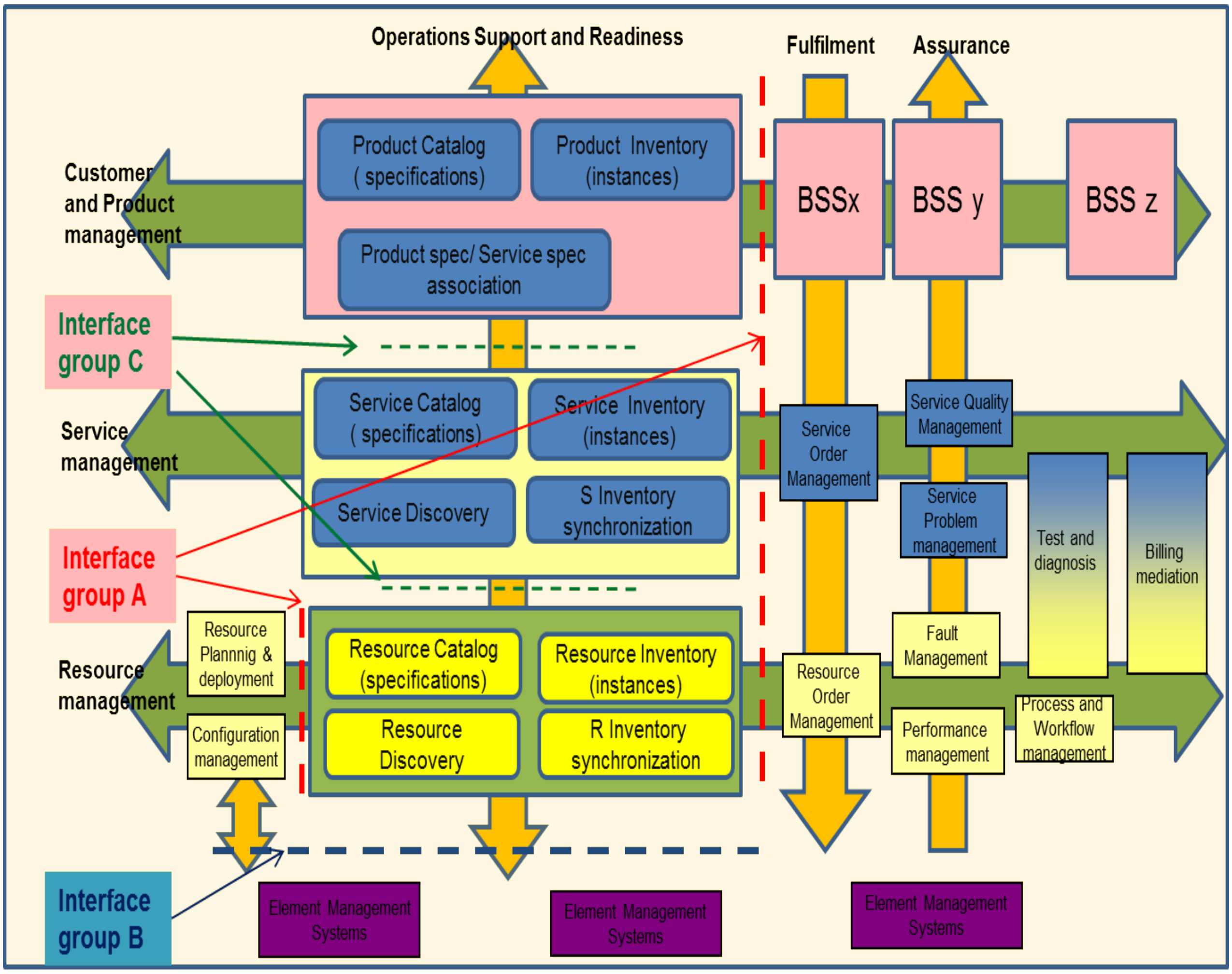


Figure 11-1: OSS reference architecture emphasizing Inventory Management

As a summary the key aspects of inventory focused OSS architecture reference model are:
For Resource Inventory Management

- Storing of resource specifications (Resource Catalogue).
- Storing of resource instances (Resource Inventory).
- Resource instance information is kept up to date with actual resource situation by resource discovery. (Resource Discovery)
- Resource instance information is synchronized with other OSS applications keeping resource information up to date throughout OSS. (Resource Inventory Synchronization).
- Resource Inventory exposes services to external systems for:
  - o to modify the content of the repository or
  - o to query the repository in order to collect specific information that it contains.

For Service Inventory Management

- Storing of service specifications (Service Catalogue).
- Storing of service instances (Service Inventory).
- Service specifications are associated with resource specifications, stored in the resource catalogue, thus capturing the relationship between a service and the set of resources supporting this service. (Service Discovery).
- Service instance information is synchronized with other OSS applications keeping service information up to date throughout OSS. (Service Inventory Synchronization).
- Service Inventory exposes services to external systems for:
    - to modify the content of the repository or
    - to query the repository in order to collect specific information that it contains.

For Product Inventory Management

- Storing of product specifications (Product Catalogue).
- Storing of product instances (Product Inventory).
- Storing associations between product and service specifications.

Inventory interfaces

- Interface group A: Interfacing between Inventory Management area (generally Resource, Service and Product Inventory Management) and other OSS applications. For each interfacing requirement presented in chapters 5.1 and 5.2 the respective positioning within the OSS reference architecture is indicated. Each interface of group A requires
    - A standardised information model of the data exchanged between the interworking OSS applications.
    - A standardised operations model including the methods and parameters transferred over the interface.
    - Standardised notifications transferred over the interface.
- Interface group B: Interfacing between Resource Inventory Management area and EMS layer. For each interfacing requirement presented in chapter 5.2 the respective positioning within the OSS reference architecture is indicated. Each interface of the group B requires:
    - A network resource model representing the different underlying infrastructures which shall be compliant with the federated network information model (FNIM, ref. NGCOR Modelling and Tooling general requirements) for inventory.
    - A standardised operations model including the methods and parameters transferred over the interface.
    - Standardised notifications transferred over the interface.

- Interface group C: Indication of potential internal interfacing between different Inventory Management area building blocks. For each interfacing requirement presented in chapters 5.1 and 5.2 the respective positioning within the OSS reference architecture is indicated. For this Interface group it is however to be noted that internal structure and functionality may differ depending on the implementation model.

It is to be noted that Figure 14: OSS reference architecture emphasizing Inventory Management structure does not imply any implementation model. Which means that implementation models derived from thisreference model can include variants e.g.

- Service and Resource Inventory may be implemented together or separately.
- Discovery and synchronization may be implemented as separate applications or jointly with inventories.
- Needed databases can be centralized or distributed and federated.

Moreover it is to be noted that some aspects were not analyzed in detail within this NGCOR project and thus are potential items to be considered for Inventory Management future work:

- Overall needs for common data management processes, represented by inventories, involving all lifecycle phases of Inventory Data Management. This is addressed by high level requirement REQ-InvM (4).
- Resource configuration data is in generic way regarded as part Resource Information Management, i.e. part of Resource Inventory Data, for example configuration information and parameters to setup and restore devices and applications of the Service Provider's Production Infrastructure. However details of the preferred model for implementation of needed data stores are not analyzed further in NGCOR Inventory Management stream. One possible implementation approach is to have a specific configuration inventory.
- Inventory Management as a subject of overall policy management framework of operators. A Policy Management Framework provides the capability to govern the observed behavior of objects within the framework, e.g. defining access to information, resources, services and the frame of administrative procedures. For example TMF Catalogue management descriptions expand the catalogue concept to include in addition to product/service/resource specifications also policy specifications. These policy specifications are to be utilized when evaluating the rules in policy decisions and enforcing the rules within the OSS architecture. One possible implementation approach is a specific policy inventory.

8.5.4 Considerations Related to Other Reference Models

Figure 6 shows the key scope of the NGCOR inventory stream in terms of the **TMF business process framework** (eTOM). The relevant level 3 processes concerned by the project's work are "**Manage Service Inventory**" (MSI) and **Manage Resource Inventory** (MRI). MRI and MSI are part of the operations process area. Vertically they are included in the **Operations Support & Readiness** processes. Horizontally they are covered by the service management & operations processes (for MSI), and by the **Resource Management & Operations** processes (for MRI). Both MSI and MRI are defined to have wide interaction horizontally and vertically.

In relation to **ITIL framework** it is considered generally that ITIL practices and related system solutions share an analogue problem with telecom inventories on how information about IT infrastructure components and services can be managed. A respective key concept in ITIL framework is the **Configuration Management System** (CMS); a coherent logical model of the IT organization's infrastructure, typically made up of several **Configuration Management Databases** (CMDBs) as physical sub-systems. It is used to store information on all configuration items (CIs) under the control of Configuration Management. CIs are mainly hardware or software items and are characterized by their attributes (recorded in the CI's Configuration Record) and their relationships to other CIs. Similarly like a telecom inventory information is used e.g. by other operations process, the ITIL CI information is utilized by e.g. ITIL incident management, problem management and change management processes. It is notable that TMF and itSMF have done a joint technical work for converging TMF and ITIL concepts – the report is: TR143 Building bridges ITIL and eTOM. [32]

The main characteristics of CMDB and also differences with inventory can be highlighted as follows:

- CMDB maintains the relationships between all service components and any related incidents, problems, known errors, changes and release documentations.
- CMDB may contain:
    - Relationships between applications and server.
    - SW version history trace for network equipment and applications in order to allow restoring previous version in case of rollback.

- Records with content of a release linked to all configuration items that are affected by the release of different types of CIs:
    - Service lifecycle CIs such as the business case, service management plans, service lifecycle plans, service design package, release, change plans and test plans. These CIs provide a picture of the service provider's services, how these services will be delivered, what benefits are expected, at what cost, and when they will be realized.
    - Service CIs such as:
        - Service capability assets: management, organization, processes, knowledge, people.
        - Service resource assets: financial capital, systems, applications, information, data, infrastructure and facilities, financial capital, people.
        - Service model.
        - Service package.
        - Release package.
        - Service acceptance criteria.
    - Organization CIs: Organization's business strategy or other policies that are internal to the organization but independent of the service provider. Regulatory or statutory requirements.
    - Internal CIs comprising those delivered by individual projects, including tangible (data centre) and intangible assets such as software that are required to deliver and maintain the service and infrastructure.
    - External CIs such as external customer requirements and agreements, releases from suppliers or sub-contractors and external services.
    - Interface CIs that are required to deliver the end-to-end service across a service provider interface (SPI).
- CIs include also details such as supplier, cost, purchase date and renewal date for licences and maintenance contracts and the related documentation such as SLAs and underpinning contracts.

The Inventory that is considered in OSS architecture provides to CMDB only information related to network configurations and service configurations linked to network resources, and not information related to cost, licenses, contracts, etc. CMDB can be considered as a federated DB that takes from inventory only a set of information and takes from other sources additional information needed to support other ITIL processes.

Considering scoping with regards to 3GPP specifications it is to be noted that it is not possible to show direct match. 3GPP specifications do not model distinct management layers and structures for upper layer NMS/ OSS (service management, resource management). Both resource infrastructure information and service related information is defined via NRM IRPs and interface IRPs.

Inventory Management IRP from 3GPP is defining the main task of the Inventory Management function at Itf-N to provide an efficient access for network management systems to the static inventory data of all related managed network elements. This is regarded as an essential part of overall Inventory Management reference model providing standard inventory data to be uploaded to NMS/ OSS concerning the network elements in the scope of 3GPP.

8.6 INVENTORY MANAGEMENT STREAM DETAILED INFORMATION

8.6.1 Service Inventory Management realization examples

8.6.1.1 Service scenario example on Service Problem Management facilitated by Service Inventory Management [79]

8.6.2

Introduction

Extensive growth of telecom market and its constant evolution create highly competitive environment for service providers and make them focus more than ever on the quality of service delivery to retain their customer base. For the effective service assurance it is critically important to have detailed and highly consolidated service, resource and customer information. Fast access to this information and ability to quickly identify customer to service to resource relation, extended knowledge base, predefined rules for root cause identification and problem resolution patterns tied to service type and service structure are key points to guarantee that service issue will be resolved quickly and with minimal impact on customer.

The examples provided in this chapter are aimed to illustrate how Service Inventory consolidates all service-related information and thus is centric for service problems prevention, analysis and resolution.
The examples visualize generic use case 4.3.5.2 Service inventory support for service problem management: Impact analysis and root cause analysis on the example of VoIP service.

Prerequisites from scenarios

For successful implementation of these example service scenarios the following use cases as pre-requisites are required

- UC-SIM- 1; Deriving service specification from product specification and Modeling service reflecting the underlying technology infrastructure
  - Customer Facing Service and Resource Facing Service specifications are determined
  - Technology infrastructure components needed to implement the specified services are determined
  - Quality and performance characteristics required per CFS and RFS are identified

- UC-SIM-2; Analyzing service models details from system architecture design process point of view - the service meta-model
  - Service information models designed to include capabilities to support for service assurance
    - Information on mapping of the SLA and related SLA parameters to service specification
    - Information on mapping of the customer SLA parameters to service level KQIs/KPIs
    - Information on calculation and aggregation of customer SLA based on service level KQI/KPIs
    - Values for thresholds and time dependencies of SLA parameters and respective service level KQIs/KPIs
    - Information on mapping of a service model to resource model
    - KQI/KPI calculation and aggregation rules based on service/resource information model structure
    - information on consequences if service quality or service performance targets are not met

Principal Approaches to Service Problem Management

Two principal scenarios can be distinguished for service problem management—reactive problem management and proactive problem management. Both scenarios involve Service Problem Management core from one side for aggregating and correlation of incoming data such as network alarms, resource performance information or customer trouble tickets, and Customer, Service and Resource Inventory from the other side to supply information that allow tracking bottom to top relationships to effectively detect problem source, severity, and impact.

Reactive Problem Management

Reactive problem management scenario originates from several sources that include network fault event received from downstream Fault Management systems, planned maintenance event, or customer complaint received from upstream customer care systems. Receiving such a request results in creation of a service trouble-ticket in Service Problem Management system, and invokes processes that depending on the origin of the request can be:

- o Root cause identification and resolution
- o Building impact propagation tree, identification of affected customers, customer notification and problem resolution.

Reactive problem management cases will be considered in more details below in this chapter.

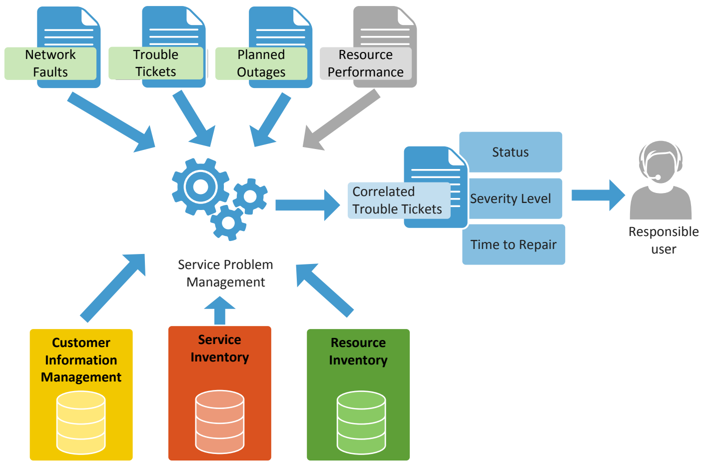


Figure 12-1: Information flows related to reactive problem management

Proactive Problem Management

Proactive Problem management scenario implies early identification of potential service issues and undertaking corrective actions before customer is even noticing the problem. Proactive problem management is based on collecting and analyzing service performance data and requires constant monitoring of service performance parameters and comparing it to thresholds pre-established for the given service type. In this scenario Service Inventory cumulates performance data relevant to a specific service instance, provides allowed threshold values and SLA, and allows quick identification of services where SLA is under the risk of violation.

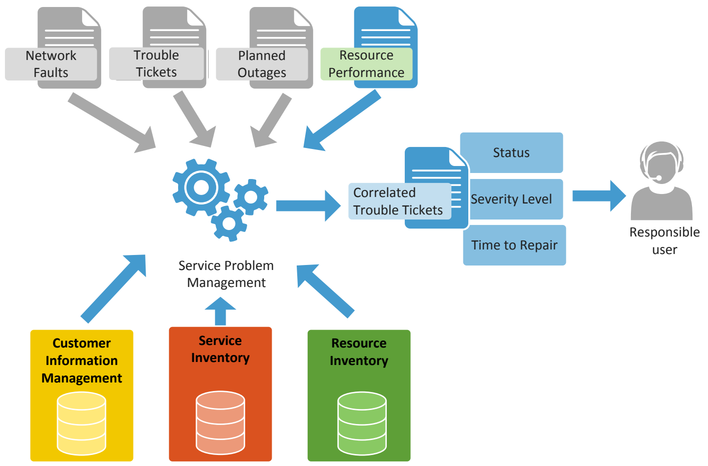


Figure 12-2: Information flows related to proactive problem management

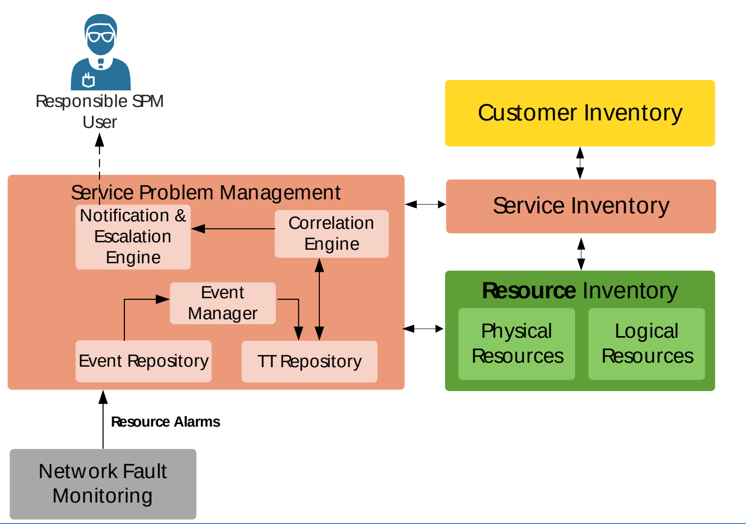
Proactive problem management will not have detailed consideration here and is listed to provide more holistic view on difference aspects of service problem management.

Impact Analysis

This use case is provided to exemplify how Service Problem Management uses service inventory information to analyze the impact of network fault event to customer services.

Business Flow

The main steps of the process can be described as following:



Receive alarm from FMS
Create, validate and prioritize alarm
Create Resource TT and associate it with Resource Inventory
Perform impact analysis and propagation, identify affected services and customers
Correlate TT information with existing tickets, planned outages, and create/modify Service TT
Collect details of service statuses, orders, SLA
Define Service TT severity
Notify results of impact analysis basing on notification/escalation rules to SPM responsible user

Figure 12-3: Main steps related to service problem impact analysis

Impact analysis is performed based on the inventory information available.

Resource Inventory	Allows localization of physical resources affected by event Provides physical resource structure and details Provides information on impact on logical resources associated with physical resources Provides access to planned outage information for the resource thus allowing correlation of network event with this information
Service Inventory	Provides information on impact on Resource Facing Services associated with erroneous resources Provides information on service topology and Customer Facing Services associated with affected RFS Provides information on SLA metrics and SLA level associated with service type or service instance and allows issue severity assessment
Customer Inventory	Allows identification of affected customers through customer to CFS relationship

Figure 18 is an illustration how inventory information captured on different levels helps in the analysis of impact of resource failure to customer.

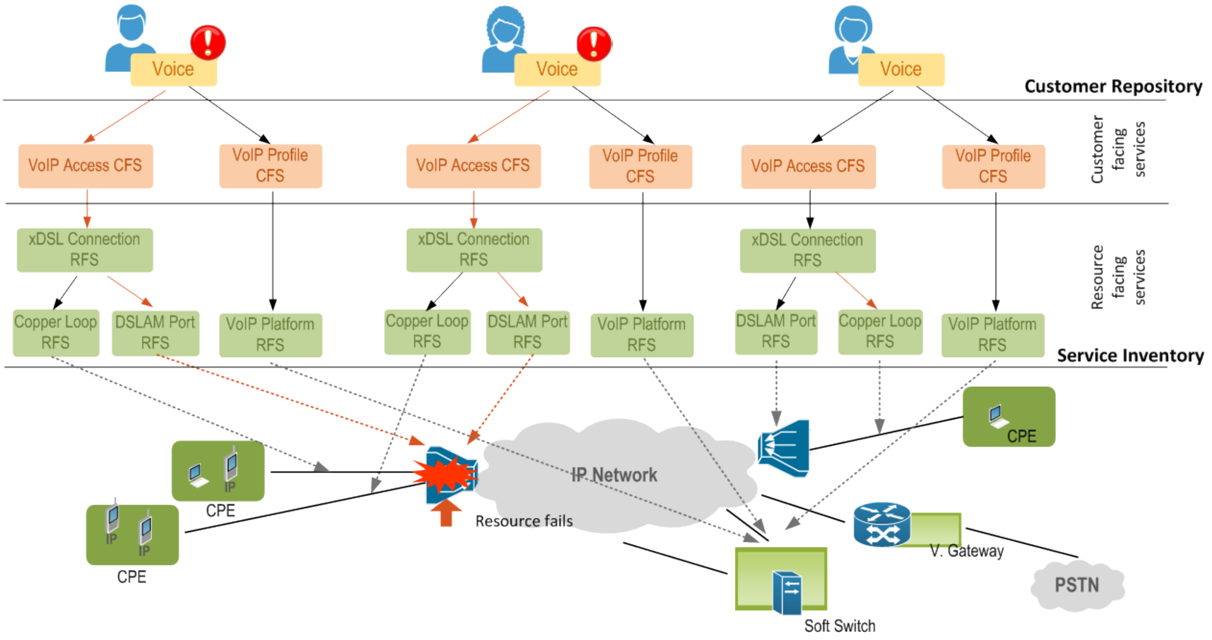


Figure 12-4: Analysis of impact of resource failure to customer supported by inventory information

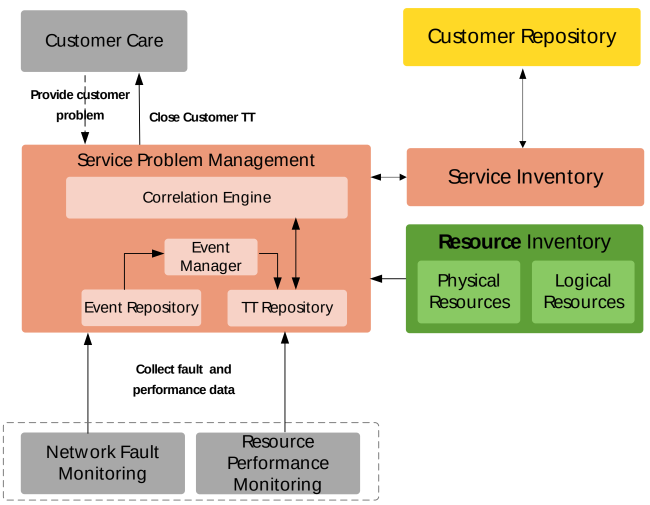
Alternative example of utilization of information stored in Service Inventory would be planned outage tracking to enhance customer impact analysis capabilities by taking into consideration planned maintenance work and network outages. This will allow preemptive identification of all services/customers that will be impacted by specified outage/maintenance work.

Root Cause Localization

This use case is provided to exemplify how Service Problem Management uses service inventory information to perform root cause localization after customer complaint on service quality is received.

Business Flow

The main steps of the process can be described as following:



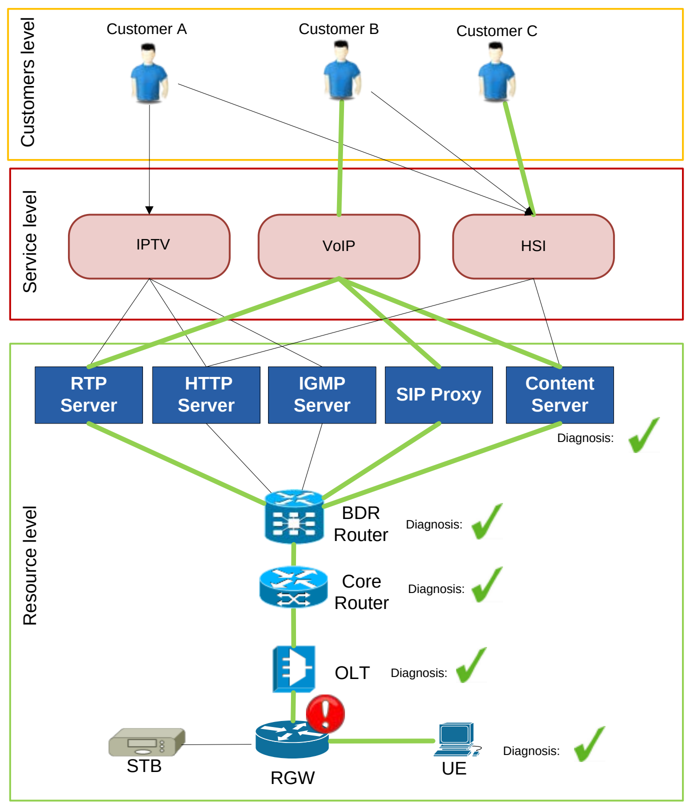
Receive customer complaint and confirm problem
Create Service TT
Identify list of known problems (service incidents, planned maintenances, known errors) for verified service
Identify service component and depending resources structure
Query data sources based on service/resources structure (planned outages, KPI/KQIs, related tickets)
Correlate and enrich data
Examine problem based on gathered data and pre-defined metrics and localize problem source

Figure 12-5: Main steps related to service problem root cause analysis

Problem localization is performed based on the inventory information available.

Resource Inventory	Provides access to planned outage information for the resource thus allowing correlation of network event with this information Provides information on resource infrastructure and topology
Service Inventory	Provides information on customer service related to customer complaint Provides information on service topology and Resource Facing Services associated with customer service Allows identification of resources providing service through RFS to resource associations Provides information on service level KPI/KQIs values and thresholds set up per service/service type Allows issue severity assessment basing on SLA level defined for the service
Customer Inventory	Provides access to open and history trouble tickets for customer

The example below demonstrates how KPI/KQI values defined for the components implementing service structure are used in problem analysis and root cause detection. Service topology information and its association to resource level allows collection resource performance data relevant for the service while pre-defined rules allow detection of the problem localization.



Problem Confirmation

<u>Complaint</u>

Poor Voice quality

<u>KPI/KQIs</u>

Data Rate < 500 Kbps
Packet Loss Rate > 15%
Packet Jitter > 2 ms
Transmission Rating Factor < 60

<u>Possible Root Causes</u>

Network: Link Overloaded
Network: RGW CPU capacity depleted

Problem Localization

<u>Root cause</u>

Poor Voice quality

<u>KPI/KQIs</u>

Service Circuit Throughput < 500 Kbps
Congestion alarms exists on Service Circuit
Service Circuit Bandwidth left < 5%

<u>Root cause</u>

RGW Packet Transmission Delay

<u>KPI/KQIs</u>

RGW Packet Jitter > 2 ms
KPI: Round Trip Time > 400 ms

Figure 12-6: Illustration of KPI/KQI values defined for the components implementing service structure are used in problem analysis and root cause detection

8.6.2.1 Service scenario example on Service Quality Management facilitated by Service Inventory Management [80]

Introduction

Traditional network assurance comprises of two complementary systems: Performance Management (PM) and Fault Management (FM). The first one deals with network performance metrics (KPI), and the second one – with network outages. Performance metrics can have a defined threshold, which should generate an alarm feed to the FM system, once exceeded. This way PM and FM systems provide comprehensive network assurance. But, as both systems manage the network only from the resource perspective, they can't directly provide information about the impact on customer services. PM and FM can tell you if some network elements are experiencing outages or what the technical parameters of network connections are, but they will not inform you what kind of impact these network problems have on customer services. The transformation described below aims for being able to translate network faults and metrics into customer service issues and metrics (KQIs).

This example provided in this chapter is aimed to illustrate how Service Inventory consolidates all service-related information and thus is centric for service quality management. The examples visualize 4.3.5.1Service inventory support for service quality management on the example of Blackberry service.

Prerequisites from scenarios

For successful implementation of these example service scenarios the following use cases as prerequisites are required

- UC-SIM- 1; Deriving service specification from product specification and Modeling service reflecting the underlying technology infrastructure
  - Customer Facing Service and Resource Facing Service specifications are determined
  - Technology infrastructure components needed to implement the specified services are determined
  - Quality and performance characteristics required per CFS and RFS are identified

- UC-SIM-2; Analyzing service models details from system architecture design process point of view - the service meta-model
  - Service information models designed to include capabilities to support for service assurance
    - Information on mapping of the SLA and related SLA parameters to service specification
    - Information on mapping of the customer SLA parameters to service level KQIs/KPIs
    - Information on calculation and aggregation of customer SLA based on service level KQI/KPIs
    - Values for thresholds and time dependencies of SLA parameters and respective service level KQIs/KPIs
    - Information on mapping of a service model to resource model
    - KQI/KPI calculation and aggregation rules based on service/resource information model structure
    - information on consequences if service quality or service performance targets are not met

Employing servcie model to PM to SQM tranformation

Transformation should be based on augmenting the PM system with service quality management (SQM). This augmentation should enable to translate technical network metrics (KPIs) into customer service metrics (KQIs). The calculations should be based on service modelling (maintained in the network andservice inventory), that enables capturing different types of customer services, with different requirements towards network resources. These requirements must be taken into account when performing the calculations mentioned above.

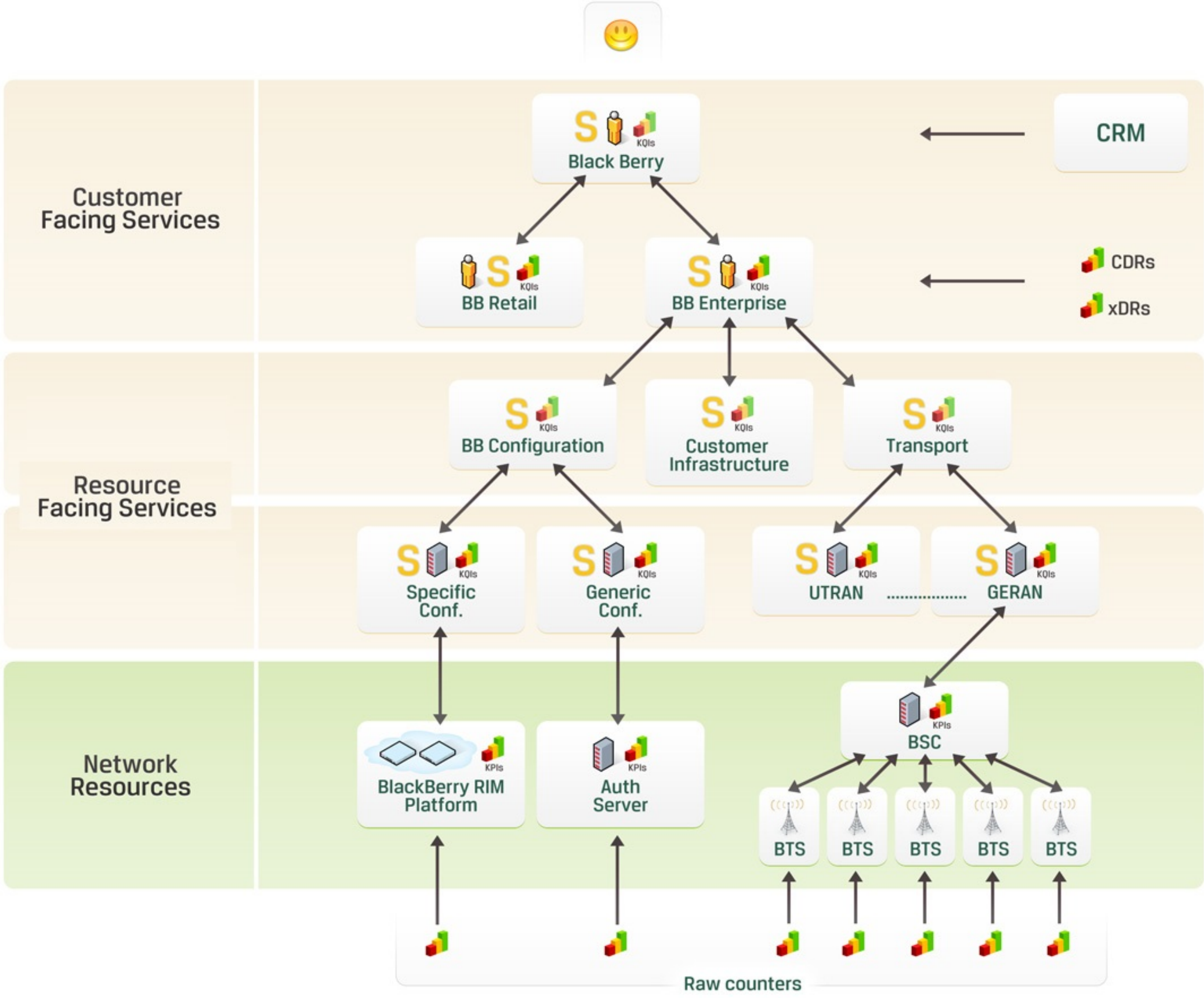


Figure 12-7: Employing the service model for KPI to KQI translation and end-to-end SQM

KQI definitions are calculated using customer service models and formulas that translate KPIs into KQIs along a service tree, as depicted in Figure 21. This means that KQIs are as good as the service model and formulas, which makes it challenging to define them correctly at first attempt. Therefore it is crucial for service providers to have a mechanism for KQI verification and tuning in the form of a learning process.

Service model and KQI formula tuning

The idea is based on using information obtained from customer complaints. These have one important characteristic – they come directly from the customer, and thus reflect a real-life perception of the quality of service. Information from endto-end probing systems can play a similar role in monitoring application sessions, so that they can be easily interpreted as direct indicators of customer service quality. The verification is performed by matching KQIs with customer complaints and probing data. If there is a customer complaint about the quality of a service, for which KQIs are OK, then it can mean that the KQI calculation needs tuning. The problem may result from the customer service model that does not correctly capture all dependencies between network resources and customer services. It can also be an outcome of formulas incorrectly translating resource KPIs into KQIs. Feedback from customer complaints and probing data allows defining the KQIs correctly. This process is not easy, and requires an iterative approach.

Matching the calculated KQIs with the corresponding customer complaints and probing data solves two problems. It enables to verify the KQIs and assure that they can be trusted. But it also provides the benefit of stream lining the resolution of customers' problems.

8.6.2.2 Some industry examples related on service modelling and Inventory Management

There are many different ways products, services and resources can be modeled according to the TM Forum SID model (see chapter A.1) in terms of their hierarchical structuring. The hierarchical relationship of Product, Service and Resource is specified by the introduction of Customer Facing Services (CFS) and Resource Facing Services (RFS). A generic example for this kind of structuring is shown in Figure 15.

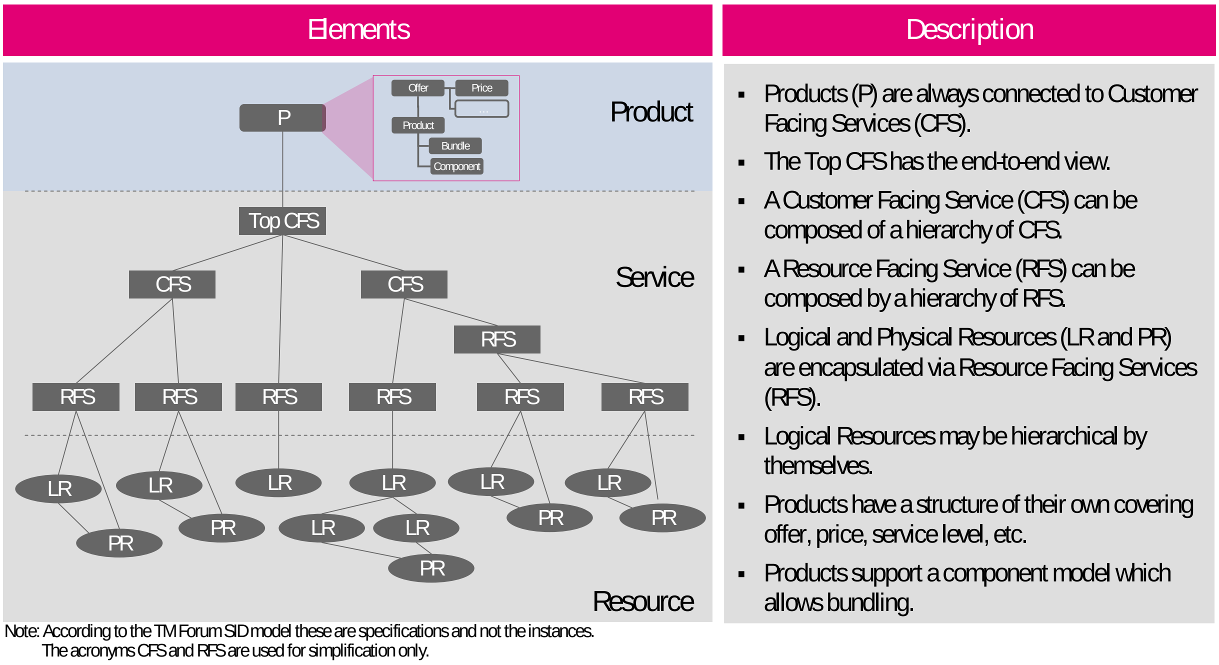


Figure 12-8: Hierarchical Structuring of Products, Services and Resources

Figure 23 shows a draft example for the conceptual modelling of a data link product based on Optical Transport Network (OTN) following these rules.

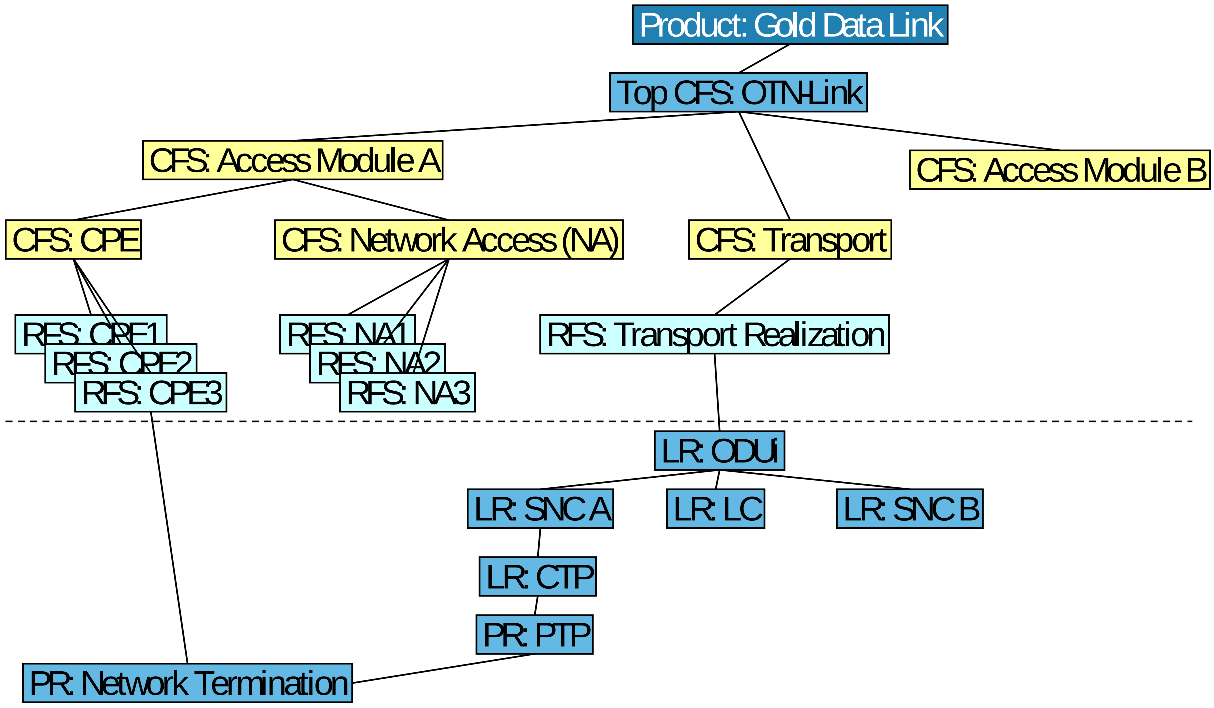


Figure 12-9: Example for a conceptual modelling of an OTN link product

There are several further examples for modelling of services based on the TM Forum SID model to get a better understanding of this concept. A selection of them is given in the following:

- **TM Forum TR153, Product-Service-Resource Information Model for E-mail, Case Study** [70]**:** This case study presents a top-down analysis of an example mail service from the product marketing level down to the resources. It identifies the different levels of the construction of a marketable product from services and resources and explains the major business entities in a tutorial style. The goal of the case study is to build a common understanding of these major entities and their relations on the basis of a real-world example.
- **TM Forum SD2-21, Ethernet Service Specification** [71]**:** An example of an Ethernet Service Definition and associated Service Template (Specification) is provided for the provisioning of a Broadband Ethernet Access line service.
- **TM Forum SD2-19, VoIP Service Definition** [72]**:** This document contains a Service Definition example for Voice over IP and also includes an example of a Service Template (Specification) which shows how it fits into the overall product/service context.
- **TM Forum GB917, SLA Management Handbook** [73]**:** This document defines a framework for specifying, deploying, managing and assessing the operation of Service Level Agreements (SLA). It also includes some examples in the context of CFS/RFS modelling related to SLA management.
- **TMF867** Product and Service Assembly (PSA) Catalyst, Interface Implementation Specification, Release 2.0, [82]
    - PSA architecture envisages that knowledge of bundling should be removed from existing systems, as far as possible, and be collected within new Active Catalogue systems.
    - An Active Catalogue is the place where all of the service and product building blocks are modeled, for example network equipment, applications, or even more abstract building blocks

such as work instructions and instructions for rating. These building blocks are modeled as components within the Active Catalogue and can be assembled into service or product offerings that make sense to the customer or to a product manager.

- Active Catalogue component definition includes full instructions for automated CAM-like handling of the component. The components understand or reference the processes that live within the traditional OSS/BSS stack needed for delivery (Fulfillment) and management (Assurance) of that component, for example the activation process, the billing process, or the element managers that manage resources directly. Each existing system remains in control of its own specialist area, with its own Service Creation tools, etc. The change from the traditional approach is mainly to make these systems offer functions of smaller scope, specifically designed for reusability.

8.7 CONCLUSIONS

Development of Inventory Management and migration to well-governed service and resource information management facilitated by new inventory solutions is foreseen to be one of the main challenges in coming years within operator's OSS landscape. By taking the Inventory Management as the focal point of OSS architecture development it is possible to take into account the different needs arising from the service production and operations in a holistic way and pave the way for more efficient system development as well as more cost-efficient production and operations as the end result. As a key direction to standardization and solutions from OSS suppliers is the need for standardized service and resource information models which are to, lead lower implementation, integration and maintenance costs and more radid development.

NGCOR Inventory Management stream has described about 20 use cases related to Service and Resource Inventory Management. It is understood that there are possibilities to consider tens or hundreds process use cases and various levels of details of them. The viewpoint of NGCOR has been to analyze a selected set of use cases, which is regarded to give comprehensive enough rationale for wanted directions service and Resource Inventory Management development overall by setting the main principles, concepts, inventory information usage and interaction, as well as and benefits of those. Regarding the derived Inventory Management requirements it can also be stated that it is possible to develeop more granular and detailed level of requirements. It is left up to forthcoming projects and work if more detailed use case or requirements will be defined.

Based on an analysis of the current activities in standardization organizations on Inventory Management the following **recommendations addressing the NGCOR needs** are given concerning future activities:

- **TM Forum:**
  - The work on TIP generic patterns with information model independent concepts should be continued. In the context of NGCOR an application of these patterns to resource and service inventory domains has turned out to be important. The usage of SID is a good choice for the first step. As soon as inventory definitions are provided by the JWG on MA, the generic TIP patterns can also be applied to this joint model.
  - The work on catalogue management interfaces should be continued. Especially the interfaces between service and resource catalogues with resource and service inventories including information modelling, in line with the work of TIP Inventory, are of interest in the context of NGCOR.
  - In the TAM specification [52] there are some parts to be added concerning catalogue and Inventory Management: Functionality and supported business services for Service Catalogue Management and

Resource Catalogue Management, and supported business services for Resource Inventory Management.

- TM Forum is expected to continue its wide prorams on e2e multi-cloud management area for further detailed specifications of cloud service management interfaces. Especially unform service and resource modeling is seen a key issue from Inventory Management point of view.

- **3GPP SA5:**

  - In 3GPP SA5 the MSDO Model Alignment work on UIM inventory definitions should be considered in furure Inventory specifications as soon as they are available.

- **Multi-SDO JWG on Model Alignment (MA):**

  - Inventory related objects, attributes and relationships should be defined in the Umbrella Information Model (UIM) according to the requirements from NGCOR, 3GPP and TM Forum.

- **ETSI ISG for NFV**
  - In the work starting up in ETST ISG a consistent management and orchestration architecture is required to be worked on. To rapidly align management and orchestration north bound interfaces to well defined standards and abstract specifications is of key importance.

8.7.1

8.8 REFERENCES

[18] NGMN Alliance NGMN TOP OPE Requirements Version 1.0
[19] NGMN NGCOR Consolidated Requirements V1.3
[20] University of Southern California - Center for Software Engineering - COTS Software Integration Cost Modelling Study 1997
[21] COCOTS (COnstructive COTS) - a cost estimation model to capture most important costs associated with COTS component integration, October 2002
[22] "Next-generation service assurance improves operational efficiency" in TM Forum CaseStudy Handbook 2012
[23] 3GPP TR 32.828 version 1.5.0. Study on Alignment of 3GPP Generic NRM IRP and TMF Shared Information/Data (SID) Model
[24] 3GPP TS 32.140. Subscription Management (SuM) requirements
[25] 3GPP TS 32.101 Telecommunication management; Principles and high level requirements
[26] 3GPP TS 32.300 Configuration Management; Name convention for Managed Objects.
[27] 3GPP TS 32.341/2/6. File Transfer (FT) Integration Reference Point (IRP); Requirements
[28] 3GPP TS 32.611/2/5 v10 Configuration Management (CM); Bulk CM Integration Reference Point (IRP): Requirements
[29] 3GPP TS 32.622. Configuration Management (CM); Generic network resources Integration Reference Point (IRP); Network Resource Model (NRM)
[30] 3GPP TS 32.690: Inventory Management (IM); Requirements; Version 11.0.0 Release 11; 09/2012.
[31] 3GPP TS 32.691: Inventory Management (IM) network resources Integration Reference Point (IRP); Requirements; Version 11.0.0 Release 11; 11/2012.
[32] 3GPP TS 32.692: Inventory Management (IM) network resources Integration Reference Point (IRP); Network Resource Model (NRM); Version 11.0.0 Release 11; 09/2012.
[33] 3GPP TS 32.696: Inventory Management (IM) network resources Integration Reference Point (IRP); Solution Set (SS) definitions; Version 11.1.0 Release 11; 03/2013
[34] 3GPP TS 32.xyz series on NRM.
[35] ATM Forum, Technical Committee, Network Management, M4 Network View CMIP MIB Specification, CMIP Specification for the M4 Interface, Sep, 1995.
[36] JOSIF Guidebook. Source: http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook
[37] NGWW 3GPP SA5-TM Forum model alignment JWG meeting in Budapest, April 4-6, 2011.
[38] NGWW Fixed Mobile Convergence (FMC) Network Management – Federated Network model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011.
[39] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3.
[40] TM Forum (2008a, Mai). DDP BA, TMF518_MRI, Version 1.1.
[41] TM Forum (2008b, Mai). DDP BA, TMF518_MSI, Version 1.0.
[42] TM Forum (2011, January). TM Forum Interface Program, Inventory Interface, Progress Status at TAW Paris.
[43] TM Forum GB922, Information Framework (SID) Suite, Release 9.0. Source: http://www.tmforum.org/browse.aspx?catID=9285&artf=artf2048
[44] TMF MTOSI 2.0. Source: http://www.tmforum.org/MTOSIRelease20/MTOSISolutionSuite/35252/article.html
[45] TM Forum MTOSI 2.0: Network Resource Fulfillment DDP IA, TMF612_NRF, Version 1.0.
[46] TM Forum Information Framework (SID) Suite; Release 9.5. Source: http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html
[47] TM Forum MTOSI Rel. 2.1 supporting document SD2-5_Communication_Styles.
[48] TM Forum SID Rel. 9.5.

[49] TMF & itSMF TR 143 Building bridges ITIL and eTOM.
[50] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx.
[51] UML Superstructure Specification, v2.1.1.
[52] 3GPP TS 32.300 Telecommunication management; Configuration Management; Name convention for Managed Objects
[53] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3
[54] S5vTMFa169 (3GPP/TM Forum Concrete Model Relationships and Use Cases) from 3GPP SA5-TM Forum Resource Model Alignment JWG ftp://ftp.3gpp.org/tsg_sa/WG5_TM/Ad-hoc_meetings/Virtual-TMF-Align/S5vTMFa169.zipftp://ftp.3gpp.org/tsg_sa/WG5_TM/Ad-hoc_meetings/Virtual-TMF-Align/S5vTMFa169.zip
[55] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx
[56] Fixed Mobile Convergence (FMC) Network Management – Federated Network Model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011
[57] TM Forum MTOSI Release 2.1 (http://www.tmforum.org/MTOSIRelease21/11998/home.htmlhttp://www.tmforum.org/MTOSIRelease21/11998/home.html)
[58] TM Forum Information Framework (SID) Suite; Release 9.5 (http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.htmlhttp://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html)
[59] TM Forum MTOSI Release 2.1: Supporting document SD2-5_Communication_Styles (http://www.tmforum.org/MTOSIRelease21/11998/home.htmlhttp://www.tmforum.org/MTOSIRelease21/11998/home.html)
[60] JOSIF Guidebook (http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook)
[61] JOSIF Guidebook (http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook)
[62] OMG Unified Modeling Language (OMG UML), Superstructure, Version 2.3 (http://www.omg.org/spec/UML/2.3/Superstructure/PDFhttp://www.omg.org/spec/UML/2.3/Superstructure/PDF)
[63] TM Forum MTOSI Release 2.1: Supporting document SD0-2_Guidelines_BA (Business Agreement Guidelines) (http://www.tmforum.org/MTOSIRelease21/11998/home.htmlhttp://www.tmforum.org/MTOSIRelease21/11998/home.html)
[64] TM Forum Business Process Framework (eTOM) Release 9 (http://www.tmforum.org/StandardsPacks/8175/home.htmlhttp://www.tmforum.org/StandardsPacks/8175/home.html)
[65] CCITT Rec. X.733 specification
[66] CCITT Rec. X.210 | ISO/TR 8509
[67] CCITT Rec. X.710 | ISO/IEC 9595
[68] eTOM Release 9.0, GB921 Addendum D,, TM Forum, August 2010
[69] TM Forum TAM Release 4.5, TMF, April 2011
[70] SID Release 9.5, GB922 Concepts and principles, TMF, March 2011
[71] This concept is explained further in TM Forum document SD2-1, MTOSI Implementation Statement (see section 2.5.1, Publisher Notification Suppression).
[72] TM Forum Manage Resource Inventory - DDP BA, TMF518_MRI, Version 1.1, May 2008.
[73] TM Forum Manage Service Inventory - DDP BA, TMF518_MSI, Version 1.0, May 2008.
[74] OSS/J Inventory API, JSR-142 Overview, Release 1.0, TMF888, TM Forum Approved Version 1.3, January 2010
[75] TM Forum comparison study of OSS/J, MTOSI and 3GPP inventory interface approaches

[76] TMF-SII_Inventory –Harmonizationn-Study_FDD_V1-0
[77] TMForum Interface Program, Inventory Interface, Progress Status at TAW Paris (Jan 2011).
[78] TM Forum Product, service and resource inventory retrieval for cloud and IT
[79] TM Forum Product, service and resource inventory update for cloud and IT
[80] in 3GPP TR 32.828 version 1.5.0
[81] 3GPP TS 32.341/2/6
[82] TMForum TR 146 Lifecycle Compatibility Release 1-0
[83] ITIL v3
[84] TM Forum, Catalogue Management FDD v1.12
[85] 3GPP TS 32.171 Subscription Management
[86] TM Forum Information Framework (SID), Release 12.5, Service Overview Business Entity Definitions, GB922 - 4SO, Version 9.7, September 2011.
[87] TM Forum TR 153, Product-Service-Resource Information Model for E-mail, PLM Case Study, Release 1.0, February 2010.
[88] TM Forum SD2-21, Ethernet Services Specification, V1.0, 2011.
[89] TM Forum SD2-19, Voice over IP Service Definition, V1.0, 2008.
[90] TM Forum GB917, SLA Management Handbook, Release 3.1, November 2012.
[91] TM Forum TR194 1.5, Multi-Cloud Service Management Pack – Introduction
[92] TM Forum TR195 1.5, Multi-Cloud Service Management Pack – Business Guide
[93] TM Forum TR196 1.5, Multi-Cloud Service Management Pack – Technical Guide
[94] TM Forum TR197 1.5, Multi-Cloud Service Management Pack – SLA Business Blueprint
[95] TM Forum TR178, Enabling End-to-End Cloud SLA Management
[96] Netcracker, Service scenario example on service problem management facilitated by Service Inventory Management
[97] Comarch, Service scenario example on service quality management facilitated by Service Inventory Management
[98] A group of operators, Network Functions Virtualisation – Introductory White Paper at “SDN and OpenFlow World Congress”, Darmstadt-Germany, October 22-24, 2012
[99] TMF867 Product and Service Assembly (PSA) Catalyst, Interface Implementation Specification, Release 2.0

APPENDIX:
A: SERVICE MODELLING ISSUES

A.1 Service Modelling in SID

The following considerations give a brief overview on the service modelling concept of the TM Forum SID model. They are taken from the current TM Forum SID specification Release 12.5 [69]. There are several important sources of information for these concepts. The most important of these is the Directory Enabled Networks (DEN-ng) service model.

For further more detailed information about the SID service information model including business entity definitions, definition of the attributes appropriate for the business level, and business models of the entities and their main relationships in UML, see TM Forum specification GB922 [69].

A.1.1 Conceptual Basic Service Model

Categories of the key service entities that need to be modeled are:

- A Service that is part of a Product, which is obtained by a Customer – this is a CustomerFacingService.
- A Service that is indirectly part of a Product, but is invisible to the Customer – it exists to support one or more CustomerFacingServices. This is a ResourceFacingService.

The reason that Services are linked to Products is that Customers obtain Products, not Services. Hence, they need to be able to express their needs in a language understood by an average consumer in order to determine which ProductOfferings support their requirements. Likewise, Service Providers and Enterprises need to be able to understand these requirements in order to realize the ProductOffering. These considerations yield the basic conceptual service model shown in Figure 24.
CFServiceRequiresRFServices aggregation defines the set of ResourceFacingServices that are required by a particular CustomerFacingService in order for that CustomerFacingService to operate correctly. A ResourceFacingService is related to LogicalResources and PhysicalResources through two aggregations, *LogicalResourcesImplementRFS* and *PhysicalResourcesHostRFS*. These aggregations define the set of LogicalResources and PhysicalResources, respectively, which are required for this ResourceFacingService to function correctly.
LogicalResourcesImplementRFS is used to define the set of LogicalResources, such as Memory and DeviceInterfaces, which are required for this particular ResourceFacingService to function correctly.
PhysicalResourcesHostRFS aggregation has a slightly different connotation. It defines the set of PhysicalResources, such as PhysicalDevices and PhysicalPorts, which are required for this particular ResourceFacingService to function correctly. Thus, the former aggregation defines the *operational* aspects of the ResourceFacingService, while the latter defines its *hosting* aspects. This separation is, of course, facilitated by the design of the Service (CustomerFacingServices vs. ResourceFacingServices) and Resource (PhysicalResource vs. LogicalResource) models.
is the superclass for both PhysicalResource as well as LogicalResource. Thus:

- PhysicalResources, such as a Customer's router, can be tied to a Product through the *ProductHasPhysicalResources* aggregation.
- LogicalResources, such as the programming of a particular device interface, are represented as ResourceFacingServices; hence, the *LogicalResourcesImplementRFS* aggregation relates these LogicalResources to a ResourceFacingService.

- Abstract items like “GoldService” are CustomerFacingServices and are represented using the *ProductHasCustomerFacingServices* aggregation.
- “GoldService” is supported by particular types of ResourceFacingServices through the *CFServiceRequiresRFServices* aggregation.

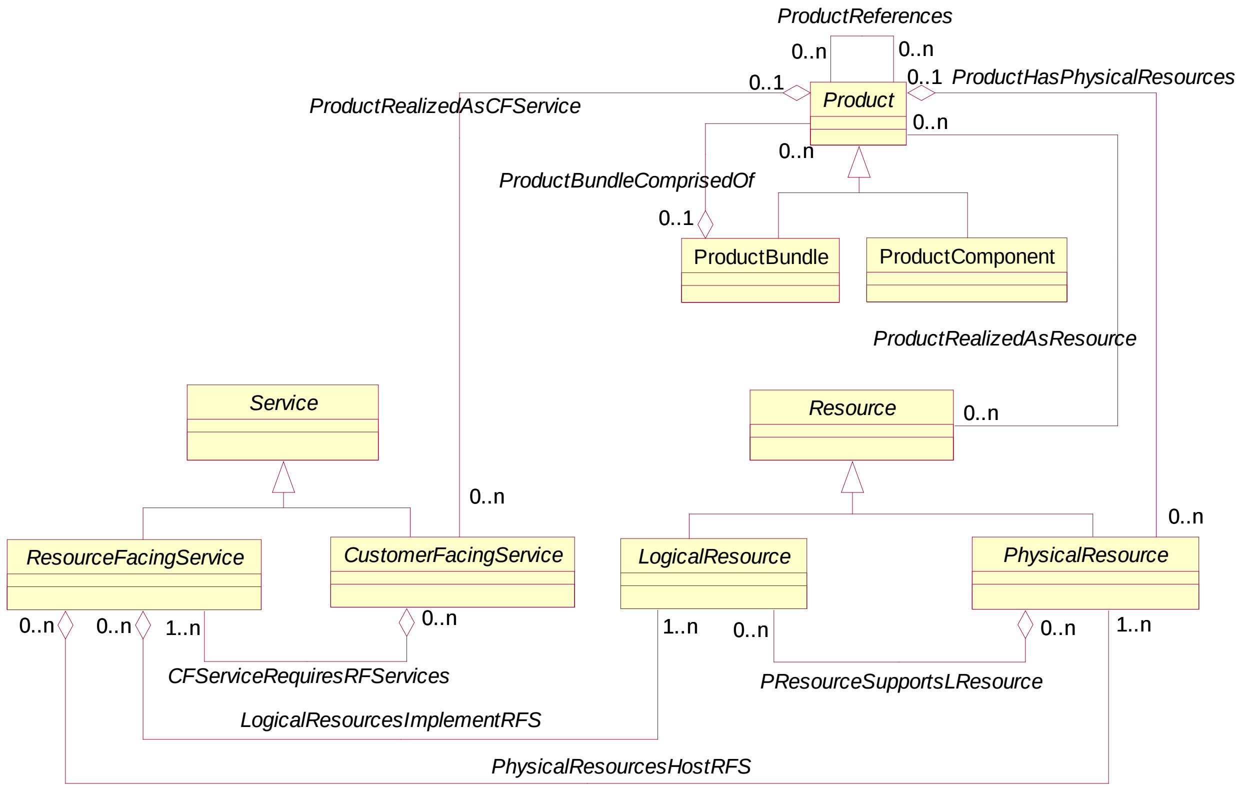


Figure 0-1: Conceptual Basic Service Model [69]

The model distinguishes between two types of Services – those that the Customer may be directly aware of, and those that the Customer is not directly aware of, but which are required to implement the functionality that the Customer desires. These are called CustomerFacingServices and ResourceFacingServices, respectively. In particular, the Customer may only see Resources and CustomerFacingServices, since they correspond to the physical and logical components of a Product that a Customer may be directly aware of.

A.1.2 ServiceSpecifications

ProductOfferings are tangible or intangible entities that Service Providers market, sell or lease to Customers. A ProductSpecification is a detailed description of a tangible or intangible object made available externally in the form of a ProductOffering to Customers, or other Parties. The information described by a ProductSpecification is a set of invariant data that is common to all realizations of that ProductSpecification. A ProductSpecification may exist as a single ProductSpecification, or consists of a set of ProductSpecifications supplied together as a collection.

ServiceSpecification is an abstract base class for representing a generic means for implementing a particular type of Service. In essence, a ServiceSpecification defines the common portions of a set of Services, while Service defines a specific instance that is based on a particular ServiceSpecification. This relationship is represented by the *SpecifiesService* dependency. This is shown in Figure 25: below.

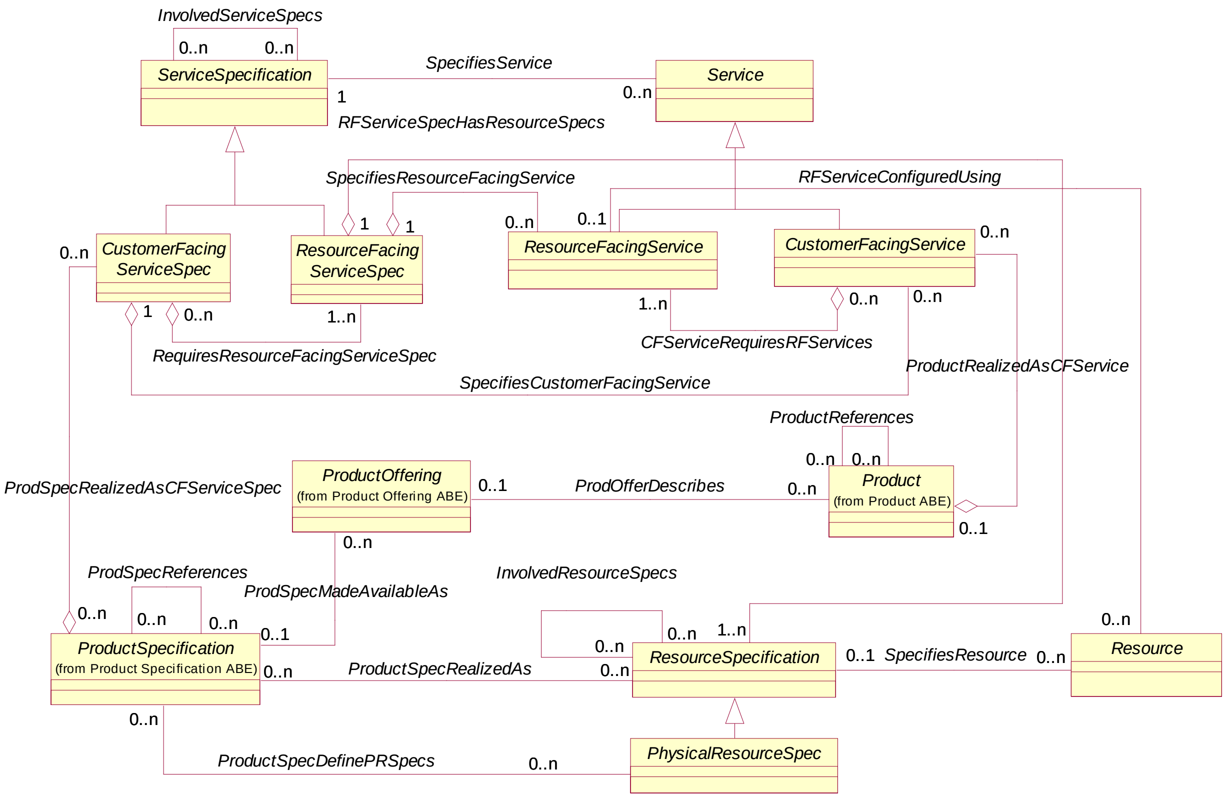


Figure 0-2: ServiceSpecifications [69]

ServiceSpecifications are generic in nature, just as Services are. The two subclasses of ServiceSpecification, CustomerFacingServiceSpec and ResourceFacingServiceSpec, are defined in an analogous manner to the two subclasses of Service, CustomerFacingService and ResourceFacingService.

The ServiceSpecification entity is designed to be subclassed to reflect different application-specific uses, and thus does not have attributes of its own.

There are many different types of CustomerFacingServices. They can be grouped together into similar Services so that each group is related to a particular CustomerFacingServiceSpec. A CustomerFacingServiceSpec can therefore be used to define the common and invariant characteristics and behavior for a set of CustomerFacingServices. Multiple CustomerFacingServiceSpecs can model the common characteristics and behavior of different groups of CustomerFacingServices. Furthermore, there are many different types of ResourceFacingServices. A similar logic is used to define how ResourceFacingServiceSpecs characterize the behavior of different groups of ResourceFacingServices. This is shown inFigure 26 below.

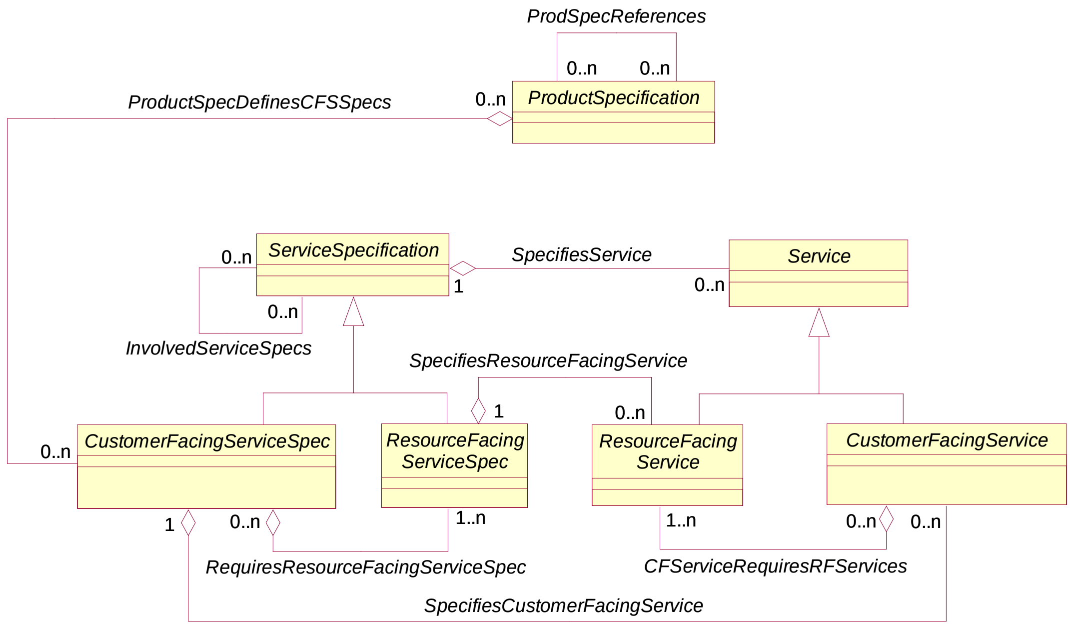


Figure 0-3: Subclassing ServiceSpecification [69]

A.1.3 SLA Modelling

This chapter shows the current state of the Service Level Agreement (SLA) Modelling work in the TM Forum SID specification [69] which is conformant with the TM Forum SLA Management Handbook [73].

A business party, such as a customer, expects a certain level of Service to be associated with a Product or Service procured from another business party, like a service provider or another enterprise. Such expectations are defined by a Service Level Specification (SLS), which is associated to a Product, Service or their respective Specifications. A Service Level Specification represents a pre-defined or negotiated set of Service Level Objectives (SLO) which defines the quality goal of a SLS. In addition, certain consequences are associated with not meeting the Service Level Objectives. Service Level Agreements are expressed in terms of Service Level Specifications.

Figure 27 shows a simple view of a Service Level Specification without attributes. The two subclasses of ServiceLevelSpecification are shown merely to emphasize the two different types of specifications.

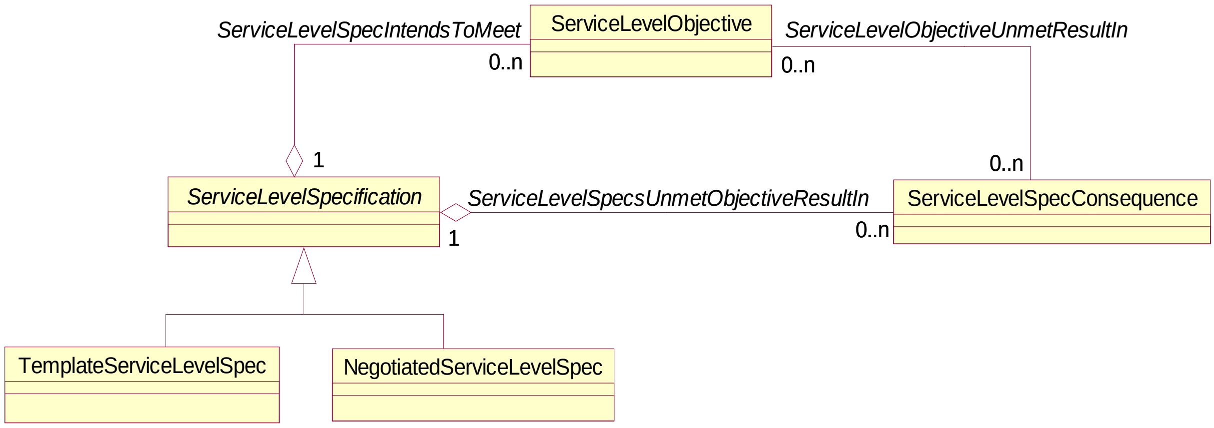


Figure 0-4: Service Level Specification Overview [69]

Customer Service Level Agreements are expressed in terms that a Customer can understand. These Service Level Agreements are defined in terms of Service Level Specifications related to ProductOfferings and ProductSpecifications. ProductSpecifications are used in order to define a set of invariant characteristics and behavior that the set of Service Level Specification will cover.

Internal Service Level Agreements are usually defined in terms of resource-facing Service Level Specifications. Supplier/partner Service Level Agreements can be expressed in terms of either customer-facing or resource-facing Service Level Specifications.

Figure 28 shows the Service Level Specification relationship to Products, Services, and their associated specifications.

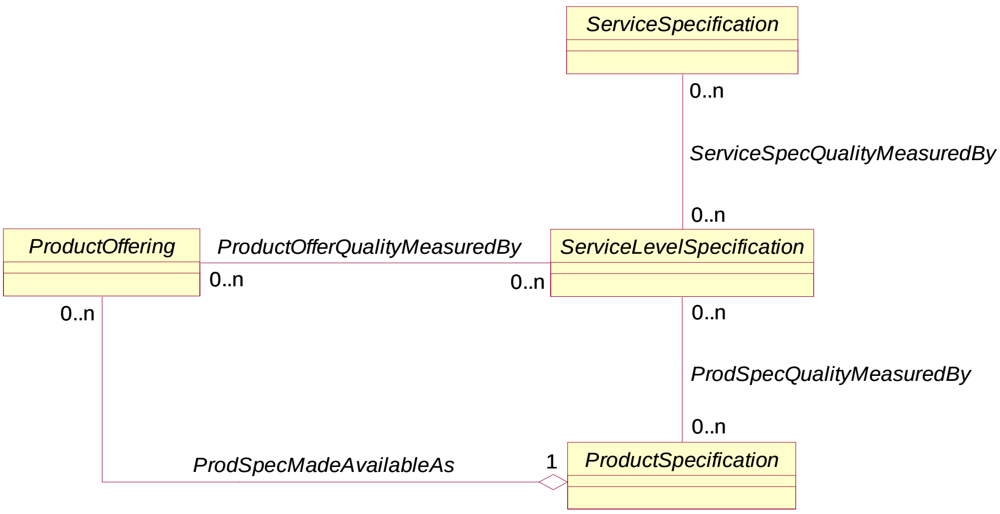


Figure 0-5: Associating Service Level Specifications with Products and Services [69]

Service level objectives are defined in terms of parameters and metrics, thresholds, and tolerances associated with the parameters. Figure 29 shows the Service Level Objectives with the Parameters that define them.

Service Level Specification parameters can be one of two types. A Key Quality Indicator (KQI) provides a measurement of a specific aspect of the performance of a Product (i.e., ProductSpecification, ProductOffering, or Product) or a Service (i.e., ServiceSpecification or Service). A KQI draws its data from a number of sources, including Key Performance Indicators (KPIs). A KPI provides a measurement of a specific aspect of the performance of a Service (whether it is a network or a non-network based Service) or a group of Services of the same type. A KPI is restricted to a specific Resource type.

In one of the next versions of the SID specification detailed relationships with all SLA-related entities and the Resource and Service entities will be added. The definition of the classes' attributes shown in Figure 29 is to be found in the Service Addendum of the SID specification [69].

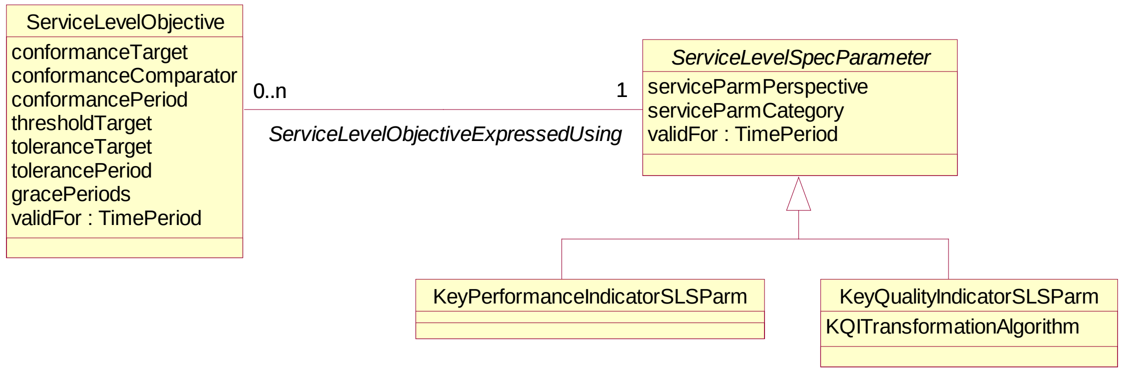


Figure 0-6: Service Level Specification Objectives and Parameters [69]

Violations to Service Level Agreements usually result in some consequences for the provider of the Service. The consequence could be a general one that applies to any objective violation, or the consequence could be associated with a specific objective. The figure below shows how consequences of violating a Service Level Agreement fit into the Service Level Specification model. The definition of the classes' attributes shown in Figure 30 is to be found in the Service Addendum of the SID specification [69].

In SID no attempt was made to build a detailed model that represents the prescribed actions. Rather, the shown model is intended to be an extensible framework that enables the adopters of the model to customize their extensions for this entity.

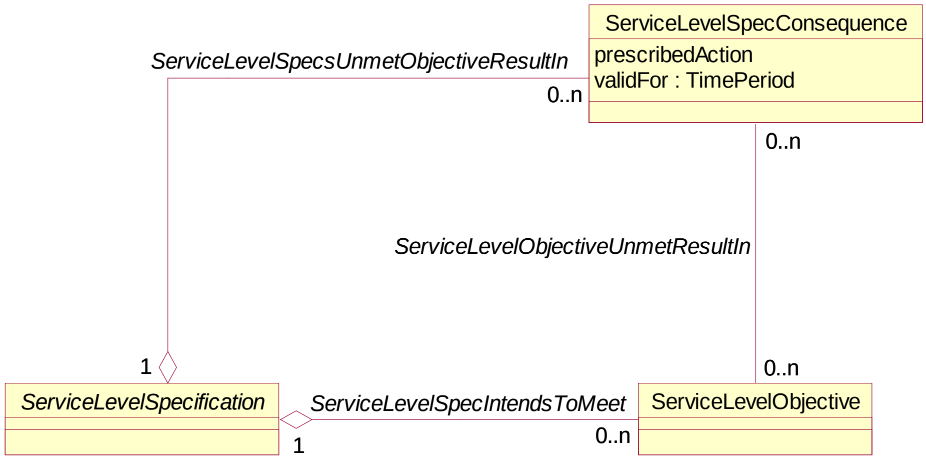


Figure 0-7: Service Level Specification Consequences [69]

The applicability of Service Level Specifications, Service Level Objectives, and Service Level Specification consequences may vary by day and/or time of day. For example, a Service Level Objective may be represented by one set of metrics during weekdays and by another set during weekends. This is handled by introducing a Service Level Specification Applicability entity as shown in Figure 31.

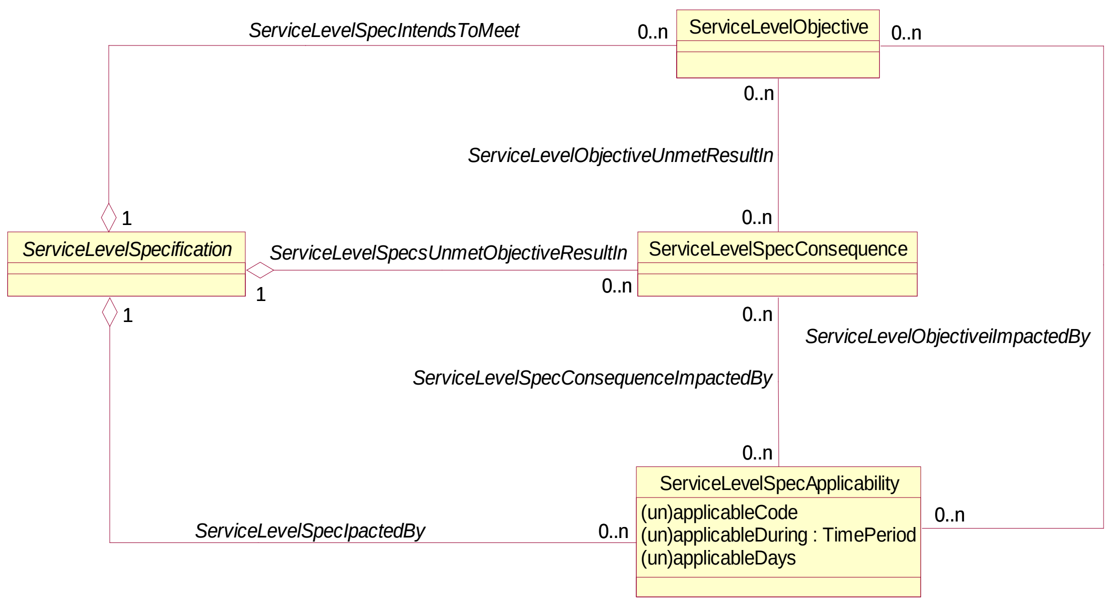


Figure 0-8: Service Level Specification Applicability [69]

A detailed definition of the SLA-related entities with their attributes and relationships is included in the SID Service Addendum (see [69]). The work on SLA modelling in SID is still in progress and will be extended in further versions of the SID model. A harmonization with SLA modelling activities in other organizations is in scope as well.

B: INFORMATION ON MERGING NGCOR PHASE 1 MATERIAL AND NGCOR PHASE 2 MATERIAL

8.9 Note 1:

8.10 Regarding Inventory Management interfacing descriptions from NGCOR phase 1

Note: During the first steps of NGCOR phase 1 project different high level Inventory Management interface descriptions were defined covering all layers; resource, service and product inventories. These descriptions are removed from the final NGCOR deliverable except those addressing product Inventory Management interfaces(which are nowincluded in chapter 2.3.3. Descriptions addressing resource and service inventory interfacing areconsidered being embedded into respective resource and Service Inventory Management requirements.

8.11 Note 2

8.12 Regarding high level Inventory Management requirements from NGCOR phase 1

Note: During the first steps of NGCOR phase 1 project the focus of NGCOR Inventory stream was to get a common view on Inventory Management area in broad sense; the main Inventory Management concepts, the main roles and characteristics of inventories within OSS/ BSS environment of operators, those requirements were called high level requirements in the NGCOR phase 1 deliverable. The **high level requirements were covering twolayers; resource and service inventories.** The high level requirements deal with functional, information/ operations modelling and interfacing aspects for Resource Inventory and Service Inventory. **Those high level requirements are now positioned in the respective parts of resource and service inventory requirements in chapter 5 of this deliverable. Some high level requirements from NGCOR phase 1 are enhanced in terms of content and description. Please note also that numbering of requirements – also those merged from NGCOR phase 1 is changed due to differernt document structure.**

8.13 Note 3

8.14 Removal of some detailed requirements of NGCOR phase 1 when merging to NGCOR phase 2 document

Some NGCOR phase 1 requirements derived from Resource Inventory Management use case were removed when merging NGCOR phase 2 document as duplicates or as content/substance wise meaning the same. Those were in NGCOR phase 1

- REQ-Inv (39), REQ-Inv (41), REQ-Inv (46), REQ-Inv (47), REQ-Inv (48), REQ-Inv (53)

Two NGCOR phase 1 requirements related to use cases Resource Inventory Management support for Configuration Management (in NGCOR phase 1 Resource Configuration) was removed when aligning content with Configuration Management stream of NGCOR phase 2. Those were in NGCOR phase 1

- REQ-Inv (51), REQ-Inv (55),

C: NGCOR INVENTORY MANAGEMENT REQUIREMENTS AND THEIR ADDRESSEES

8.14.1

The following table summarizes the requirements that have been elaborated and collected concerning Inventory Management by the NGCOR project and show the addressees of these requirements

InvM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-InvM (1)	X		X
REQ-InvM (2)	X		X
REQ-InvM (3)	X		X
REQ-InvM (4)	X		X
REQ-InvM (5)	X		X
REQ-InvM (6)	X		X
REQ-InvM (7)	X		X
REQ-InvM (8)	x		x
REQ-InvM (9)	X		X
REQ-InvM (10)	X		X
REQ-InvM (11)	X		X
REQ-InvM (12)	X		X
REQ-InvM (13)	X		X
REQ-InvM (14)	X		X
REQ-InvM (15)	X		X
REQ-InvM (16)	X		X
REQ-InvM (17)	X		X
REQ-InvM (18)	X		X
REQ-InvM (19)	X		X
REQ-InvM (20)			X
REQ-InvM (21)			X
REQ-InvM (22)			X
REQ-InvM (23)	X		X
REQ-InvM (24)	X		X
REQ-InvM (25)			X
REQ-InvM (26)	X		X
REQ-InvM (27)	X	X	X
REQ-InvM (28)	X		X
REQ-InvM (29)	X		X
REQ-InvM (30)			X
REQ-InvM (31)			X
REQ-InvM (32)	X	X	X
REQ-InvM (33)	X		X
REQ-InvM (34)	X	X	X
REQ-InvM (35)			X
REQ-InvM (36)			X
REQ-InvM (37)			X
REQ-InvM (38)			X
REQ-InvM (39)		X	X
REQ-InvM (40)			X
REQ-InvM (41)			X
REQ-InvM (42)			X

InvM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-InvM (43)			X
REQ-InvM (44)	X		X
REQ-InvM (45)	X		X
REQ-InvM (46)	X		X
REQ-InvM (47)	X		X
REQ-InvM (48)	X		X
REQ-InvM (49)	X	X	X
REQ-InvM (50)	X	X	X
REQ-InvM (51)	X	X	X
REQ-InvM (52)		X	X
REQ-InvM (53)	X		X
REQ-InvM (54)	X		X
REQ-InvM (55)	X		X
REQ-InvM (56)	X		X
REQ-InvM (57)	X		X
REQ-InvM (58)	X		X
REQ-InvM (59)	X		X
REQ-InvM (60)	X		X
REQ-InvM (61)	X		X
REQ-InvM (62)			X
REQ-InvM (63)			X
REQ-InvM (64)	X		X
REQ-InvM (65)	X		X
REQ-InvM (66)	X		X

NGCOR

Next Generation Converged Operations Requirements

Stream "Business Scenarios for Network Sharing"

by NGMN Alliance

Version: 1.1

Date: 2013-07-22

Version:	**1.1**
Date:	**2013-07-22**
Document Type:	**Draft**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**NGCOR**
Editor / Submitter:	**Jean-Michel Cornily, Orange**
Contributors:	**Tayeb Ben Meriem, Orange**
Approved by / Date:	**NGMN Board / 7th November 2013**

Abstract: Short introduction and purpose of document

This document contains all requirement identified by NGCOR Phase 2 project – Stream on Converged Operations.

Document History

Date	Version	Author	Changes
2012/12/17	V0.1	J-M. Cornily, Orange T. Ben Meriem, Orange	First draft
2013/01/15	V0.2	T. Ben Meriem, Orange	Remove the Umbrella part (section 1 and 2) Include Yvonne comments Describe requirements according to the template
2013/04/09	V0.3	J-M. Cornily, Orange	Take into account feedback from NGCOR partners
2013/04/10	V0.4	J-M. Cornily, Orange T. Ben Meriem, Orange	Include Tayeb's comments
2013/04/11	V0.5	J-M. Cornily, Orange T. Ben Meriem, Orange	Editorial enhancements
2013/06/06	V1.0	J-M. Cornily, Orange	Additional feedback from partners during the Torino meeting (May 6-8th)
2013/07/22	V1.1	Thomas Kulik, Deutsche Telekom AG	numeration of chapters, figures and tables changed

9 BUSINESS SCENARIOS FOR NETWORK SHARING (BSNS)

9.1 Multi-Operator RAN Sharing scenarios

9.1.1 Introduction

Many “RAN Sharing scenarios” exist either in the literature or in the field:

- Passive RAN sharing, also known as infrastructure sharing (including site sharing), is out of the scope of this document. Please refer to section 1.4.1 for a brief description of passive RAN Sharing;
- Active RAN sharing, where active elements of the RAN are shared, i.e. eNodeBs in an LTE network. This scenario is addressed in section 1.2;
- GWCN (Gateway Core Network), in which not only the radio access network elements are shared but, also, the core network elements. This scenario is addressed in section 1.3.

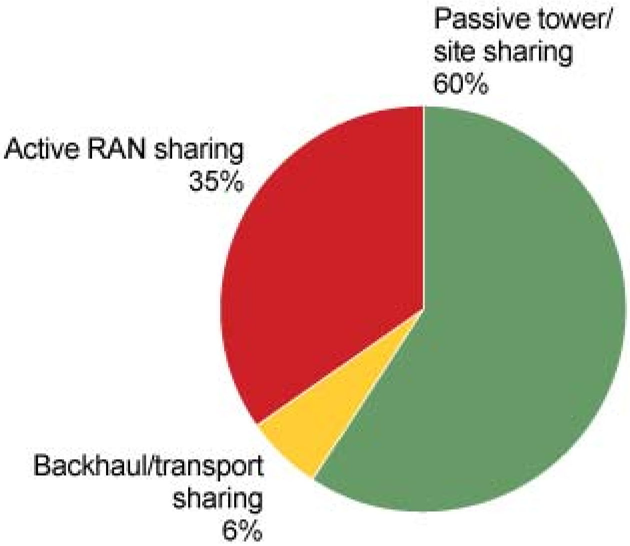


Figure 0-1: Types of network sharing[1]

- Also, national roaming is sometimes considered as a RAN sharing scenario. In the same spirit, to some extent, Mobile Virtual Network Operators (MVNO) could be also considered as a RAN sharing scenario. See section 1.4 for a short introduction to these scenarios. Both are out of the scope of this document.

9.1.2 Active RAN Sharing

9.1.2.1 Network architecture perspective

The two scenarios called MOCN (Multiple Operator Core Network) and MORAN (Multiple Operator Radio Access Network) are both active RAN sharing scenarios characterized by:

- Sharing Operators have a common (E-)UTRAN;

[1] Source: Informa Telecoms & Media – Dec. 2011

- Sharing Operators have their individual Core Network;
- Sharing Operators have their own PLMN code(s).

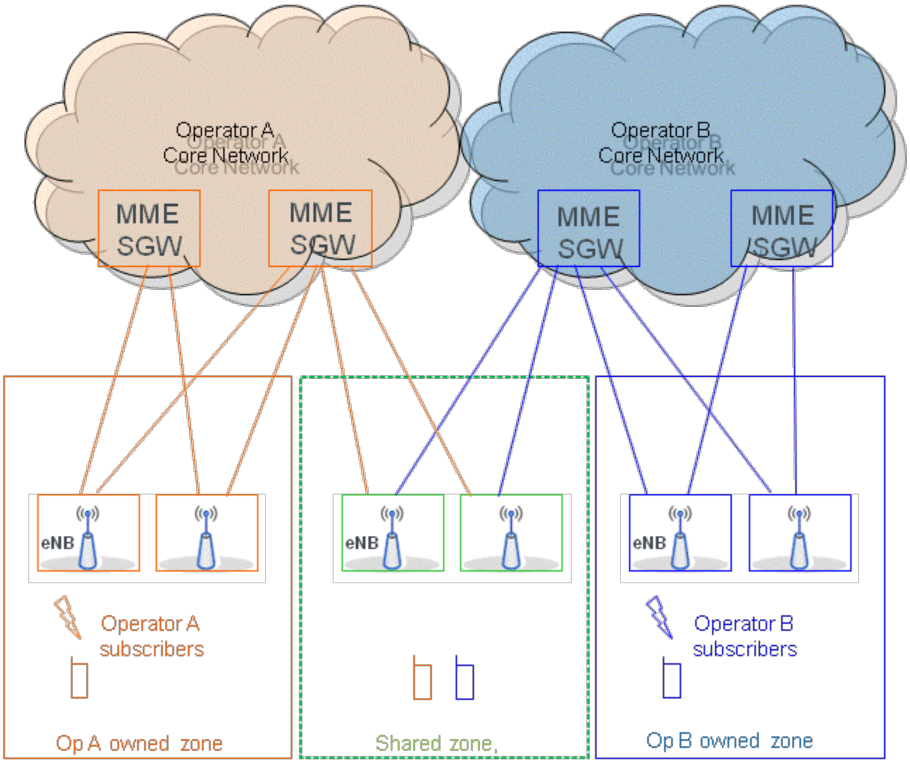


Figure 0-2: MOCN-MORAN for LTE - Commonalities

NB #1: as shown by Figure 2, in a given country, each mobile network operator can have its own RAN in addition to the RAN shared with other mobile network operators. For instance, each mobile network operator has its own RAN in dense urban areas and shares a common RAN in areas (e.g. rural areas) where it is not economically viable to deploy one eUTRAN per operator.

NB #2: A RAN Sharing agreement may exist between operators so as to build, operate and maintain a common network in one radio technology (e.g. LTE) whereas this RAN sharing agreement does not apply to other radio technologies (e.g. 2G / 3G).

9.1.2.1.1 Multiple Operator Core Network (MOCN)

MOCN (Multiple Operator Core Network) is a RAN Sharing scenario characterized by:

- Common features:
  - Sharing Operators have a common E-UTRAN
  - Sharing Operators have their individual Core Network
  - Sharing Operators have their own PLMN code
- MOCN-only feature: Sharing Operators use the same frequency on the shared eNodeBs (implying that the spectrum is pooled).

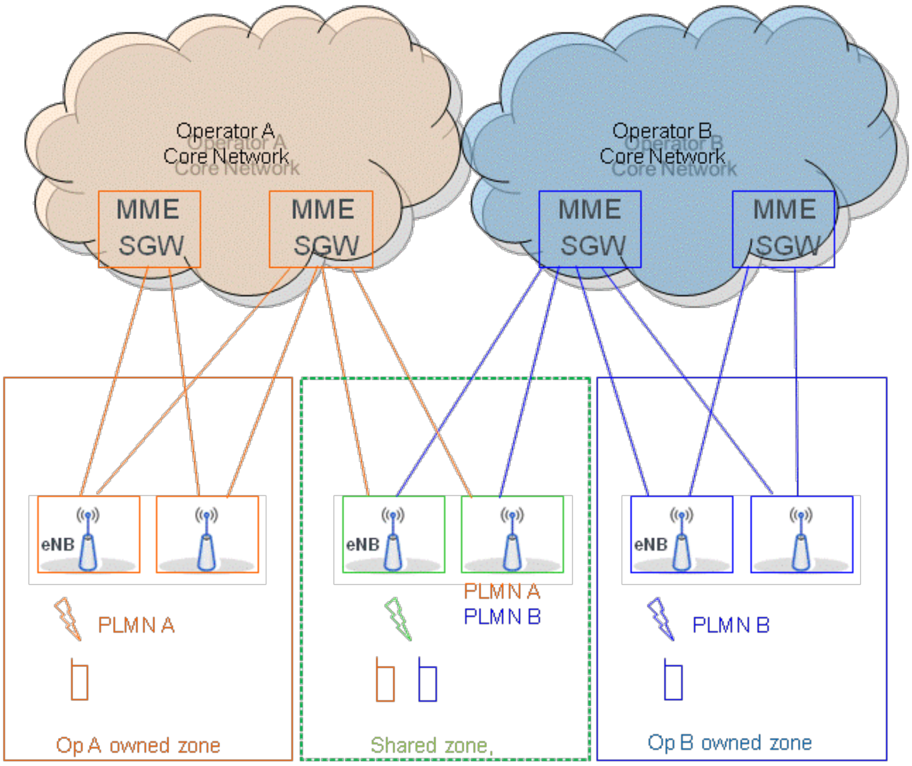


Figure 0-3: MOCN for LTE - Architecture

In a 3G network, the MOCN scenario can be depicted as follows:

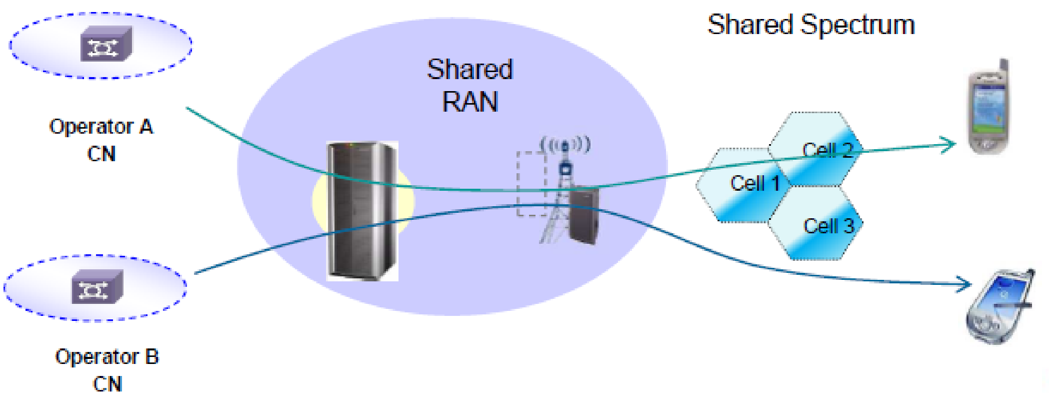


Figure 0-4: MOCN for 3G - Architecture

9.1.2.1.2 Multiple Operator Radio Access Network (MORAN)

The scenario called MORAN (Multiple Operator Radio Access Network) is a RAN sharing scenario characterized by:

35. Common features:
    - Sharing Operators have a common E-UTRAN.
    - Sharing Operators have their individual Core Network.
    - Sharing Operators have their own PLMN code.

36. MORAN-only feature: Sharing Operators have their own frequencies and cell settings on the shared eNodeBs (spectrum is assigned to each Operator).

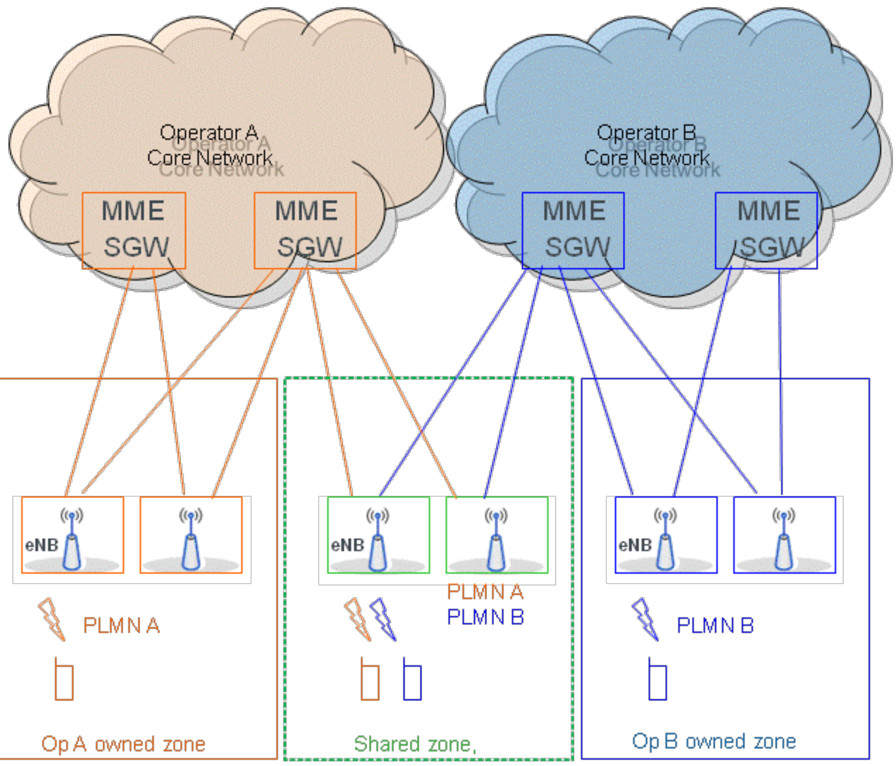


Figure 0-5: MORAN for LTE - Architecture

In a 3G network, the MORAN scenario can be depicted as follows:

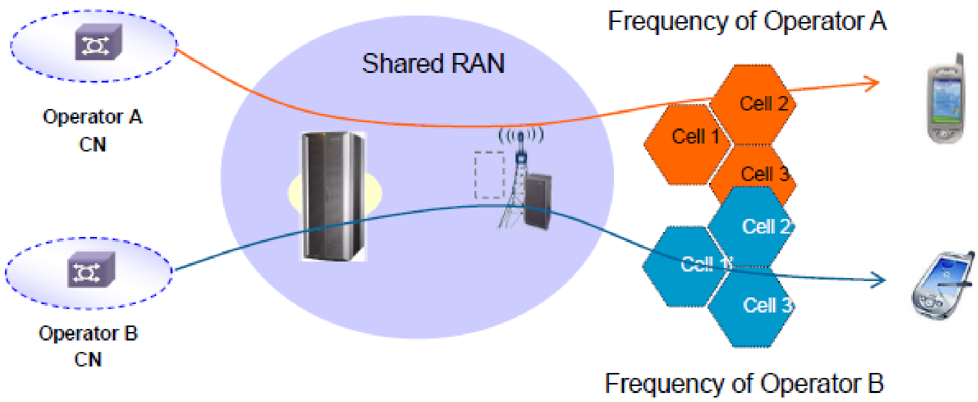


Figure 0-6: MORAN for 3G - Architecture

9.1.2.1.3 Transport network sharing

At each shared eNodeB, the following transport network layer configuration shall be ensured:

- The S1 interfaces between the shared eNodeB and each Sharing Operator's core network shall be secured;
- In order to separate the traffic between a shared eNodeB and each Sharing Operator's core network, VLANs shall be used;
- Each shared eNodeB is configured with one telecom VLAN to each Sharing Operator core network (signaling + user planes) + one single OA&M VLAN to the Master Operator Element Management System.

The responsibility for the configuration and assurance of the S1-MME and S1-U links is part of the RAN Sharing agreement clauses. In addition to sharing the Radio Access Network, there are scenarios where the mobile backhaul network can be shared as well. This is out of the scope of this document.

9.1.2.2 Network Management perspective

9.1.2.2.1 Roles

In a RAN Sharing deployment, two roles can be identified:

Role name	Description
Master Operator (MO)	The Master Operator (MO) is the owner of the shared network and is responsible for the management of his network. The Master Operator provides network and OA&M services to other Operators, called Sharing Operators. The Master Operator does not provide communication services to end users, i.e. does not have subscribers.
Sharing Operator (SO)	Sharing Operators (SO) are Mobile Communication Service Providers. In order to be able to offer their communication services, they use the Master Operator's network. Sharing Operators are clients of the Master Operator, in that they have a RAN Sharing contract with the Master Operator to be able to benefit from the Master Operator's network and operation services. Sharing Operators offer communication services to end users.

Figure 7 illustrates the responsibilities of Master Operator and Sharing Operators as well as interactions between them.

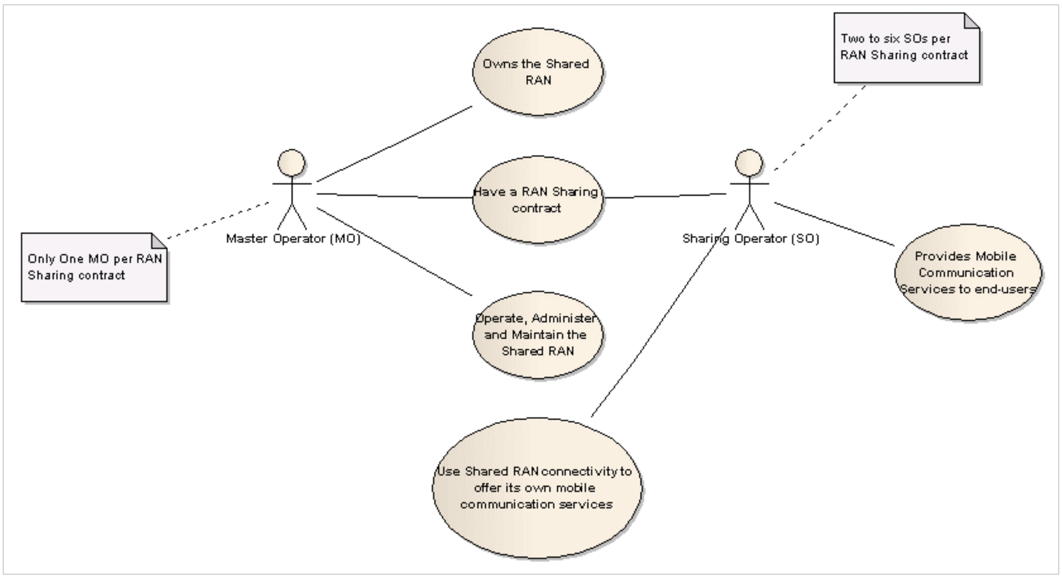


Figure 0-7: RAN Sharing – Roles and (inter)actions

Note #1: In a RAN Sharing contract where e. g. two Mobile Communication Service Providers share their network:

- Each Mobile Communication Service Provider plays a role of Sharing Operator;
- The role of Master Operator can be played by either:
    - One of the Sharing Operators (i. e. Mobile Communication Service Providers) – see for example http://www.telegeography.com/products/commsupdate/articles/2007/10/12/orange-and-vodafone-make-3g-network-sharing-pact/ , or
    - A Joint-Venture (JV) between the two Mobile Communication Service Providers – see for example http://www.rethink-wireless.com/2011/07/22/orange-tmo-merge-networks-poland.htm , or
    - A 3rd-party network Operator – see for example http://www.lightsquared.com/what-we-do/ .

Figure 8 shows that how these three operation models are divided up so far worldwide.

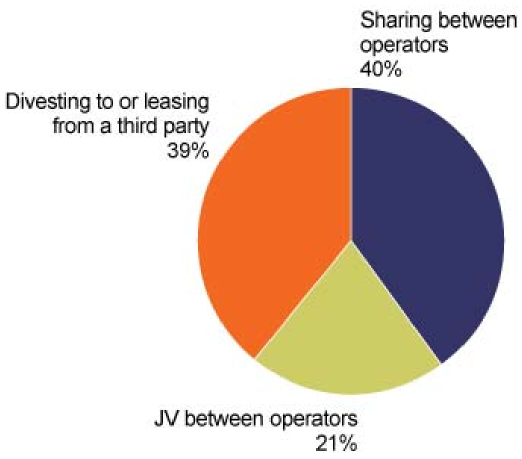


Figure 0-8: RAN Sharing – Repartition of operation models[2]

Note #2: Regardless of whom the Master Operator is (Operator A, Operator B, JV or 3rd-party player), the Master Operator can decide to outsource part or all of the activities related to the operation of the shared network. The outsourcing dimension does not challenge the principles described in the current document.

Note #3: Similarly, any Sharing Operator can decide to outsource a part or whole its network operation. In principle, this does not challenge what is mentioned in the current document.

9.1.2.2.2 Resources

In a shared RAN environment, the following systems will provide management capabilities:

Abbreviation	Title	Description
MO-SR-EMS	Master Operator – Shared RAN – Element Management System	The EMS enabling the Master Operator to manage the Shared RAN resources. It has direct OA&M links to the shared NEs. This EMS comes from the same supplier as the shared RAN.

[2] Source: Informa Telecoms & Media – Dec. 2011

MO-NMS	Master Operator – Network Management System	Network Management System belonging to the Master Operator, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Master Operator or supplied by Independent Software Vendors (ISV).
SO-EMS	Sharing Operator – Element Management System	An EMS enabling the Sharing Operator to manage its own RAN. It has direct OA&M links to its own NEs. This EMS comes from the same supplier as the Sharing Operator RAN.
SO-NMS	Sharing Operator – Network Management System	Network Management System belonging to the Sharing Operator, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Sharing Operator or supplied by Independent Software Vendors (ISV). A Fault Management SO-NMS of a Sharing Operator may collect alarm / event notifications issued by both the Shared RAN and the Sharing Operator-specific RAN (and potentially by other network elements of the Sharing Operator).
	Shared RAN	A Radio Access Network owned by a Master Operator and which provides radio access connectivity to multiple Sharing Operators. Depending on the scenario, part or whole of the resources of the Shared RAN are put in common between Sharing Operators.
	Shared RAN resources	The resources which constitute the shared RAN. Depending on the scenario, these resources can be either all shared between Sharing Operators (cf. MOCN) or a subset of them can be unshared (cf. MORAN). Shared RAN resources are blue coloured in Figure 9.
	Shared RAN shared resources	The part of Shared RAN resources that are common to all Sharing Operators.
	Shared RAN unshared resources	The part of Shared RAN resources that are dedicated to a Sharing Operator.
	Operator-specific RAN	The Radio Access Network of an Operator, out of any RAN Sharing contract. In a given country, Sharing Operators, in addition to getting RAN connectivity from a Master Operator, may have their own RAN, for their own usage.
	Operator-specific RAN resources	The resources which constitute the Operator-specific RAN. Operator-specific RAN resources are green coloured for resources belonging to Operator A RAN, respectively yellow coloured for resources belonging to Operator B RAN.

9.1.2.3 Management Architecture

Two main management architectures can be identified:

1. **Alternative #1**, in which the Master Operator offer management capabilities to Sharing Operators via its Shared RAN Element Management System;
2. **Alternative #2**, in which the Master Operator offer management capabilities to Sharing Operators via its Network Management System.

9.1.2.3.1 Management Architecture #1

According to this Management Architecture #1, the Master Operator Element Management System for the Shared RAN (MO-SR-EMS) is connected to Network Management Systems of all Sharing Operators (SO-NMS), as well as to its own NMS(s) (MO-NMS).

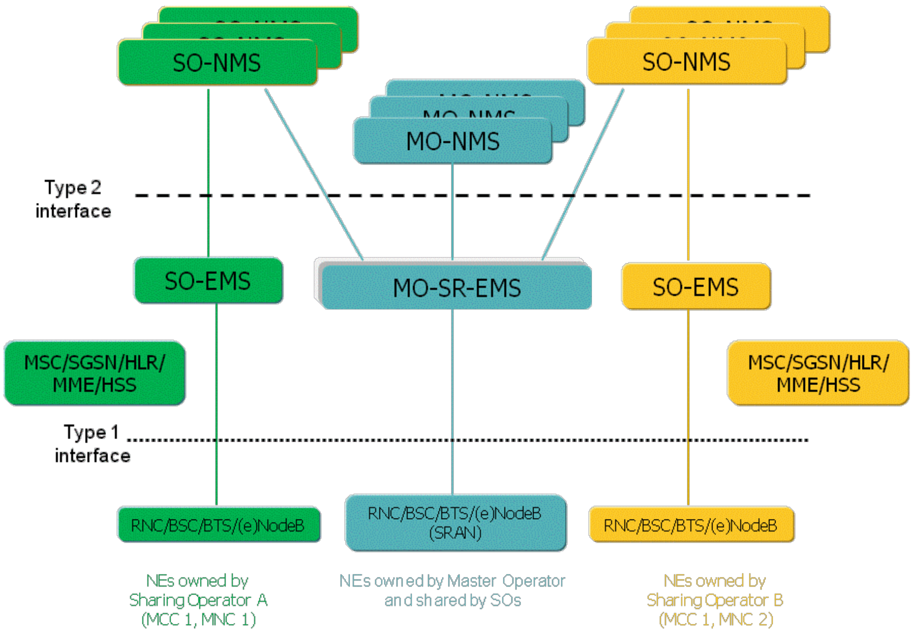


Figure 0-9: RAN Sharing – Management Architecture #1[3]

9.1.2.3.2 Management Architecture #2

According to this Management Architecture, the Master Operator Element Management System for the Shared RAN (MO-SR-EMS) is only connected to its own Network Management Systems (MO-NMS); the Master Operator Network Management System(s) for the Shared RAN (MO-NMS) is connected to Network Management Systems of all Sharing Operators (SO-NMS).

[3] It should be noted that, in all management architectures depicted in Section 1, the Service Management Layer applications are out of scope. Hence, interfaces from other management systems of other layers to these applications are not represented.

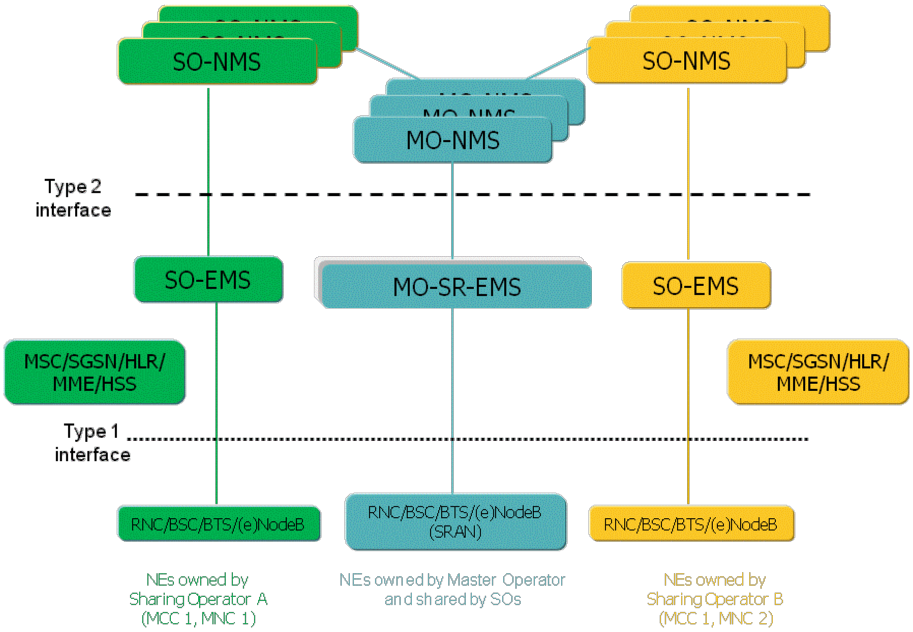


Figure 0-10: RAN Sharing – Management Architecture #2

NB: in Management Architectures #1 (cf. Figure 9) and #2 (cf. Figure 10), and according to definitions given in Section 1.2.2:

- Resources marked "RNC/BSC/BTS/(e)NodeB (SRAN)" in a blue rectangle correspond to "Shared RAN resources" of Section 1.2.2. This includes "Shared RAN shared resources" as well as "Shared RAN unshared resources" (if any);
- Resources marked "RNC/BSC/BTS/(e)NodeB" in a green rectangle correspond to "Operator-specific RAN resources" of Section 1.2.2, for Operator A;
- Resources marked "RNC/BSC/BTS/(e)NodeB" in a yellow rectangle correspond to "Operator-specific RAN resources" of Section 1.2.2, for Operator B.

9.1.2.4 Organisational Aspects

Figure 11 depicts Management Architecture #1 when the role of Master Operator is played by either a Joint-Venture or a 3rd-party network operator.

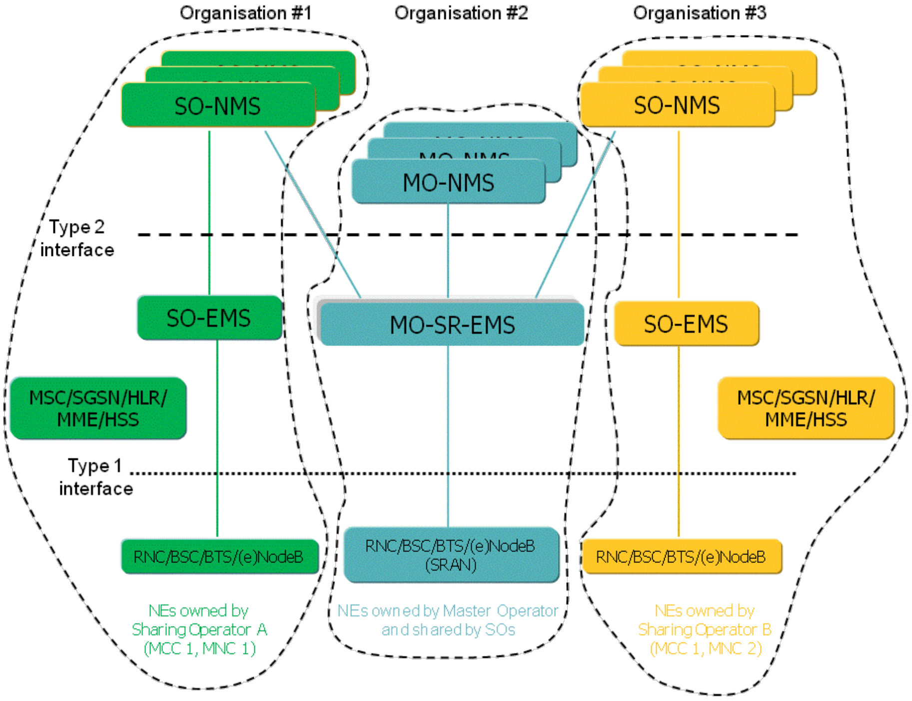


Figure 0-11: Management Architecture #1 in case of Joint-Venture or 3rd-party Operator

Figure 12 depicts Management Architecture #1 when the role of Master Operator is played by Operator A, who is simultaneously playing a role of Sharing Operator.

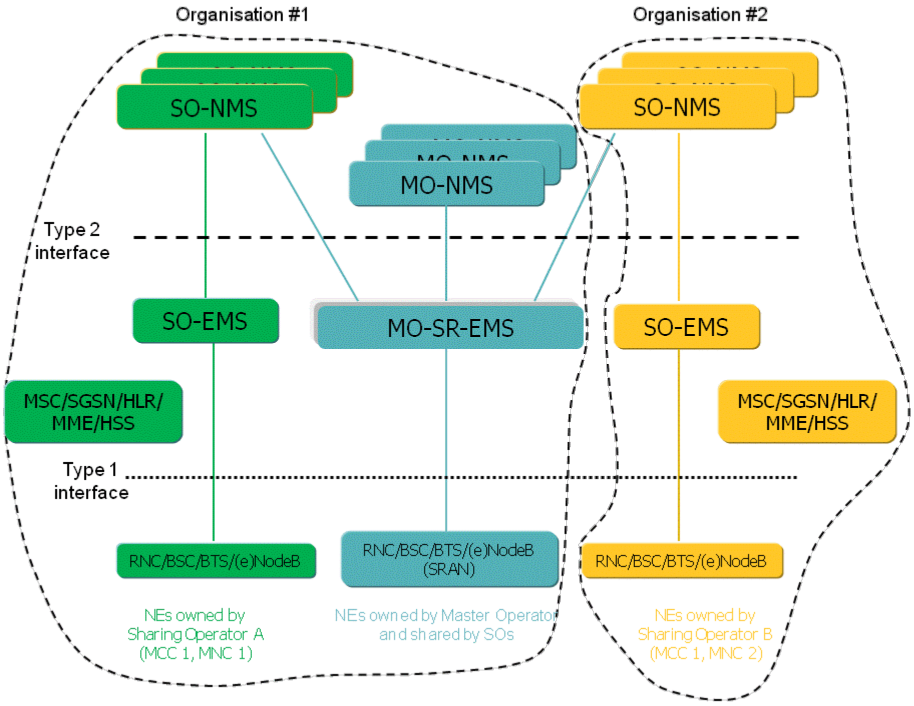


Figure 0-12: Management Architecture #1 in case of one Operator sharing his own network

Note: In the two scenarios above, there is an inter-organizational OA&M link between the MO-SR-EMS and the SO-NMSs of Sharing Operators. As of 3GPP Release 11, this is not covered by 3GPP Reference Management Architecture (cf. [9]).

Similarly, Figure 13 depicts Management Architecture #2 when the role of Master Operator is played by either a Joint-Venture or a 3rd-party network operator.

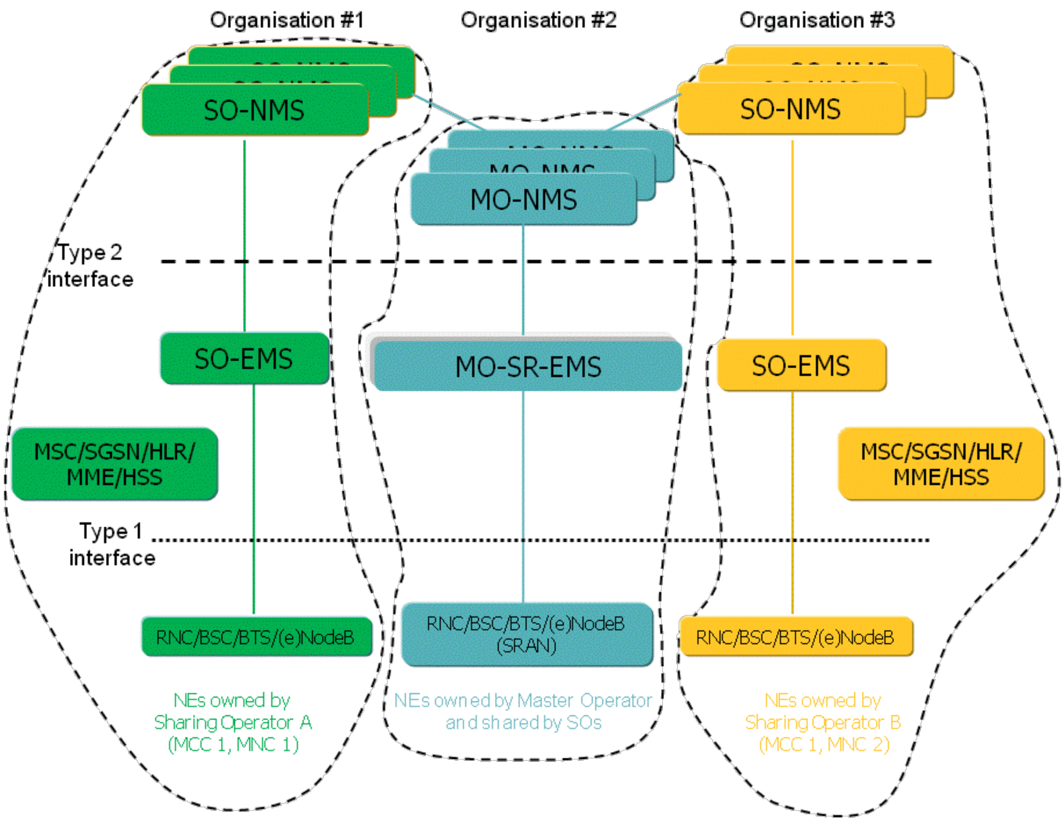


Figure 0-13: Management Architecture #2 in case of Joint-Venture or 3rd-party Operator

Figure 14 depicts Management Architecture #2 when the role of Master Operator is played by Operator A, who is simultaneously playing a role of Sharing Operator.

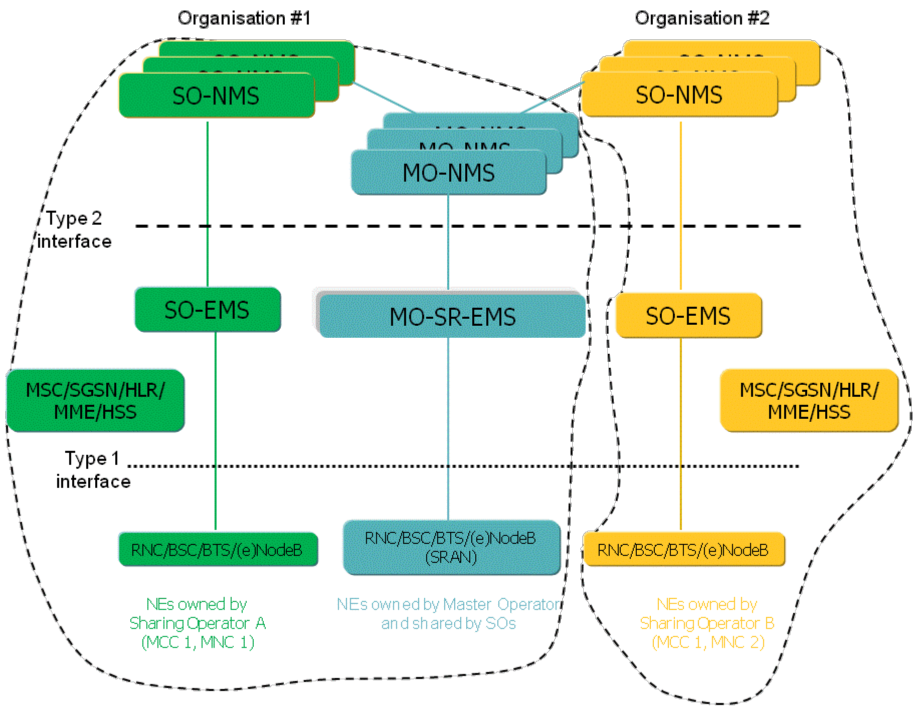


Figure 0-14: Management Architecture #2 in case of one Operator sharing his own network

9.1.2.5 Operational Requirements

In this section, we describe operators' requirements related to the operation of shared networks, labelled REQ-NS (i), "NS" standing for Network Sharing.

9.1.2.5.1 General Requirements

REQ-NS (1)

Identifier: REQ-NS (1)	**Rel. Use case id :** Management Architecture #1	**Priority: 1**
Title : Multiple MO-SR-EMS northbound interfaces to Sharing Operators		
Description: In case of Management Architecture #1, the MO-SR-EMS shall be able to support restricting the information provided or operations allowed via the northbound interface on a per Sharing Operator-basis, allowing each Sharing Operator to have its own view on the shared RAN resources.		
Rationale: Sharing Operators may each have different clauses in their RAN Sharing agreement with the Master Operator. Consequently, the interface between their respective SO-NMS(s) and the MO-SR-EMS may restrict information provided or operations allowed. Example: one Sharing Operator may be willing to be able to trigger his own performance jobs from its SO-NMS whereas another Sharing Operator may be not willing to.		

REQ-NS (2)

Identifier: REQ-NS (2)	**Rel. Use case id :** Management Architecture #2	**Priority: 1**

Title : Multiple MO-NMS east-west interfaces to Sharing Operators
Description: In case of Management Architecture #2, the MO-NMS shall be able to support restricting the information provided to SO-NMSs or operations allowed from SO-NMSs, allowing each Sharing Operator to have its own view on the shared RAN resources.
Rationale: Sharing Operators may each have different clauses in their RAN Sharing agreement with the Master Operator. Consequently, the interface between their respective SO-NMS(s) and the MO-NMS may restrict information provided or operations allowed. Example: one Sharing Operator may be willing to be able to trigger his own performance jobs from its SO-NMS whereas another Sharing Operator may be not willing to.

REQ-NS (3)

Identifier: REQ-NS (3)	**Rel. Use case id :** Management Architecture #1 & 2	**Priority: 1**
Title : Management interface – Generic Requirement		
Description: For Management Architecture #1 (respectively Management Architecture #2), the interface(s) between MO-SR-EMS (resp. MO-NMS) and SO-NMS(s) shall fulfil REQ-GEN(1) to REQ-GEN(22) from [2].		
Rationale:		

REQ-NS (4)

Identifier: REQ-NS (4)	**Rel. Use case id :** Management Architecture #1 & 2	**Priority: 1**
Title : Management interface based on Federated Network Information Model		
Description: For Management Architecture #1 (respectively Management Architecture #2), the interface(s) between MO-SR-EMS (resp. MO-NMS) and SO-NMS(s) shall be based on standardized interfaces (information model + protocol) according to 3GPP-TMF FNIM.		
Rationale:		

9.1.2.5.2 Requirements with regards to Fulfilment

9.1.2.5.2.1 ENodeB-level Resource Provisioning

In a shared RAN, the provisioning of all Shared RAN shared resources is under the responsibility of the Master Operator. In particular, (e)NodeB-level resource provisioning is done by the Master Operator, i.e. configuration of parameters related to shared (e)NodeBs, e. g.:

- (e)NodeB Id
- (e)NodeB Name
- Number of cells
- (e)NodeB Position (Latitude, Longitude)

- timeZone
- DHCP enabled / disabled
- VLAN definitions (IP address, VLAN priority) for OA&M
- Synchronisation Mode (e.g. GPS)
- Is CSFallback to other RAT Allowed?
- Etc.

And some SON (Self-Organizing Networks) related parameters, like:

- (e)NodeB Self-Configuration function switch on/off
- ANR switch on/off
- Automatic PCI Configuration switch on/off
- Energy Saving Management switch on/off
- Etc.

REQ-NS (5)

Identifier: REQ-NS (5)	**Rel. Use case id** : Fulfilment/Resource Provisioning	**Priority: 1**
Title : Configuration of Shared RAN shared resources		
Description: In a shared RAN, the configuration of shared resources is under the responsibility of the Master Operator. Sharing Operators have no management capabilities enabling them to configure those shared resources.		
Rationale:		

9.1.2.5.2.2 Cell-level Resource Provisioning

Depending on the RAN sharing scenario (MOCN, MORAN), either the Master Operator is responsible for the whole setting of common cell related parameters (in MOCN), or each Sharing Operator requests the Master Operator to set its operator-specific cell-level parameters (in MORAN). In case changes on some configuration parameter values are requested by a Sharing Operator, such requests are issued to the Master Operator who is then responsible for checking the technical feasibility of requested changes and applying them. Such configuration parameters include:

- Max number of Bearers per (e)NodeB, per cell, per Sharing Operator;
- Max number of UEs per (e)NodeB, per cell, per Sharing Operator.

REQ-NS (6)

Identifier: REQ-NS (6)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Configuration of Shared RAN unshared resources		
Description: In the shared RAN, the provisioning / configuration of Shared RAN unshared resources is under the entire responsibility of the owning Sharing Operator, i.e. Sharing Operators shall be allowed to provision / configure unshared resources. Consequently, the management interface between SO-NM and either MO-SR-EMS (in Management Architecture #1) or MO-NM (in Management Architecture #2) shall enable Sharing Operators to provision / configure their own resources in the shared RAN.		
Rationale: Each Sharing Operator shall be able to configure transport network layer resources, e.g. S1-MME and S1-U		

related configuration parameters for interconnecting shared eNodeBs to Operator-specific Core Network.

9.1.2.5.2.2.1 Multi-Operator Core Network – Multi-Operator Radio Access Network commonalities

Whatever the scenario which is deployed, examples of cell-level parameters to be provisioned within an (e)NodeB include:

- Cell Identity (relatively to (e)NodeB)
- Cell unique name
- Physical layer cell identity
- Cell position (latitude, longitude)
- Azimut
- Cell radius
- Cell size
- Downlink bandwidth
- Uplink bandwidth
- Etc.

9.1.2.5.2.2.2 Multi-Operator Core Network specificities

Because in MOCN, cells are shared between operators, a particular attention shall be put on the following aspects:

- Radio resource sharing policy configuration - In MOCN, the admission to shared radio resources must be controlled. The TRX Sharing policy has to be agreed between Sharing Operators (this shall be part of their sharing agreement) and configured by the Master Operator via its EMS. Four options are generally supported, as depicted in Figure 15:
    1. Fully pooled: (e)Node B radio resources are fully pooled. Each Sharing Operator SO has no resource dedicated to him. Resources are assigned to a Sharing Operator upon request on a first come first served basis. The total of resources allocated to all Sharing Operators shall not exceed 100% of available resources.
    2. Fully split: (e)NodeB radio resources are split between Sharing Operators. Each Sharing Operator SO has $X_{[SO]}$ resource dedicated to him only. Even if they are not used, these resources can't be used by any other Sharing Operators. Sum $X_{[SO]}$ for all Sharing Operators should not exceed 100%. $X_{[SO]} = 0$ means that the concerned Sharing Operator doesn't have dedicated resources.
    3. Partial reservation: A part of (e)NodeB radio resources is pooled, whereas the remaining part is equally split amongst Sharing Operators.
    4. Unbalanced: a part of (e)NodeB radio resources is unequally split between Sharing Operators (possibly one Sharing Operator is assigned 0% of the resources). The rest of (e)NodeB radio resources is pooled.

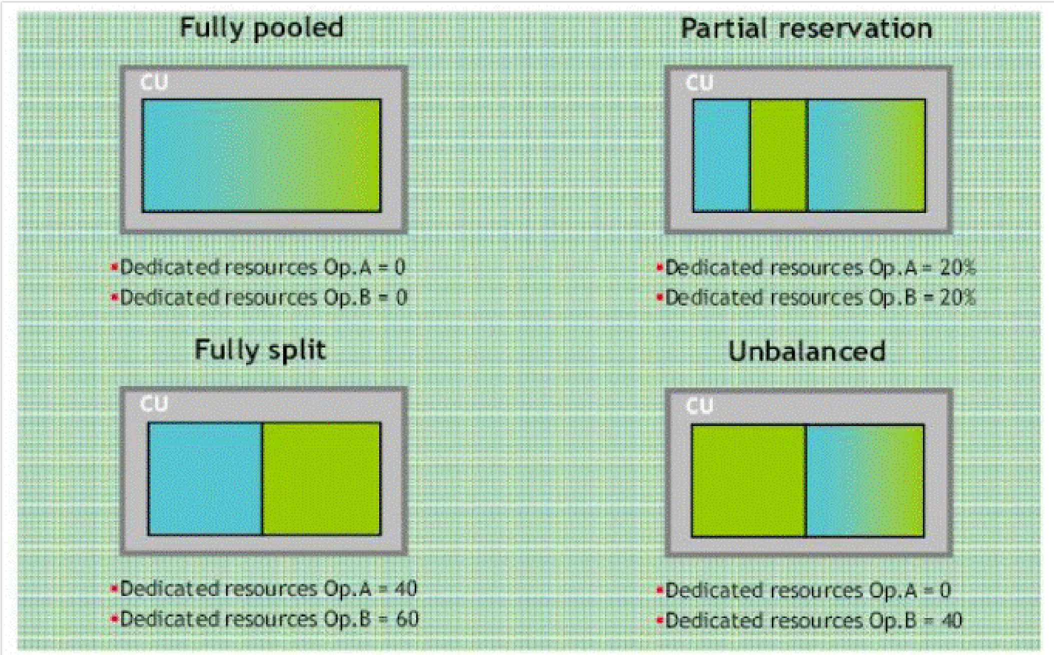


Figure 0-15: TRX sharing policy in MOCN

REQ-NS (7)

Identifier: REQ-NS (7)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Radio resource sharing policy		
Description: All settings related to radio resource sharing policy in MOCN are under the entire responsibility of the Master Operator.		
Rationale: Those settings will result from agreements between the Master Operator and the Sharing Operators, captured in the RAN Sharing contract.		

REQ-NS (8)

Identifier: REQ-NS (8)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Support of “Fully pooled” scenario		
Description: The Master Operator shall be able to configure (e)NodeB radio resources sharing according to the “Fully pooled” scenario.		
Rationale:		

REQ-NS (9)

Identifier: REQ-NS (9)	**Rel. Use case id** : Fulfilment/Resource Provisioning	**Priority: 1**

Title : Support of “Fully split” scenario
Description: The Master Operator shall be able to configure (e)NodeB radio resources sharing according to the “Fully split” scenario.
Rationale:

REQ-NS (10)

Identifier: REQ-NS (10)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Support of “Partial reservation” scenario		
Description: The Master Operator shall be able to configure (e)NodeB radio resources sharing according to the “Partial reservation” scenario.		
Rationale:		

REQ-NS (11)

Identifier: REQ-NS (11)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Support of “Unbalanced” scenario		
Description: The Master Operator shall be able to configure (e)NodeB radio resources sharing according to the “Unbalanced” scenario.		
Rationale:		

REQ-NS (12)

Identifier: REQ-NS (12)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Radio resource sharing granularity		
Description: The Master Operator shall be able to configure (e)NodeB radio resource sharing at a granularity of 1%.		
Rationale:		

REQ-NS (13)

Identifier: REQ-NS (13)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Sharing Operators view on radio resource sharing policy settings		
Description: In MOCN, it shall be possible that each Sharing Operator have its own view of its radio resources, whatever		

the radio resource sharing policy settings are (Fully Pooled, Fully Split, Partial reservation, Unbalanced). A Sharing Operator shall not have the view of other SO radio resources.
Rationale: Sharing Operators shall then be able to check that the Master Operator applies radio resource sharing policy, as defined in the RAN Sharing contract.

- Neighbour Relationship Table provisioning - In a shared (e)NodeB, the neighbour relationships between its shared cells and the neighbour cells in Operator-specific RAN (e)NodeBs (i.e. unshared (e)NodeBs) have to be managed cautiously, as well as handover policies. This is illustrated in Figure 16.

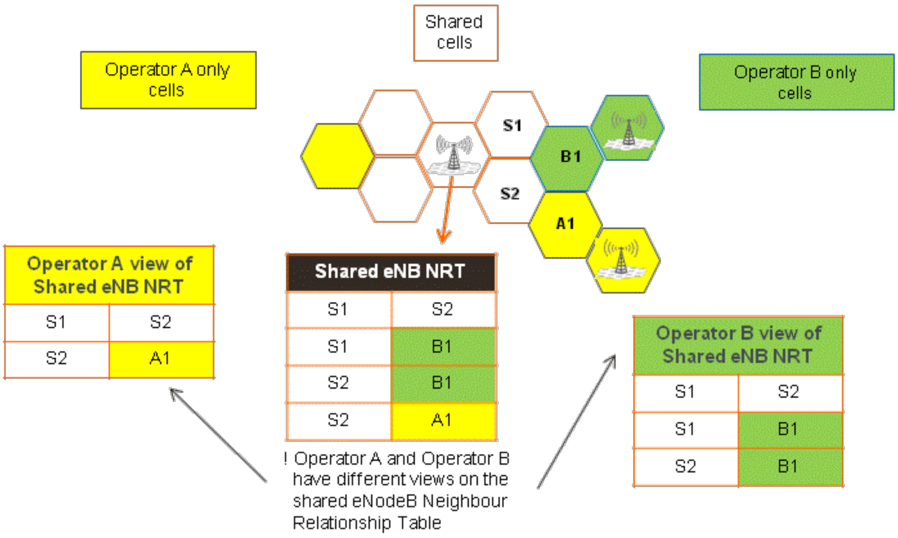


Figure 0-16: Neighbour Relation Table of a shared eNodeB in MOCN

This example shows that operator A and operator B have different views of neighbours of cells S1 and S2. By no way, operator A shall see B1 as a neighbour cell of S1 and S2. Similarly, operator B shall never see A1 as neighbour of S2. This happens only when RAN sharing is deployed.

REQ-NS (14)

Identifier: REQ-NS (14)	**Rel. Use case id :** Fulfilment/Resource Provisioning	**Priority: 1**
Title : Sharing Operators partial view on shared eNodeB NRT		
Description: In MOCN, it shall be possible that each Sharing Operator have its own view of neighbour relationships between cells of the Shared RAN and Operator-specific RAN.		
Rationale: Sharing Operators shall then be able to check that the Master Operator applies radio resource sharing policy, as defined in the RAN Sharing contract.		

REQ-NS (15)

Identifier: REQ-NS (15)	Rel. Use case id : Fulfilment/Resource Provisioning	Priority: 1
Title : X2 links between shared eNodeBs and Operator-specific eNodeBs		
Description: It shall be possible that each Sharing Operator configure separately parameters such as X2 blacklist, X2 white list, X2 handover black list, for shared (e)NodeBs which are located at the border between the shared RAN and Operator-specific RANs.		
Rationale: It's up to each Sharing Operator to agree with the Master Operator whether X2 connection requests are allowed between shared eNodeBs and eNodeBs belonging to the Sharing Operator. The same applies for setting whether X2 handover between those eNodeBs is allowed.		

REQ-NS (15)

Identifier: Req-NS (15a)	Rel. Use case id : Fulfilment/Resource Provisioning	Priority: 1
Title : Delegation		
Description: It shall be possible that any Sharing Operator provides Master Operator with delegation with respect to Shared RAN resources configuration capabilities.		
Rationale: A Sharing Operator may prefer to rely on the Master Operator for Shared RAN configuration purposes. In such a case, the Sharing Operator must provide the Master Operator with all configuration data needed. The Master Operator is then responsible to apply configuration changes on the Shared RAN on behalf of the Sharing Operator.		

9.1.2.5.2.3 Resource Inventory Management

In a shared radio access network, as mentioned earlier (cf. Sections 1.2.1.1 and 1.2.1.2), managed resources can be shared or unshared (i.e. dedicated per Sharing Operator). Consequently, in OA&M system(s)[4]:

- Shared RAN resources have to be marked as either Shared or Unshared;
- For unshared resources, the resource owner (Operator) must be identified, e.g. via its PLMN Id (Mobile Network Code);

This applies to (e)NodeBs and cells (and possibly transport network resources – out of scope of the current version of this document).

REQ-NS (16)

Identifier: REQ-NS (16)	Rel. Use case id : Fulfilment/Resource Inventory	Priority: 1
Title : Differentiating Shared RAN shared resources from unshared resources		
Description: Since, in a shared RAN, some managed resources can be shared while others are dedicated per Operator,		

[4] Within the Master Operator EMS and some OSS applications of Sharing Operators (e.g. Inventory Management applications).

	the following information shall be visible over the management interface between the MO-SR-EMS (in Management Architecture #1) / MO-NMS (in Management Architecture #2) and SO-NMS(s): a/ managed resources shall be marked as either Shared or Unshared, and b/ for unshared resources, the resource owner (Operator) must be uniquely identified, e.g. via its PLMN Id (Mobile Network Code).
Rationale:	

9.1.2.5.3 Requirements with regards to Assurance

9.1.2.5.3.1 Alarm Management

The Master Operator is responsible for the maintenance of all the shared network elements. Alarms related to shared resources are under the responsibility of Master Operator:

1. Alarms issued by shared resources within (e)NodeBs shall be sent to the Master Operator EMS and displayed on its GUI;
2. The Master Operator is responsible for acknowledging / clearing the alarms, and triggering repair actions;
3. The Master Operator shall have all rights to control / manage resources;
4. Depending on the RAN Sharing contract agreement, alarm notifications may be sent by the Master Operator EMS to Sharing Operators NMS for INFORMATION only.

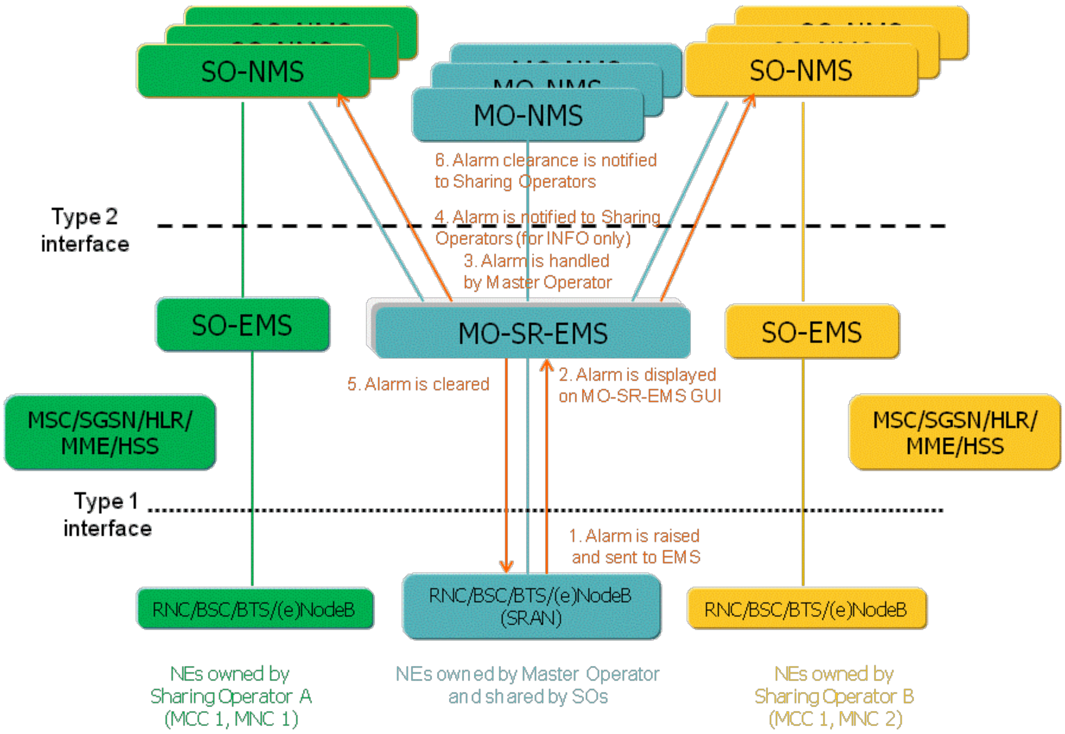


Figure 0-17: Example of alarm handling in RAN Sharing (Alarm occurring on a Shared RAN shared resource)

REQ-NS (17)

Identifier: REQ-NS (17)	**Rel. Use case id :** Assurance/Alarm	**Priority: 1**

Title : Handling of alarms related to Shared RAN shared resources		
Description: Depending on RAN Sharing contract clauses, Sharing Operators may be willing to stay informed of events / alarms occurring on the Shared RAN shared resources, despite they do not own these resources. It shall be possible for Sharing Operators to distinctively subscribe event / alarm notifications occurring on Shared RAN shared resources.		
Rationale:		

Depending on the RAN Sharing contract agreement, alarms related to Shared RAN unshared resources can be under the responsibility of the Sharing Operator which owns the resource (cf. item No. 3 below) or not (cf. item No. 2 below):

1. Alarms issued by shared (e)NodeBs shall be sent to the Master Operator EMS (MO-SR-EMS) and displayed on its GUI. Depending on the agreements passed between the Master Operator and the Sharing Operators, either:
2. Alarm is handled by Master Operator (See Figure 17):
    a. The Master Operator is responsible for acknowledging/ clearing the alarm, and triggering repair actions;
    b. The Master Operator shall have all rights to control / manage resources;
    c. The alarm notification may be sent by the Master Operator EMS to the Sharing Operator (which owns the resource) NMS for INFORMATION only;
3. Or Alarm is handled by owning Sharing Operator (See Figure 18):
    a. The Master Operator is NOT responsible for acknowledging / clearing the alarm, and triggering repair actions. Instead:
    b. The alarm notification is sent by the Master Operator EMS to the Sharing Operator (which owns the resource – example: Operator B in Figure 18) NMS for ACTION;
    c. The Sharing Operator shall have all rights to control / manage its resources;
    d. The Sharing Operator takes appropriate repair action and then clear the alarm, when relevant, from its OSS application;
    e. The Master Operator EMS is informed of the clearing of the alarm.

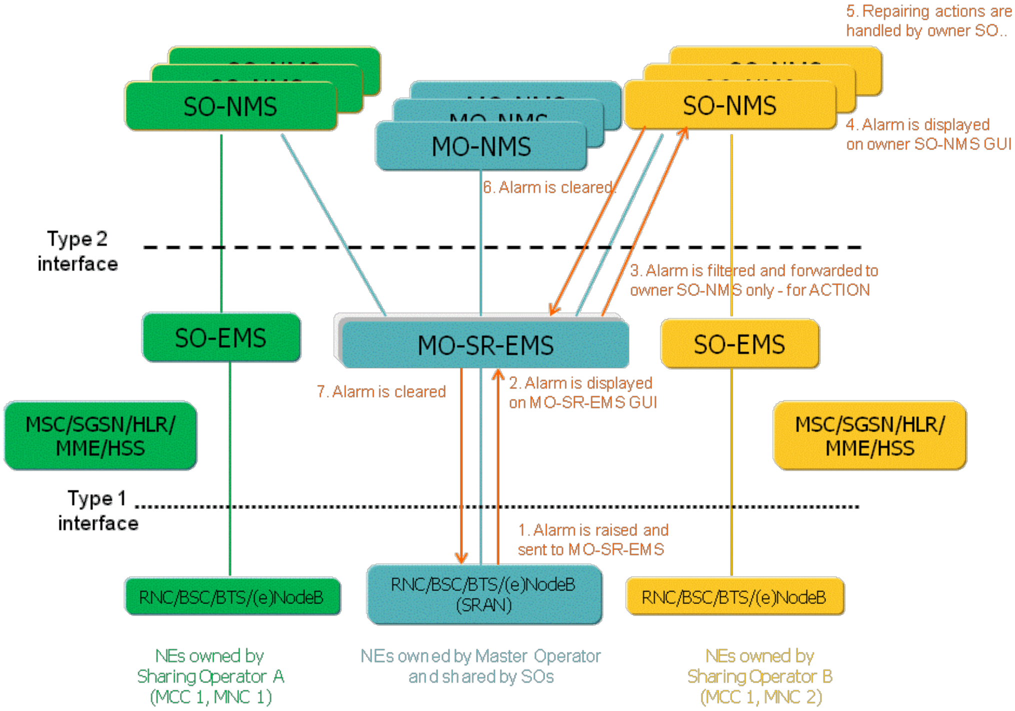


Figure 0-18: Example of alarm handling in RAN Sharing (Alarm occurring on a Shared RAN unshared resource)

Whoever is responsible for handling alarms, he shall have all necessary information about (e)NodeBs, including site information, equipment-level information, cell parameters, topology information, etc. so as to be able to enrich, correlate, filter, etc. alarms.

9.1.2.5.3.2 Performance Management

Master Operator and Sharing Operators, in their RAN Sharing contract, agree on SLAs defined in terms of KPIs and, for each KPI, threshold values above / below which the network service is not correctly provided by the Master Operator to Sharing Operators. The Master Operator generally commits to provide all Sharing Operators, at a given and commonly agreed periodicity (e. g. monthly), with a list of valued Key Performance Indicators for informing Sharing Operators about the:

- Availability of services supported by the shared RAN.
- Quality of service measured on shared cells and/or unshared cells (if any).
- Radio resource usage rate.
- Volume of data carried by the shared and unshared cells (if any).

Example of indicators (non-exhaustive list):

Indicator	Applicability
Call setup success rate	Voice, Data
Link Failure Rate	Voice, Data
Average Bandwidth per User	Data
Radio resource usage rate per Sharing Operator	Voice, Data
Volume of data per Sharing Operator	Data

9.1.2.5.3.3 Trace/ MDT Management

Under Trace Management, we include the following:

1. Location-based Trace, consisting in tracing the traffic on a cell, a group of cells, a tracking area, etc.
2. Equipment Trace, consisting in tracing the traffic on some interfaces of an equipment such as the S1-MME interface of a given eNodeB;
3. Subscriber Trace (based on IMSI or IMEI), consisting in tracing the traffic related to a given subscriber;
4. Minimization of Drive Tests (MDT)

REQ-NS (18)

Identifier: REQ-NS (18)	**Rel. Use case id :** Assurance / Performance (Trace/MDT)	**Priority: 1**
Title : Secure file transfer to TCE		
Description: When triggering the trace / MDT job, the IP address of the Trace Collection Entity shall be indicated by the NMS application which initiates the job (MO-NMS or SO-NMS) so that all network elements involved in the Trace job can collect trace information and send them to this Trace Collection Entity, via secured file transfer mechanisms. Special attention shall be put on inter-organizational domain file transfer, e.g. from shared (e)NodeBs / MO-SR-EMS to Sharing Operators' Trace Collection Entities.		
Rationale:		

9.1.2.5.3.3.1 Signalling Based Activation

REQ-NS (19)

Identifier: REQ-NS (19)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Signalling Based Activation by Sharing Operators on their subscribers / UEs		
Description: In MOCN and MORAN, Signalling Based Activation can only be triggered by Sharing Operators, to collect measurements from UEs of their subscribers only (including subscribers of a MVNO supported by the Sharing Operator and subscribers of an Operator having a roaming agreement with the Sharing Operator). Each Sharing Operator shall be able to activate signalling based trace / MDT from its Core Network OSS applications to its Core Network elements (e.g. HSS, SGSN or MME), by providing selected subscriber / UE identifier(s).		
Rationale: The Master Operator (as a role) has no subscribers. Only Sharing Operators have subscribers. Only Sharing Operators have knowledge of their subscribers' Ids as well as of their subscribers' UE Ids.		

REQ-NS (20)

Identifier: REQ-NS (20)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Signalling Based Activation by Master Operator on Sharing Operators' subscribers / UEs		

Description: In MOCN and MORAN, the Master Operator is not allowed to activate any signalling based trace/ MDT on Sharing Operators' subscribers / UEs. In GWCN, depending on the RAN Sharing agreement, clauses, the Master Operator may be allowed to activate signalling based trace / MDT from its shared Core Network OSS applications, by providing selected Sharing Operators' subscriber / UE identifier(s).		
Rationale:		

Identifier: Req-NS (20a)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Signalling Based Activation by a Sharing Operator on other Sharing Operators' subscribers/ UEs		
Description: A Sharing Operator is not allowed to activate any signalling based trace / MDT on other Sharing Operators' subscribers / UEs.		
Rationale:		

REQ-NS (21)

Identifier: REQ-NS (21)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Signalling Based Activation from OSS applications		
Description: How Signalling Based Activation is triggered from Core Network OSS applications down to the Core Network elements (e.g. HSS or SGSN / MME), by providing selected subscriber/ UE identifier(s), shall be standardized.		
Rationale: In case of signalling based activation on the HSS, it shall be standardized how this is achieved. If this is achieved via the EMS of the Sharing Operator HSS, how this can be done through this EMS Itf-N shall be standardized. If this is achieved via the HSS provisioning interface (from some OSS application), it shall be standardized, based on the Common Baseline Information Model. In case of signalling based activation on the MME via the EMS of the Sharing Operator MME, how this can be done through this EMS Itf-N shall be standardized.		

REQ-NS (22)

Identifier: REQ-NS (22)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Signalling Based Trace of users moving to shared RAN		
Description: When a subscriber / UE, selected for signalling based trace/ MDT, is located in the Shared RAN or moves from a Operator-specific RAN to the Shared RAN, whether the Sharing Operator Core Network shall propagate the trace / MDT to Shared RAN NEs shall be mentioned in the RAN Sharing agreement. Consequently, it shall be possible to configure this feature in a standardized way from Sharing Operators OSS applications on their Core Network elements (HSS / SGSN / MME).		

Rationale:

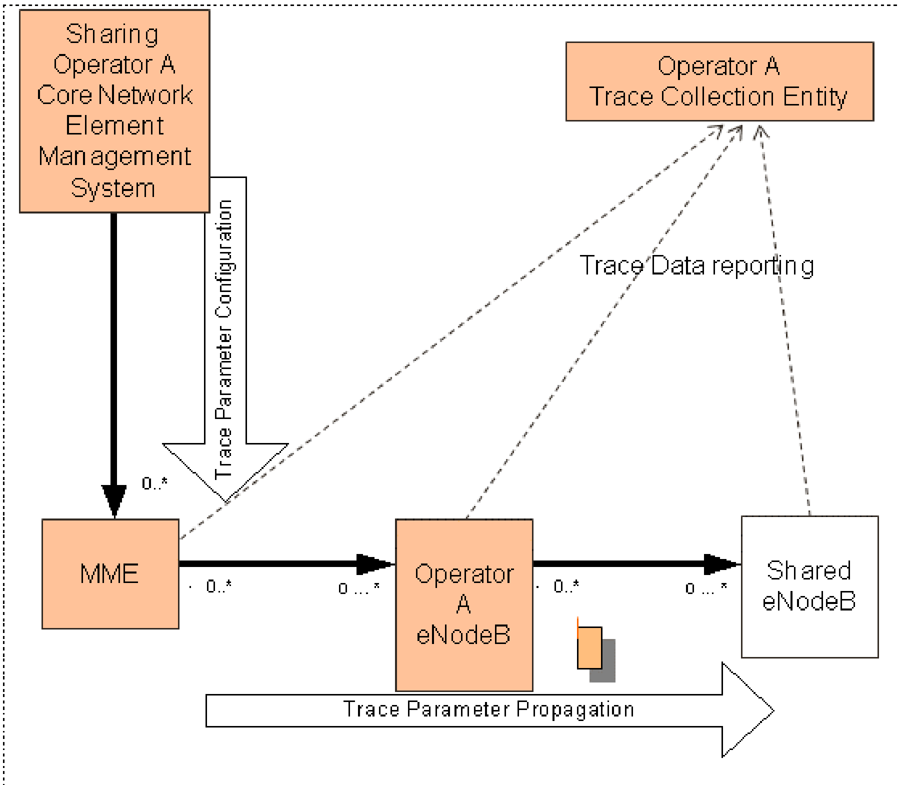


Figure 0-19: Tracing a subscriber in a shared E-UTRAN

9.1.2.5.3.3.2 Management Based Activation

REQ-NS (23)

Identifier: REQ-NS (23)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Management Based Activation rights		
Description: In principle, Management Based Activation of trace / MDT on Shared RAN NEs can only be triggered via the Master Operator Shared RAN EMS. However, whether it can be triggered from the Master Operator NM only or from a Sharing Operator NM as well shall be mentioned in the RAN Sharing agreement. Consequently, the Master Operator Shared RAN EMS shall be able to handle management based activation requests of trace / MDT from Sharing Operators NM applications.		
Rationale:		

REQ-NS (24)

Identifier: REQ-NS (24)	Rel. Use case id : Assurance / Performance (Trace /MDT)	Priority: 1
Title : Arbitration in case of multiple simultaneous trace job requests		
Description: In case of simultaneous management based activations of trace/ MDT from Sharing Operators, the Master Operator is allowed to reject or postpone any request, based on e.g. expected high load in NEs, etc. In such a case, the requesting Sharing Operator NMS shall be informed by the Master Operator MO-SR-EMS/ MO-NMS.		
Rationale:		

REQ-NS (25)

Identifier: REQ-NS (25)	Rel. Use case id : Assurance / Performance (Trace /MDT)	Priority: 1
Title : Arbitration based on RAN sharing agreement		
Description: In MOCN, since conflicts may occur between simultaneous management based activations of trace / MDT from Sharing Operators on shared cells, the Master Operator is allowed to reject / postpone any request. In such a case, the requesting Sharing Operator shall be informed by the Master Operator MO-SR-EMS/ MO-NMS.		
Rationale:		

REQ-NS (26)

Identifier: REQ-NS (26)	Rel. Use case id : Assurance / Performance (Trace /MDT)	Priority: 1
Title : Triggering allowed from owning Operator only		
Description: In principle, in MORAN, management based activation of trace / MDT on a cell / group of cells shall be possible from the NMS of the Sharing Operator which owns the cell / group of cells only. Depending on the RAN Sharing agreement, it may be possible for the Master Operator as well to do so from its MO-NMS.		
Rationale:		

REQ-NS (27)

Identifier: REQ-NS (27)	Rel. Use case id : Assurance / Performance (Trace /MDT)	Priority: 1
Title : Area-based trace/ MDT on Sharing Operator subscribers / UEs		
Description: In MOCN, in case of management based activation of trace / MDT by a Sharing Operator on a number of cells, it shall be possible for a Sharing Operator to select its own subscribers / UEs for participation to the trace / MDT.		
Rationale:		

REQ-NS (28)

Identifier: REQ-NS (28)	**Rel. Use case id :** Assurance / Performance (Trace /MDT)	**Priority: 1**
Title : Management Based Activation by Sharing Operators on other subscribers / UEs		
Description: In case of management based activation of trace / MDT by a Sharing Operator on a number of cells, it shall be possible for the Sharing Operator to collect measurements from subscribers / UEs of other Sharing Operators, depending on 1/ RAN Sharing agreement (between Sharing Operators) clauses and 2/ concerned users' consent.		
Rationale:		

9.1.2.5.3.4 Self-Organizing Networks

The activation of SON functions shall be done cautiously in a shared E-UTRAN, especially in cases where both the Master Operator and Sharing Operators activate some SON functions in their respective network. For eNodeBs/ cells at the border between the shared RAN and the Sharing Operators dedicated networks, some undesirable effects known as "ping-pong" effects shall be avoided when e.g. a SON function running in the Master Operator RAN change some configuration parameters of a shared eNodeB / cell whereas, more or less simultaneously, either the same or another SON function running in a Sharing Operator RAN changes some configuration parameters of a neighbor eNodeB / cell. Knowing that modifying configuration parameters of an eNodeB / cell may have side effect on neighbor eNodeBs / cells, this could never converge, i.e. come to a steady state in reasonable time duration.

Conflicts shall be detected between:

- Any given SON function deployed in the shared RAN and in Sharing Operators' networks, e.g. between the *Automatic PCI Configuration* function deployed in the shared RAN and the *Automatic PCI Configuration* function deployed in the Sharing Operators' RANs;
- Two different SON functions deployed in the shared RAN and in Sharing Operators' networks, e.g. between the *Mobility Load Balancing* function deployed in the shared RAN and the *Handover Optimisation* function deployed in the Sharing Operators' RANs.

For all SON functions that are deployed using a distributed architecture (i. e. the SON function runs in the eNodeBs), they generally rely on the usage of either X2 (between neighbor eNodeBs) or S1 links (between eNodeBs and core network elements). The RAN sharing agreement shall stipulate whether the Master Operator and the Sharing Operators accept to have X2 links between their respective eNodeBs which are neighbor to each others.

REQ-NS (29)

Identifier: REQ-NS (29)	**Rel. Use case id :** Assurance / SON	**Priority: 1**
Title : Switch on / off SON functions on shared RAN		
Description: It shall be possible for the Master Operator to switch on/off any SON function on a cell/ group of cells of the Shared RAN. When switching a SON function off, the concerned cell / group of cells shall return to a		

	“nominal” state within a minimal duration, i.e. shall ensure coverage and capacity as initially planned (prior to the activation of the SON function).
Rationale:	

REQ-NS (30)

Identifier: REQ-NS (30)	**Rel. Use case id :** Assurance / SON	**Priority: 1**
Title : Self-Configuration of shared eNodeBs		
Description: The activation of the SON function “Self-Configuration of eNodeBs” in the Shared RAN shall be decided and handled by and only by the Master Operator.		
Rationale:		

9.1.3 Active RAN + Core Network Sharing (GWCN)

9.1.3.1 Network architecture perspective

GWCN (GateWay Core Network) is an architecture scenario in which not only the RAN network elements are shared between Sharing Operators but also some mobile core network elements. In the figure below, we show an example of GWCN where MMEs are shared and S-/P-GWs are not shared.

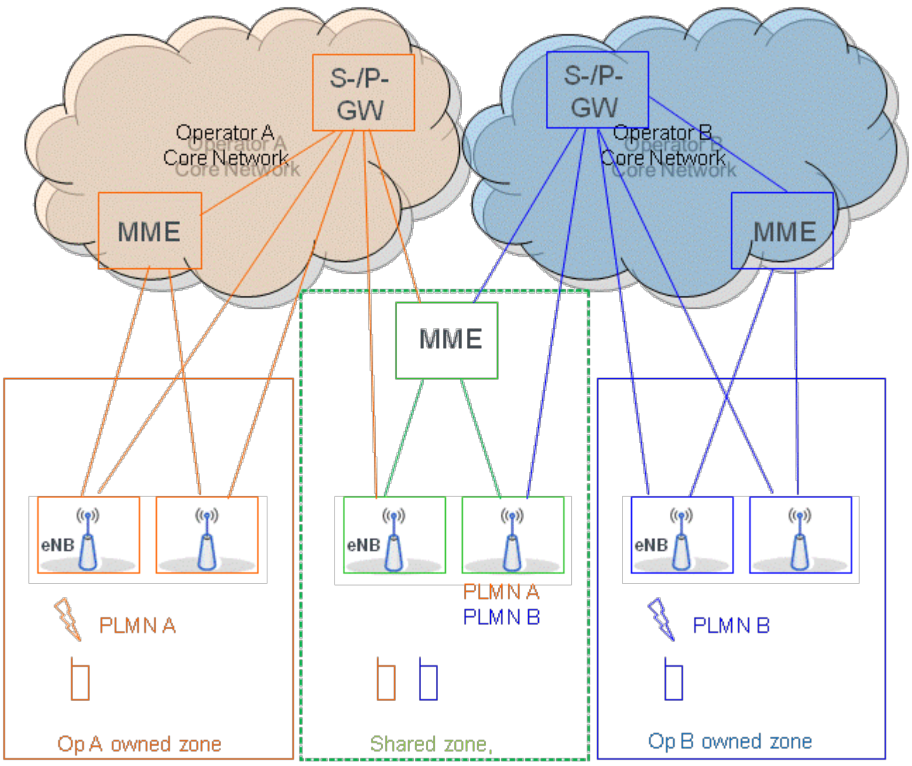


Figure 0-20: GWCN for LTE - Architecture

9.1.3.2 Management perspective

9.1.3.2.1 Roles

In GWCN, same roles as in active RAN Sharing exist, i.e. Master Operator and Sharing Operator. There is no additional role.

9.1.3.2.2 Resources

In GWCN, in addition to the systems described in section 1.2.2, the following system is required:

Abbreviation	Title	Description
MO-SCORE-EMS	Master Operator – Shared Core Network – Element Management System	The EMS enabling the Master Operator to manage the Shared Core Network. It has direct OA&M links to the shared Core NEs. This EMS generally (though not necessarily) comes from the same supplier as the shared Core Network Elements.

9.1.3.3 Management Architecture

9.1.3.3.1 Management Architecture #3

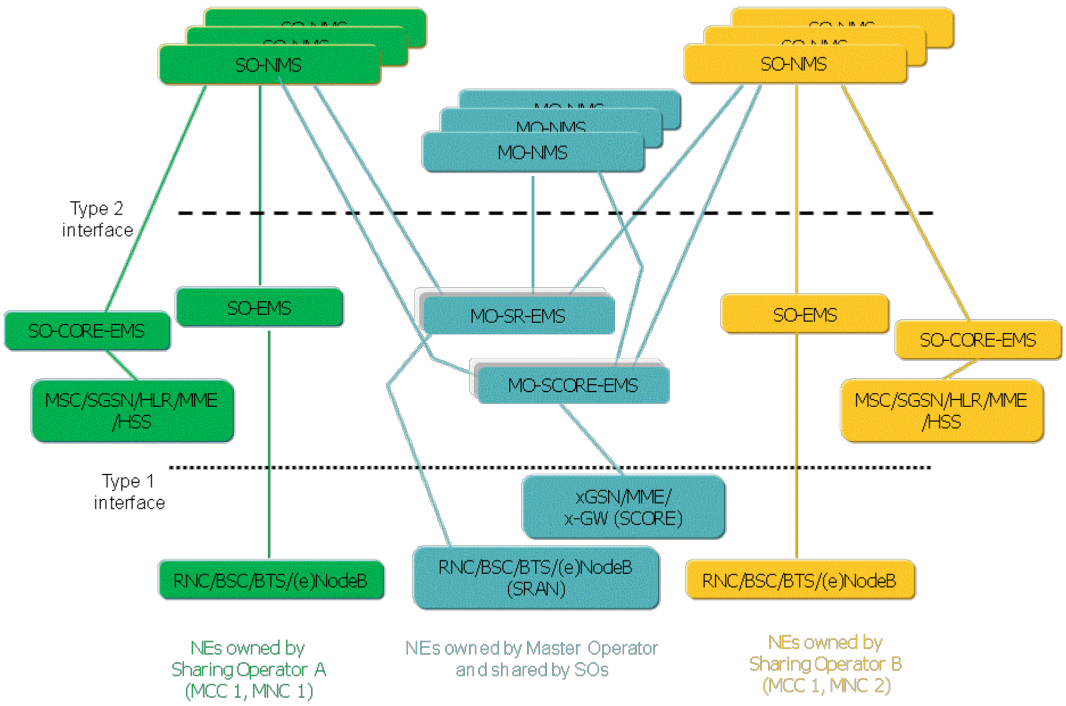


Figure 0-21: GWCN - Management Architecture #3

9.1.3.3.2 Management Architecture #4

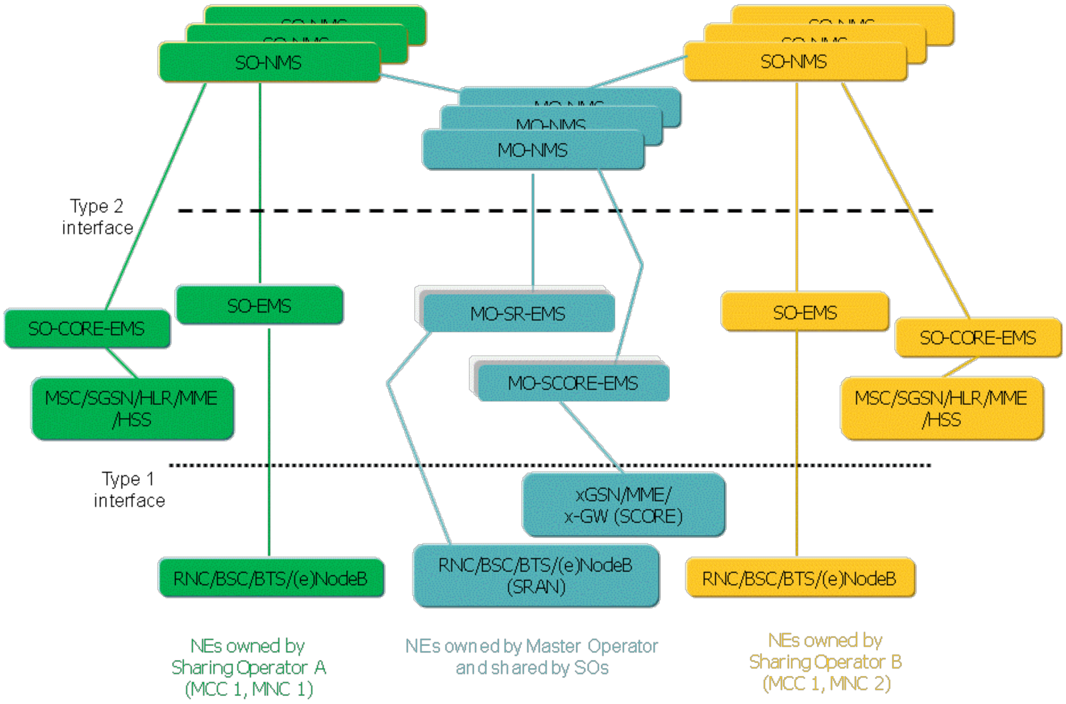


Figure 0-22: GWCN - Management Architecture #4

9.1.4 Other (out of scope) network sharing scenarios

9.1.4.1 Passive RAN Sharing

Passive RAN sharing (also known as site or infrastructure sharing) is used by mobile operators to save CAPEX and OPEX as well as to speed up deployment of base stations, because of the complexity and the expense of finding new sites to improve their coverage. Environmental (visual) and public health concerns are an additional driver for passive RAN sharing.

Figure 0-23: Passive RAN Sharing

Active RAN elements, i.e. eNodeBs in LTE, are not shared.

9.1.4.2 Regional/ National Roaming

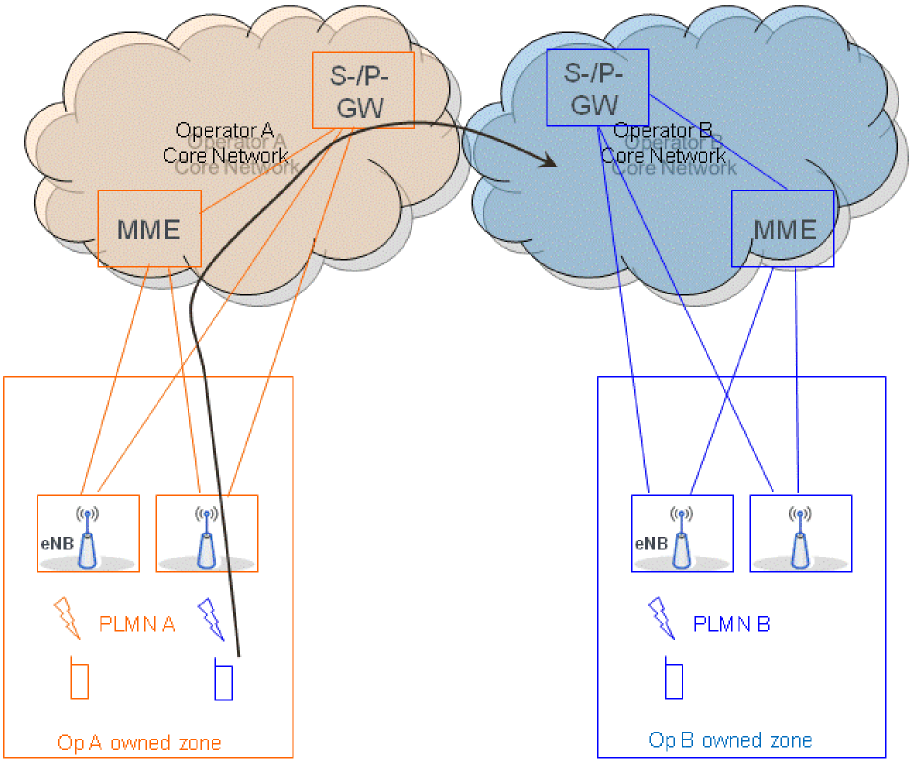


Figure 0-24: Regional / National Roaming

9.1.4.3 Mobile Virtual Network Operator (MVNO)

Depending on architectural options taken by MVNOs in terms of sharing its core network elements with the Hosting Mobile Network Operator, some MVNO models could be considered a variant of network sharing.

Light MVNOs typically do not have a limited own infrastructure. They use incumbent mobile network infrastructure such as radio equipment as a commodity, while the MVNO offers its own advanced and differentiated services based on exploitation of their own value added service infrastructure. The goal of offering value-added services is to differentiate versus the incumbent mobile operator, allowing for customer acquisition and preventing the MVNO from needing to compete on the basis of price alone.

MVNOs have full control over the SIM card, branding, marketing, billing, and customer care operations. While sometimes offering operational support systems (OSS) and business support systems (BSS) to support the MVNO, the incumbent mobile operators most keep their own OSS/BSS processes and procedures separate and distinct from those of the MVNO.

Light MVNO has IN and charging systems, back office such as call centres and customer centres only. They do not have HLR / HSS, VLR and other mobile core network infrastructure. They share the HLR / HSS of MNO, with dedicated number series.

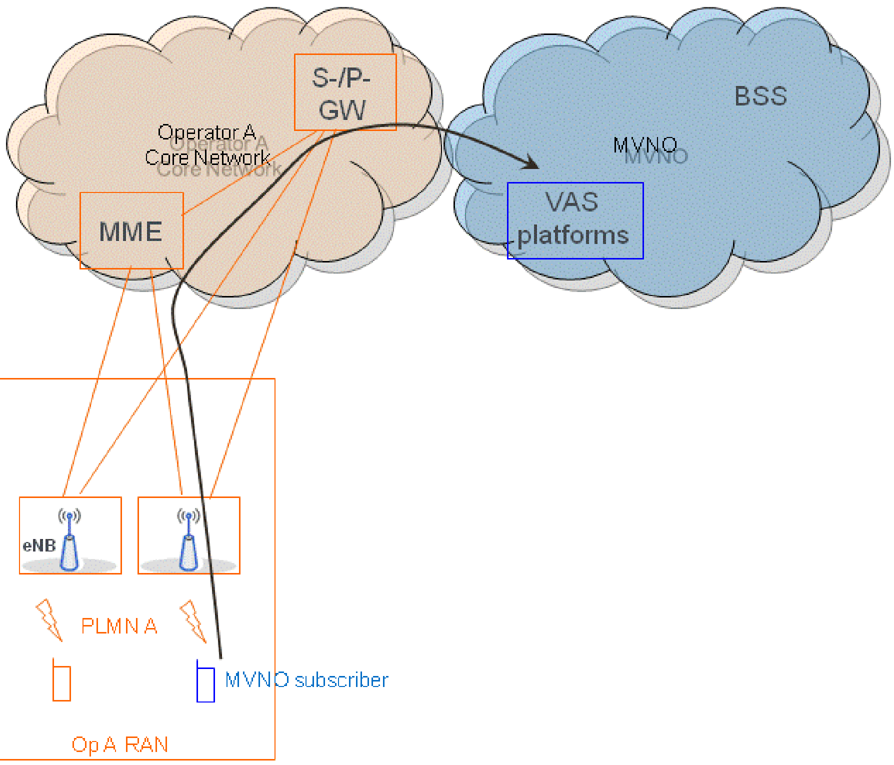


Figure 0-25: Simple MVNO Architectural Model

Some full MVNOs are actually deploying their own mobile core network and mobile IN infrastructure in order to facilitate the means to offer value-added services.

9.1.5 Information framework to capture network sharing contract

REQ-NS (31)

Identifier: REQ-NS (31)	**Rel. Use case id :** Network sharing contract (Agreement)	**Priority: 1**
Title : Standardized common information model		
Description: It is important that the Master Operator and Sharing Operators can rely on a standardized common information model to represent all the aforementioned concepts, including: • Roles (Master Operator, Sharing Operators). • Rights attached to roles (e.g. rights to configure, rights to receive alarms, etc.). • Duties attached to roles (e.g. duty for the Master Operator to provide Sharing Operators with monthly KPIs). • Delegations from Sharing Operators to Master Operator (if any). • Organisations (those which are playing roles). • Shared resources / unshared resources as part of the RAN sharing agreement. • RAN Sharing agreement, including Service Level Agreements.		

Rationale:

REQ-NS (32)

Identifier: REQ-NS (32)	**Rel. Use case id :** Network sharing contract (Agreement)	**Priority: 1**
Title : RAN Sharing contract Repository		
Description: An OSS level application – which we call here RAN Sharing contract Repository - shall offer the possibility to handle this standardized information model and support instances of this standardized information model.		
Rationale:		

REQ-NS (33)

Identifier: REQ-NS (33)	**Rel. Use case id :** Network sharing contract (Agreement)	**Priority: 1**
Title : Read Access to RAN Sharing contract Repository via standardized interface		
Description: Standardized interfaces shall enable the Master Operator and Sharing Operators to retrieve information from this OSS application.		
Rationale:		

REQ-NS (34)

Identifier: REQ-NS (34)	**Rel. Use case id :** Network sharing contract (Agreement)	**Priority: 1**
Title : Provisioning of RAN Sharing contract Repository via standardized interface		
Description: The Master Operator is responsible for populating this OSS application by instantiating aforementioned information concepts on a concrete network sharing project basis, via a standardized interface.		
Rationale:		

REQ-NS (35)

Identifier: REQ-NS (35)	**Rel. Use case id :** Network sharing contract (Agreement)	**Priority: 2**
Title : Machine-to-Machine interface to RAN Sharing contract Repository		
Description: It shall be possible for the Master Operator to access this OSS application from its MO-SR-EMS (in case of Management Architecture #1 – see Figure 26), its MO-SCORE-EMS (in case of Management Architecture #3 – see Figure 26), or from its MO-NMS (in case of Management Architecture #2 or #4 – see Figure 27) via a machine-to-machine interface.		
Rationale:		

As an example, this interface will enable the Master Operator, each time a Sharing Operator is willing to access data from the shared network, whether the request coming from the Sharing Operator is compliant with its rights (as defined in the RAN sharing agreement).

Figure 26 shows the RAN Sharing Contract Repository, in case of Management Architecture #1.

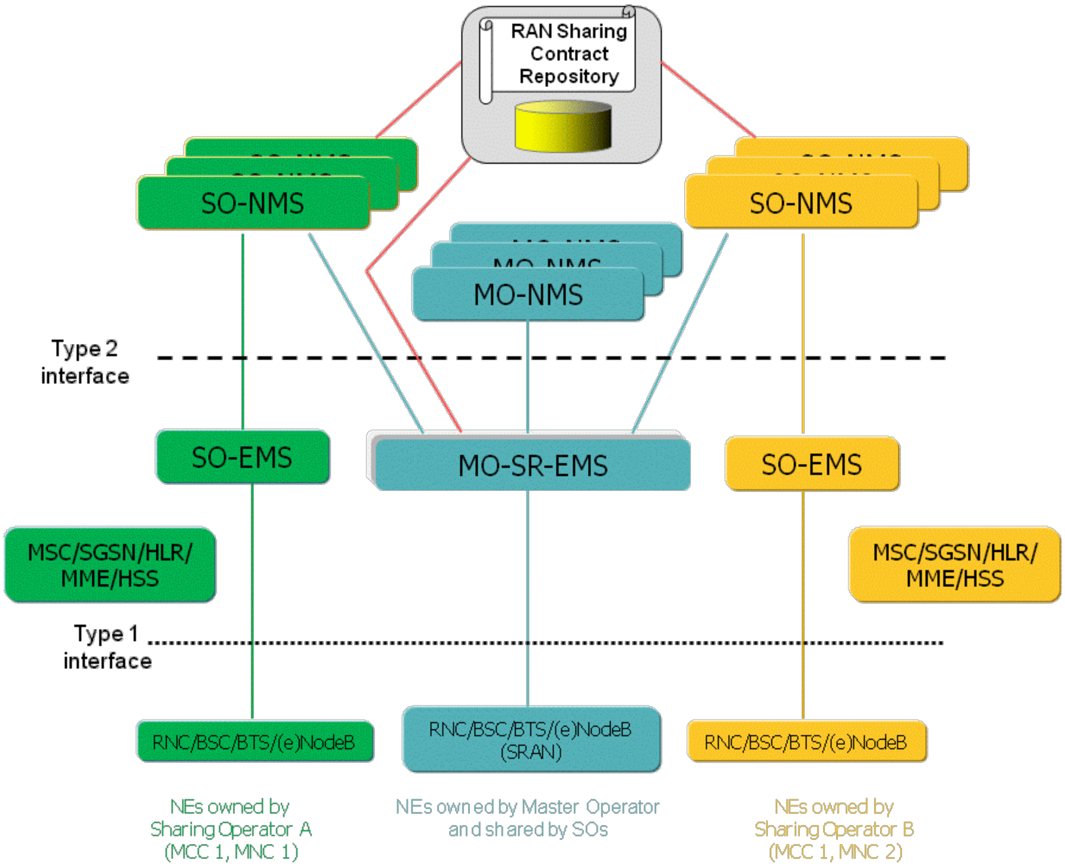


Figure 0-26: RAN Sharing Contract Repository in Management Architecture #1

Figure 27 shows the RAN Sharing Contract Repository, in case of Management Architecture #2.

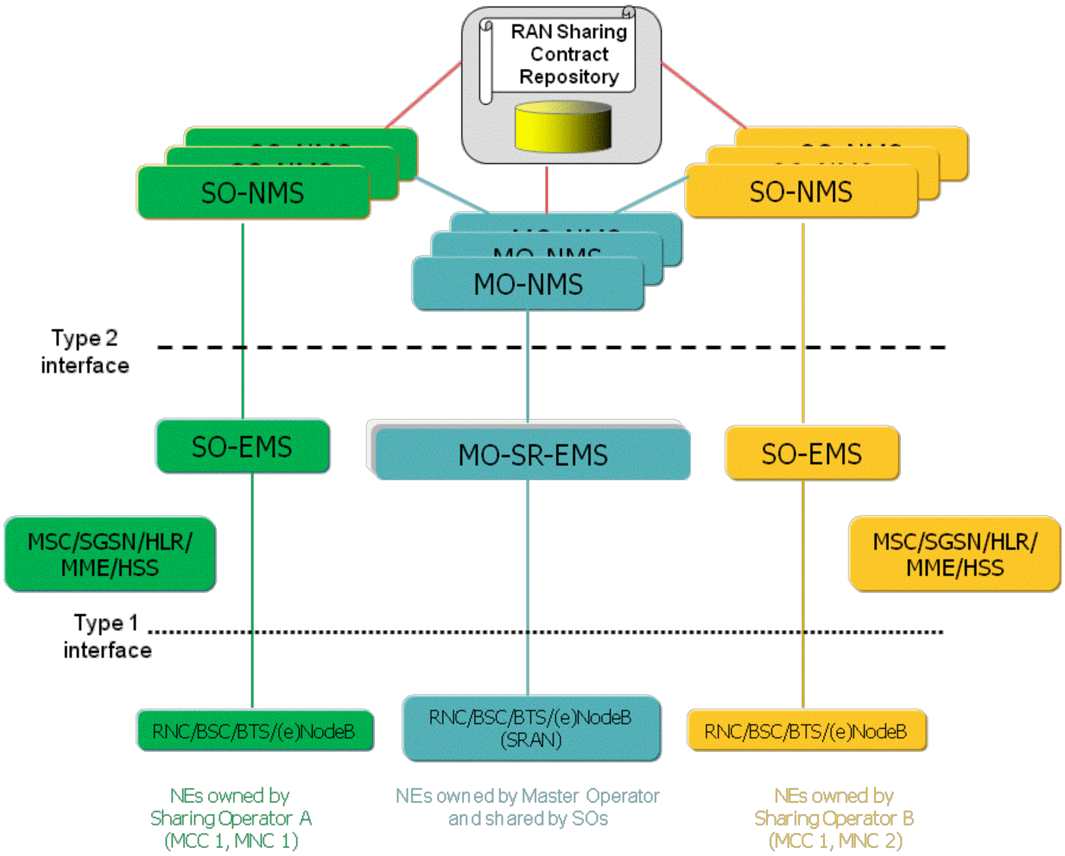


Figure 0-27: RAN Sharing Contract Repository in Management Architecture #2

9.2 Single Operator – Multi-Affiliate Network Sharing scenarios

In this section, we describe two main use cases where large operators, in their constant willingness to decrease their operational costs, put resources in common between several of their affiliates. Those shared resources can be:

- Network resources together with their Element Management System(s) – see Section 2.3;
- OSS resources, i.e. Element Management System(s) only or Element Management System(s) + Network Management System(s) – see Section 2.2.

In both use cases, the same principle applies: instead of being replicated in various affiliates of the Operator, resources are deployed once in a single affiliate domain and accessed remotely from other affiliates' network.

9.2.1 Roles

Role name	Description
Master Affiliate (MA)	The Master Affiliate (MA) is responsible for the shared Network Elements and/or Operation Support Systems. The Master Affiliate provides network and/or OA&M services to other Affiliates, called Sharing Affiliates.

Sharing Affiliate (SA)	Sharing Affiliates (SA) use the Master Operator's Network Elements and/or Operation Support Systems. Sharing Affiliates are clients of the Master Affiliate, in that they have a network and/or OSS sharing contract with the Master Affiliate to be able to benefit from the Master Affiliate's network and/or operation services.

9.2.2 OSS shared between Operator' affiliates

9.2.2.1 Resources

Abbreviation	Title	Description
MA-EMS	Master Affiliate - Element Management System	The EMS(s) enabling the Master Affiliate to centrally manage the NEs of several Affiliates. It has direct OA&M links to these NEs. This EMS generally comes from the same supplier as the NEs.
MA-NMS	Master Affiliate - Network Management System	Network Management System belonging to the Master Affiliate, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Master Affiliate or supplied by Independent Software Vendors (ISV).
SA-NMS	Sharing Affiliate – Network Management System	Network Management System belonging to the Sharing Affiliate, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Sharing Affiliate or supplied by Independent Software Vendors (ISV).
SA-SMS	Sharing Affiliate – Service Management System	Service Management System belonging to the Sharing Affiliate, part of its Operation Support Systems / Business Support Systems. SM Systems are generally dedicated to a communication service and provide an end-to-end view of this service across the network domains.

9.2.2.2 Management Architecture #5

As depicted in Figure 28, Operator's Affiliates A and B keep their network elements unshared in their own countries. However, both Element Management Systems and Network Management Systems are centralized and deployed in the country of the Master Affiliate – see Management Architecture #5 below.
Each Affiliate being responsible for service level aspects in its own country keeps its Service Management applications locally, i.e. as close as possible to its customers. In each Affiliate, Service Management applications have connections with relevant centralized Network Management Systems of the Master Affiliate.

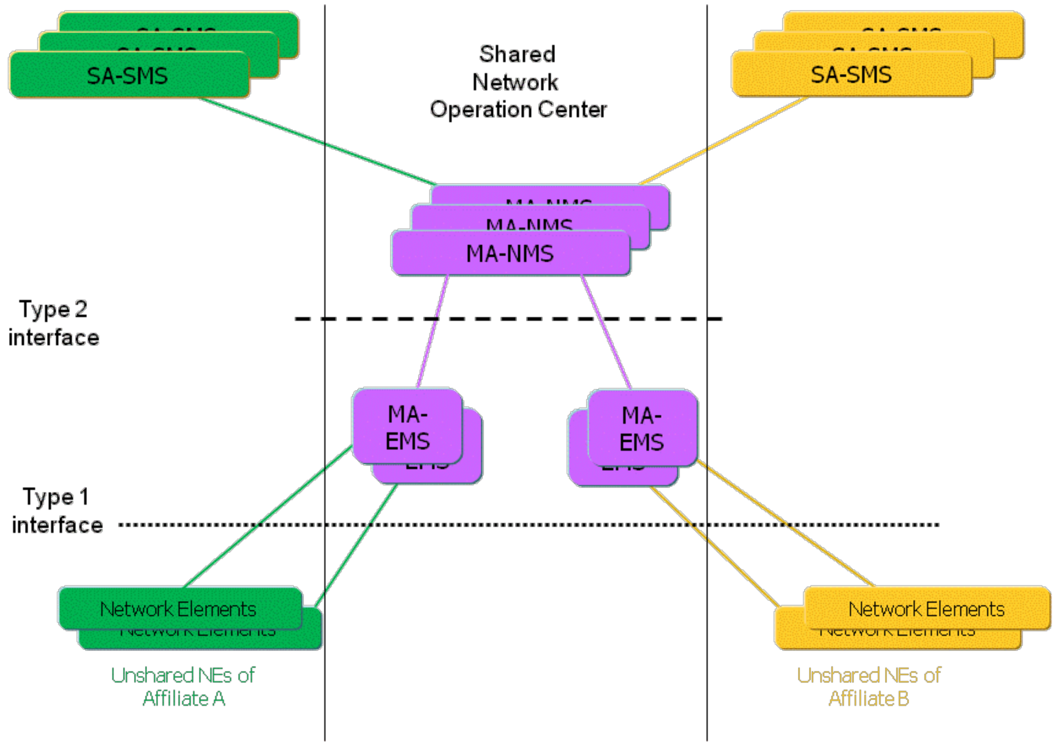


Figure 0-28: Management Architecture #5 - EMS / NMS sharing between Operator affiliates

Illustration: Affiliates A and B have circuit-switched and packet-switched mobile core networks as well as an IMS network deployed locally in their respective country. Operations of these network domains are not done locally[5] but, instead, are centralized in a unique Network Operation Centre (NOC) in a third country. In this NOC, all relevant EMSs are installed namely EMSs for circuit-switched mobile core networks of Affiliates A and B, EMSs for packet-switched mobile core networks of Affiliates A and B, and EMSs for IMS core networks of Affiliates A and B. The number of required EMSs vary according to various parameters, including cross-affiliate network element homogeneity (affiliates have bought network elements from the same vendor – in such a case, a single EMS can be envisioned – or not), vendor OSS solution homogeneity (vendors offer the same EMS platform for different network domains, e.g. circuit-switched and packet-switched mobile core networks), dimensioning aspects (number of network elements to be managed), organizational issues (each network domain is operated by a separate team with its own EMS platform), etc. Network Management Systems are also deployed centrally. They are dedicated per OA&M functional area, e.g. one NMS for Fault management, another one for Performance management, etc. They provide operational staff with a broader view of the network, in that e.g. the Fault management NMS collects alarm notifications potentially from the CS mobile core network EMS, from the PS mobile core network EMS and from the IMS core network EMS. Service Management applications are instantiated locally in the countries of Affiliate A and Affiliate B and have OA&M links with central Network Management Systems of the Master Affiliate. They provide local Service Management Centres with information about services offered to customers of their country. They have enough knowledge to e.g. calculate the impact of a fault occurring on a network element, on the service offered (for example, a network-level critical alarm detected on a P-CSCF may have different levels of impact on the Voice over LTE over IMS service: service not affected, quality of service degraded, service affected).

9.2.2.3 High-level Requirements

[5] Except Field Ops.

REQ-NS (101)

Identifier: REQ-NS (101)	Rel. Use case id : Management Architecture	Priority: 1
Title : Multiple MA-NMS interfaces to Service Management applications		
Description: The MA-NMS shall be able to support restricting the information provided to SA-SMSs or operations allowed from SA-SMSs, one set per Sharing Affiliate, allowing each Sharing Affiliate to have its own view on the network elements.		
Rationale: Sharing Affiliates may each have different clauses in their OSS Sharing agreement with the Master Affiliate. Consequently, the interface between the MA-NMS and the respective SA-SMSs may vary accordingly.		

REQ-NS (102)

Identifier: REQ-NS (102)	Rel. Use case id : Management Architecture	Priority: 1
Title : Management interface – Generic Requirement		
Description: The interface(s) between MA-NMS and SA-SMSs shall fulfil REQ-GEN(1) to REQ-GEN(22) from [2].		
Rationale:		

REQ-NS (103)

Identifier: REQ-NS (103)	Rel. Use case id : Management Architecture	Priority: 1
Title : Management interface based on Federated Network Information Model		
Description: The interface(s) between MA-NMS and SA-SMSs shall be based on standardized interfaces (information model + protocol). Though this interface is different from Itf-N (according to 3GPP terminology), it is expected that this interface can be based on 3GPP-TMF FNIM.		
Rationale:		

9.2.3 Network Elements and their OSS shared between Operator' affiliates

In order to save CAPEX and OPEX, operator' affiliates can share network elements. For a number of reasons (e.g. technical, legal, etc.), this cannot apply to all types of NEs. In particular, wire line and wireless access network elements have to remain local, i.e. close to where they are used. Conversely, some other network elements not only can be deployed centrally but do not necessarily have to be replicated in each and every country where in the Operator has an affiliate. When these affiliates are installed in the same geographical region and need similar types of network elements to offer their communication services, significant savings are obtained by deploying these network elements in a central location and sharing them amongst Operator' affiliates.

Since shared network elements, all deployed centrally in one single country, have to be accessible from other affiliate network elements, cross-border transport links must be available.

The relevance and feasibility of such a deployment scenario depend on legal, geographical, technical and economical aspects and is to be studied on a per case basis.

9.2.3.1 Resources

Abbreviation	Title	Description
MA-SNE-EMS	Master Affiliate – Shared Network Elements – Element Management System	The EMS enabling the Master Affiliate to manage the Shared NEs. It has direct OA&M links to the shared NEs. This EMS generally comes from the same supplier as the shared NEs.
MA-SNE-NMS	Master Affiliate – Shared Network Elements – Network Management System	Network Management System belonging to the Master Affiliate, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Master Affiliate or supplied by Independent Software Vendors (ISV).
SA-EMS	Sharing Affiliate – Element Management System	An EMS enabling the Sharing Affiliate to manage its operator-specific NEs. It has direct OA&M links to these NEs. This EMS generally comes from the same supplier as the NEs.
SA-NMS	Sharing Affiliate – Network Management System	Network Management System belonging to the Sharing Affiliate, part of its Operation Support Systems. NM Systems are generally dedicated to functional domains such as e.g. Fault Management, Performance Management, etc. NM Systems are generally either in-house made by the Sharing Affiliate or supplied by Independent Software Vendors (ISV).
SA-SMS	Sharing Affiliate – Service Management System	Service Management System belonging to the Sharing Affiliate, part of its Operation Support Systems / Business Support Systems. SM Systems are generally dedicated to a communication service and provide an end-to-end view of this service across the network domains.

9.2.3.2 Management Architecture

The following main management architectures can be identified.

9.2.3.2.1 Management Architecture #6

The Master Affiliate offers management capabilities to Sharing Affiliates via its Shared Network Elements Element Management System. The MA-SNE-EMS has a northbound interface towards network management layer applications of the various Sharing Affiliates (SA-NMS) in all countries, providing thus each affiliate with OA&M capabilities related to Shared Network Elements.

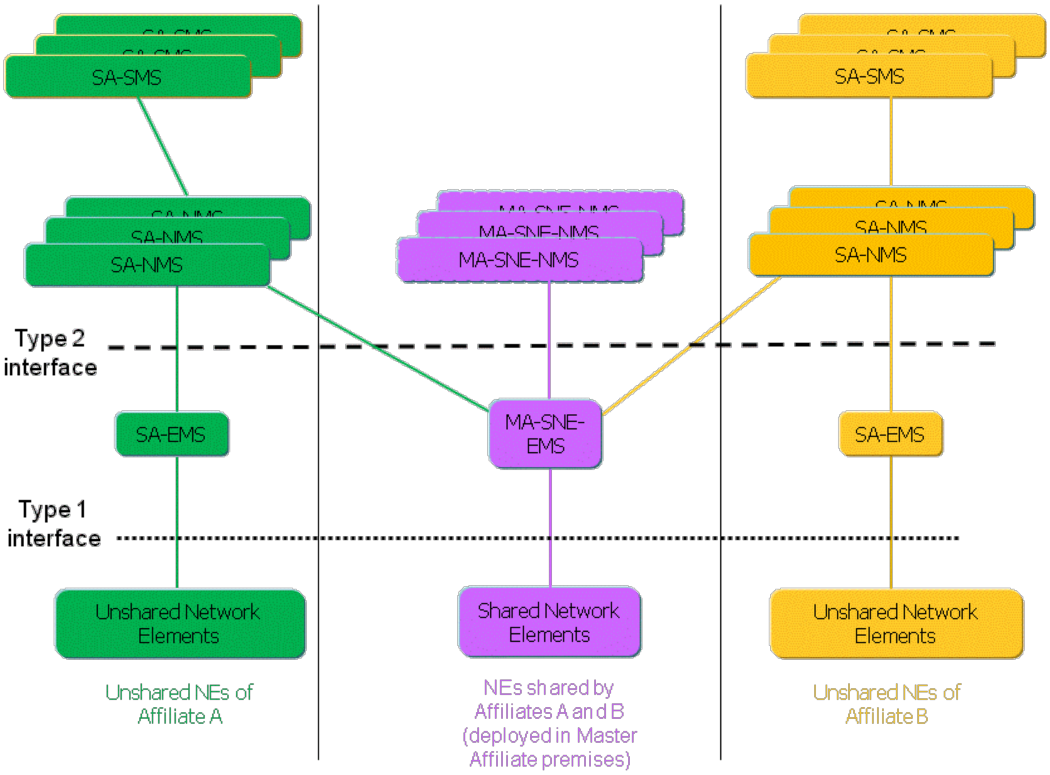


Figure 0-29: Management Architecture #6 - Network and OSS sharing between Operator affiliates

9.2.3.2.2 Management Architecture #7

The Master Affiliate offers management capabilities to Sharing Affiliates via its Shared Network Elements Network Management System(s). The MA-SNE-EMS has a northbound interface towards the network management layer applications of the Master Affiliate. The MA-SNE-NMSs have a east-west interface towards network management layer applications of each Sharing Affiliate (SA-NMS), those SA-NMSs having themselves interfaces towards their Service Management Systems (SA-SMS), providing thus each affiliate with OA&M capabilities related to Shared Network Elements and enabling Sharing Affiliates to build an end-to-end management view of their services.

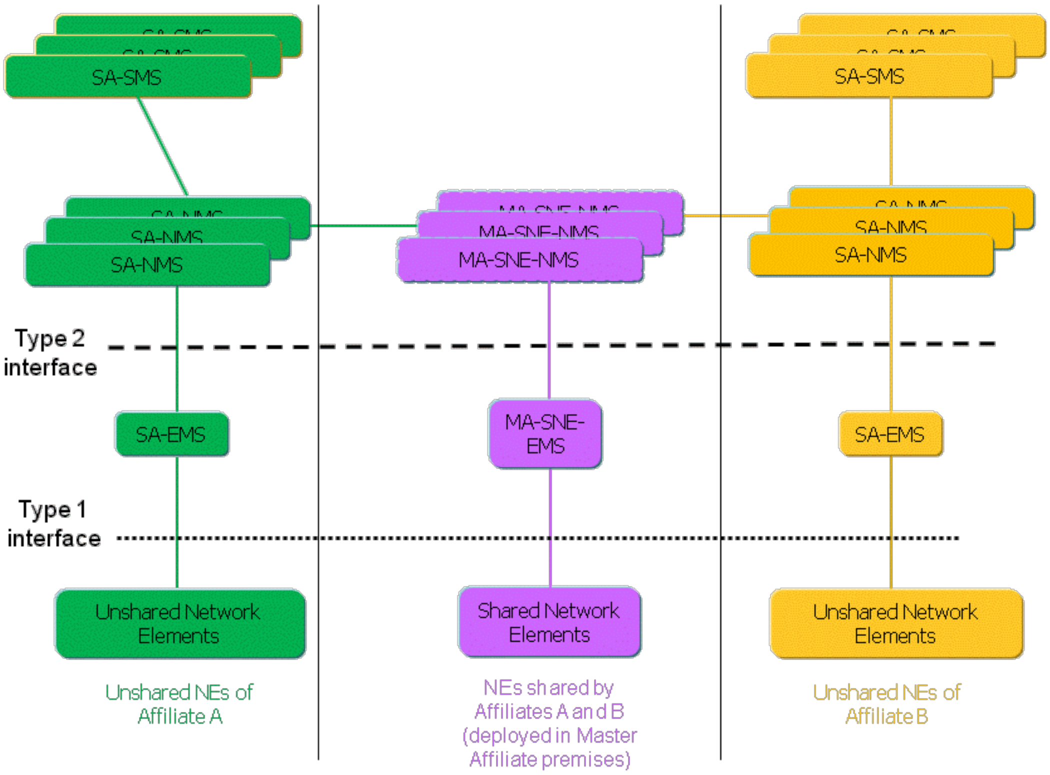


Figure 0-30: Management Architecture #7 - Network and OSS sharing between Operator affiliates

9.2.3.2.3 Management Architecture #8

The Master Affiliate offers management capabilities to Sharing Affiliates via its Shared Network Elements Network Management System. The MA-SNE-EMS has a northbound interface towards the network management layer applications of the Master Affiliate. The MA-SNE-NMS has an interface towards service management layer applications of the Sharing Affiliates (SA-SMS), providing thus each Sharing Affiliate with OA&M capabilities related to Shared Network Elements and enabling Sharing Affiliates to build an end-to-end management view of their services.

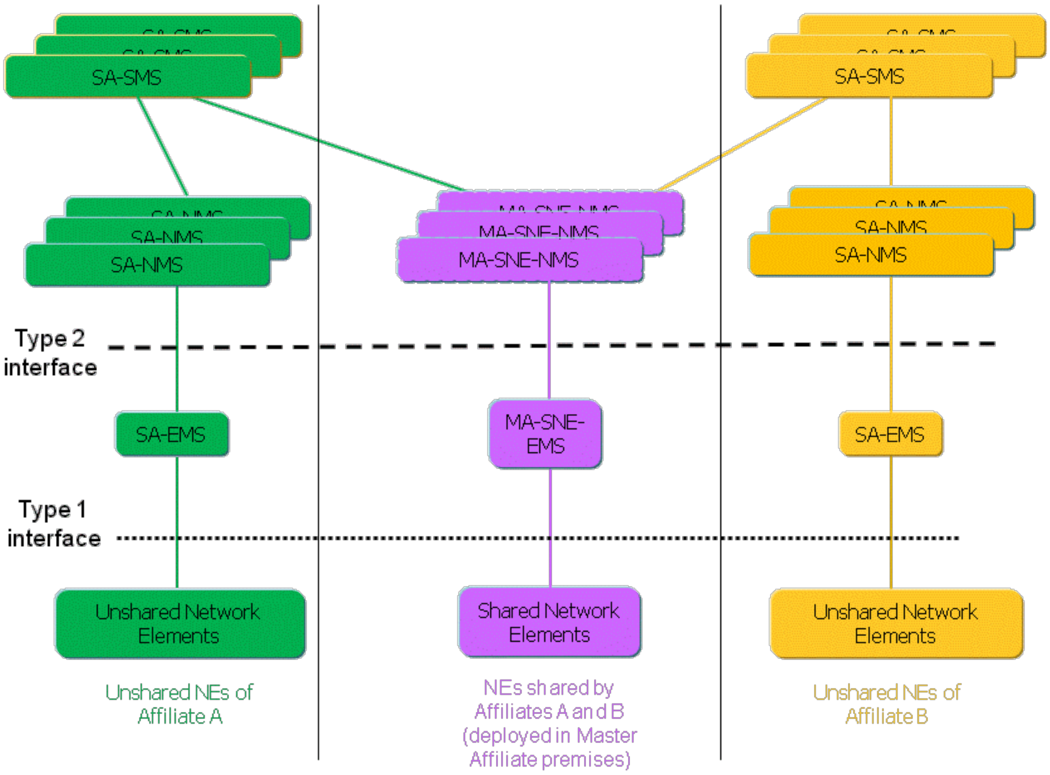


Figure 0-31: Management Architecture #8 - Network and OSS sharing between Operator affiliates

9.2.3.3 High-level Requirements

REQ-NS (201)

Identifier: REQ-NS (201)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Multiple management interfaces to Sharing Affiliates' NMSs		
Description: In Management Architecture #6 (respectively Management Architecture #7), the MA-SNE-EMS (resp. MA-SNE-NMS) shall be able to support restricting the information provided to SA-NMSs or operations allowed from SA-NMSs, one set per Sharing Affiliate, allowing each Sharing Affiliate to have its own view on the shared network elements.		
Rationale: Sharing Affiliates may each have different clauses in their Network Sharing agreement with the Master Affiliate. Consequently, the interface between their respective SA-NMS(s) and the MA-SNE-EMS / MA-SNE-NMSs may vary accordingly. Example: one Sharing Affiliate may be willing to be able to trigger performance jobs from its SA-NMS whereas another Sharing Affiliate may not.		

REQ-NS (202)

Identifier: REQ-NS (202)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Multiple management interfaces to Sharing Affiliates' SMSs		
Description:		

	In Management Architecture #8, the MA-SNE-NMS shall be able to support restricting the information provided to SA-SMSs or operations allowed from SA-SMSs, one set per Sharing Affiliate, allowing each Sharing Affiliate to have its own view on the shared network elements.
Rationale: Sharing Affiliates may each have different clauses in their Network Sharing agreement with the Master Affiliate. Consequently, the interface between their respective SA-SMS(s) and the MA-SNE-NMSs may vary accordingly.	

REQ-NS (203)

Identifier: REQ-NS (203)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface – Generic Requirement		
Description: The interface(s) between MA-SNE-EMS and SA-NMSs shall fulfil REQ-GEN(1) to REQ-GEN(22) from [2].		
Rationale:		

REQ-NS (204)

Identifier: REQ-NS (204)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface – Generic Requirement		
Description: The interface(s) between MA-SNE-NMS and SA-NMSs shall fulfil REQ-GEN(1) to REQ-GEN(22) from [2].		
Rationale:		

REQ-NS (205)

Identifier: REQ-NS (205)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface – Generic Requirement		
Description: The interface(s) between MA-SNE-NMS and SA-SMSs shall fulfil REQ-GEN(1) to REQ-GEN(22) from [2].		
Rationale:		

REQ-NS (206)

Identifier: REQ-NS (206)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface based on Federated Network Information Model		
Description: The interface(s) between MA-SNE-EMS and SA-NMSs shall be based on standardized interfaces (information model + protocol) according to 3GPP-TMF FNIM.		

Rationale:

REQ-NS (207)

Identifier: REQ-NS (207)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface based on Federated Network Information Model		
Description: The interface(s) between MA-SNE-NMSs and SA-NMSs shall be based on standardized interfaces (information model + protocol) according to 3GPP-TMF FNIM.		
Rationale:		

REQ-NS (208)

Identifier: REQ-NS (208)	**Rel. Use case id :** Management Architecture	**Priority: 1**
Title : Management interface based on Federated Network Information Model		
Description: The interface(s) between MA-SNE-NMSs and SA-SMSs shall be based on standardized interfaces (information model + protocol) according to 3GPP-TMF FNIM.		
Rationale:		

9.3 References

[100] NGMN Alliance NGMN TOP OPE Requirements Version 1.0
[101] NGMN NGCOR Consolidated Requirements V1.3
[102] TM Forum GB922, Information Framework (SID) Suite, Release 9.5, March 2011
[103] TM Forum TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx
[104] TM Forum MTOSI Release 2.1 (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[105] TM Forum Business Process Framework (eTOM) Release 9 (http://www.tmforum.org/StandardsPacks/8175/home.html)
[106] TM Forum eTOM Release 9.0, GB921 Addendum D, August 2010
[107] TM Forum TAM Release 4.5, TMF, April 2011
[108] 3GPP TS 32.101 Telecommunication management; Principles and high level requirements
[109] 3GPP TS 28.620 Fixed Mobile Convergence (FMC) Federated Network Information Model (FNIM) Umbrella Information Model (UIM)
[110] 3GPP TS 28.xyz series.

9.4 Appendix

9.4.1 Glossary and Abbreviations

Abbreviation	Meaning & Terms	Further explanation
2G/3G/LTE	Standards for mobile communication network and devices capabilities	
3GPP	3rd Generation Partnership Project	http://www.3gpp.org
3GPP SA5	Telecom Management group within 3GPP	http://www.3gpp.org/SA5-Telecom-Management
AKA	also known as	
ANR	Automatic Neighbourhood Relation	
BA	Business Agreement (TM Forum)	Requirements and usage scenario specification.
BBF	Broadband Forum	http://www.broadband-forum.org
BSS	Business Support Systems	Business Support Systems
CAPEX	Capital Expenditures	costs to set up/ change a network
CM	Configuration Management	
CMDB	Configuration Management Data Base	ITIL term
CN	Core Network	
COTS	Commercial Off the Shelf	COTS
EM	Element Management	EM
EMS	Element Management System	EMS
eNB	Enhanced NodeB	
EPC	Evolved Packet Core	Mobile Core Network for 4G
eTOM	Enhanced Telecommunication Operations Map	eTOM

Abbreviation	Meaning & Terms	Further explanation
FAB	Fullfillment, Assurance and Billing	
FCAPS	Fault, Configuration, Assurance, Performance	FCAPS
FIM	Federated Information Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Information Model part of these models contains the static data; i.e., the object classes with their attributes and the content of the notifications."
FM	Fault Management	Fault Management
FMC	Fixed Mobile Convergence	http://en.wikipedia.org/wiki/Fixed-mobile_convergence
FOM	Federated Operations Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Operations Model part of these models contains the dynamics; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
GWCN	Gateway Core Network	A variant of core network sharing model
HLR	Home Location Register	
HSS	Home Subscribe Server	It's an evolution of the current HLR used as a location server for 2G/3G networks
IRP	Integration Reference Point (3GPP term)	3GPP 32.103
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector (SDO)	ITU-T
JV	Joint Venture	
LTE	Long Term Evolution	http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution
MME	Mobility Management Entity	
MOCN	Multi-Operator Core Network	Model of Network sharing which does not share the Core Networks
MORAN	Multi-Operator Radio Access Network	A model of Network sharing at Radio access level
MSC	Mobile Switching Centers	
MTOSI	Multi Technology OS interface	TM Forum interface product. It is an XML-based Operations System (OS)-to-OS interface suite. The Network Management System-to-Element Management System communication is also covered as a special case.
MVNO	Mobile Virtual Network Operator	
NE	Network Element	Network_element
NBI	Northbound Interface	Interface between EMS and NMS
NGCOR	Next Generation Converged Operations Requirements	NGMN project
NGMN	Next Generation Mobile Network	http://www.ngmn.org
NM	Network Management	Network_management
NMS	Network Management System	Network_management_system
NOC	Network Operation Centre	
NRM	Network Resource Model (3GPP)	Contains the static data of an interface specification.
OA&M	Operation, Administration & Maintanance	OA&M
OC	Operating Committee (NGMN)	

Abbreviation	Meaning & Terms	Further explanation
OPE	Operational Efficiency	Requirements specification from NGMN.
OPEX	Operational Expenditures	Costs of running a network
OS&R	Operation, Support and Readiness	Is a Level 1 process grouping of the Business Process Framework. OS&R contains processes for ensuring operational readiness in the fulfillment, assurance and billing areas.
OSS	Operations Support System	Operations_support_system
PM	Performance Management	http://en.wikipedia.org/wiki/FCAPS
QoS	Quality of Service	QoS
RAN	Radio Access Network	http://en.wikipedia.org/wiki/Radio_access_network
RAT	Radio Access Technology	
RM&O	Resource Management & Operations	
SCP	Service Control Points	
SDO	Standards Developing Organisation	All committes, fora and partnerships that create standards, recommendations and technical reports.
S-GW	Serving Gateway	
SID	Shared Information & Data model (TM Forum)	http://www.tmforum.org/InformationFramework/1684/home.html
SLA	Service Level Agreement	KPI describing user requirements tro be translated into QOS objective at operator side within an agreement
SM&O	Service Management &Operations	
SON	Self Organizing Network	
SP	Service Provider	Company, which provides access to telephone and related communications services
TAM	Telecom Appplications Map	TMF term
TMF	TM Forum	www.tmforum.org
UE	User Equipment	
UMTS	Universal Mobile Telecommunication System	UMTS
	Business Services	These are the operations in TM Forum terminology.
	Business Use Case	High level uses case driven by a business scenario.
	common architecture	All interfaces should be part of a common architecture
	Common Core Network	Business architecture Scenario
	Common Information Model	This term is used to reference information models like TMForum SID
	Communication Partners	OSS systems, which exchange information
	Converged Framework Model	Harmonised design guidelines for tooling.
	cross-domain	Cross mobile and fixed domains
	cross-domain	Cross mobile and fixed domains
	Domain	Related to the partioning of the network
	Dynamic Requirement	Requirements which describe the operations part of the management interface.
	Element Management Layer	EMS level in layering architecture
	Element Manager	Element_Manager

Abbreviation	Meaning & Terms	Further explanation
	EMS (server)	The SW component which implements the interface in the OSS systems, which delivers a service to other OSS systems
	EMS-OSS layer	Summary of all OSS systems which deliver an EMS functionality
	eNodeB	Base Station for LTE
	entity	An entity is some tangible or conceptual thing , entity word is typically used when presenting things without a real name name or label. Entities are characterized by attributes and relationships.
	EPC Network	Mobile Core Network for 4G
	federated information / data model	See stream MT
	Federated Model	see Operations Model
	Federated Network Resource Model	see Operations Model
	femtoCell	Home NodeBB (Base Station deployed in the Home)
	management architecture	Defines the architecture between Operations Systems and the between Operations Systems and the network.
	management area	These are e.g., alarm management, inventory, performance management etc..
	Management Interface	An instance of an interface between two OSes used for management.
	Management Model	Generic term for information model and operations model.
	management operation	Operations executed via the management interface.
	management recommendations	ITU-T standards are called Recommendations.
	management workflows	Specific sequence of operations executed via the management interface.
	multi-domain network	Domains are e.g., access, metro, backhaul, core.
	multi-technology network	Technologies are e.g., ATM, OTN, SDH, Ethernet, DSL, LTE, 2G, 3G, HSPA.
	Network Abstraction Layer	A logical layer between the network and the management layer which relay an abstracted view (from management point of view) of the network.
	network data	Data which describes - from management point of view - the underlying network in an abstract way. This data can be used by all different management areas.
	Network Level Interface	An interface which is able to provide an end-to-end view of the underlying network.
	network level management	A management function which is able to manage an end-to-end view of the underlying network.
	Network Operator	Company, which provides access to telephone and related communications services
	Network Resource Model	Data model representing the equipment of a network. It's 3GPP terminology
	network technology	For Mobile , it means 2G, 3G or 4G
	network type	The type of the network (e.g. UMTS- Radio, DWH, IP, etc. ..)
	Operator	Role, responsible for the management of a network and/or service
	operator-wide OSS application	Applications developed by the operator to ensure FM, PM, CM,
	OSS application	An application which delivers a capability dedicated to the OSS domain

Abbreviation	Meaning & Terms	Further explanation
	OSS Interface	Interface between OSS systems
	physical resource	Physical resources are e.g., network elements, cables, fibres etc..
	resource	Resource is any physical or virtual component of a telecommunications network
	Resource Configuration Management	TMForum TAM definition: "The Resource Configuration Management application generates a resource plan to fulfill a resource order."
	Resource Fault Management	TMForum TAM definition: "Fault Management applications are responsible for the management of faults, or troubles, associated with the service provider's resources. "
	resource management layer	Covers all Resource Management processes as defined in the TM Forum Business Process Framework (eTOM) "Resource Management & Operations" (RM&O) layer within the operations & support, fulfillment, and assurance verticals. This process grouping maintains knowledge of resources (application, computing and network infrastructures) and is responsible for managing all these resources.(e.g. networks, IT systems, servers, routers, etc.) utilized to deliver and support services required by customers.
	shared network	Generic term which includes different model sharing (at core, access network)
	Umbrella Model	Part of the model containing artefacts that can be used/inherited in both wireline and wireless network models.
	Use Case	It refers to Business architecture scenarios and Generic & Basic architecture scenarios

9.4.2 Network Sharing Requirements and their Addressees

NS	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-NS (1)	X		
REQ-NS (2)	X		
REQ-NS (3)	X		
REQ-NS (4)	X		
REQ-NS (5)	X		
REQ-NS (6)	X		
REQ-NS (7)	X		
REQ-NS (8)	X		
REQ-NS (9)	X		
REQ-NS (10)	X		
REQ-NS (11)	X		
REQ-NS (12)	X		
REQ-NS (13)	X		
REQ-NS (14)	X		
REQ-NS (15)	X		
REQ-NS (15a)	X		
REQ-NS (16)	X		

NS	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-NS (1)	X		
REQ-NS (17)	X		
REQ-NS (18)	X		
REQ-NS (19)	X		
REQ-NS (20)	X		
REQ-NS (20a)	X		
REQ-NS (21)	X		
REQ-NS (22)	X		
REQ-NS (23)	X		
REQ-NS (24)	X		
REQ-NS (25)	X		
REQ-NS (26)	X		
REQ-NS (27)	X		
REQ-NS (28)	X		
REQ-NS (30)	X		
REQ-NS (31)	X		
REQ-NS (32)	X		
REQ-NS (33)	X		
REQ-NS (34)	X		
REQ-NS (35)	X		
REQ-NS (101)	X		
REQ-NS (102)	X		
REQ-NS (103)	X		
REQ-NS (201)	X		
REQ-NS (202)	X		
REQ-NS (203)	X		
REQ-NS (204)	X		
REQ-NS (205)	X		
REQ-NS (206)	X		
REQ-NS (207)	X		
REQ-NS (208)	X		

10 REFERENCES

[111] NGMN Alliance NGMN TOP OPE Requirements Version 1.0

[112] NGMN NGCOR Consolidated Requirements V0.93

[113] University of Southern California - Center for Software Engineering - COTS Software Integration Cost Modelling Study 1997

[114] COCOTS (COnstructive COTS) - a cost estimation model to capture most important costs associated with COTS component integration, October 2002

[115] “Next-generation service assurance improves operational efficiency” in TM Forum CaseStudy Handbook 2012

[116] 3GPP TR 32.828 version 1.5.0. Study on Alignment of 3GPP Generic NRM IRP and TMF Shared Information/Data (SID) Model

[117] 3GPP TS 32.140. Subscription Management (SuM) requirements

[118] 3GPP TS 32.101 Telecommunication management; Principles and high level requirements

[119] 3GPP TS 32.300 Configuration Management; Name convention for Managed Objects.

[120] 3GPP TS 32.341/2/6. File Transfer (FT) Integration Reference Point (IRP); Requirements

[121] 3GPP TS 32.611/2/5 v10 Configuration Management (CM); Bulk CM Integration Reference Point (IRP): Requirements

[122] 3GPP TS 32.622. Configuration Management (CM); Generic network resources Integration Reference Point (IRP); Network Resource Model (NRM)

[123] 3GPP TS 32.690 V10 Release 10. Inventory Management (IM); Requirements

[124] 3GPP TS 32.691/2/6 V10.x.0 Release 10. Inventory Management (IM) network resources Integration Reference Point (IRP): Requirements

[125] 3GPP TS 32.692. Inventory Management (IM) network resources Integration Reference Point (IRP): Network Resource Model (NRM)

[126] 3GPP TS 32.xyz series on NRM.

[127] ATM Forum, Technical Committee, Network Management, M4 Network View CMIP MIB Specification, CMIP Specification for the M4 Interface, Sep, 1995.

[128] JOSIF Guidebook. Source: http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook

[129] NGWW 3GPP SA5-TM Forum model alignment JWG meeting in Budapest, April 4-6, 2011.

[130] NGWW Fixed Mobile Convergence (FMC) Network Management – Federated Network model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011.

[131] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3.

[132] TM Forum (2008a, Mai). DDP BA, TMF518_MRI, Version 1.1.

[133] TM Forum (2008b, Mai). DDP BA, TMF518_MSI, Version 1.0.

[134] TM Forum (2011, January). TM Forum Interface Program, Inventory Interface, Progress Status at TAW Paris.

[135] TM Forum GB922, Information Framework (SID) Suite, Release 9.0. Source: http://www.tmforum.org/browse.aspx?catID=9285&artf=artf2048

[136] TMF MTOSI 2.0. Source: http://www.tmforum.org/MTOSIRelease20/MTOSISolutionSuite/35252/article.html

[137] TM Forum MTOSI 2.0: Network Resource Fulfillment DDP IA, TMF612_NRF, Version 1.0.

[138] TM Forum Information Framework (SID) Suite; Release 9.5. Source: http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html

[139] TM Forum MTOSI Rel. 2.1 supporting document SD2-5_Communication_Styles.

[140] TM Forum SID Rel. 9.5.

[141] TMF & itSMF TR 143 Building bridges ITIL and eTOM.

[142] TR143 Abgerufen Juli 18, 2011, von about:blank

[143] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx.

[144] UML Superstructure Specification, v2.1.1.

[145] 3GPP TS 32.300 Telecommunication management; Configuration Management; Name convention for Managed Objects
[146] S5-102610 S5vTMFa033 E NSN Proposed enhancement of Generic NRM IOCs v3
[147] S5vTMFa169 (3GPP/TM Forum Concrete Model Relationships and Use Cases) from 3GPP SA5-TM Forum Resource Model Alignment JWG ftp://ftp.3gpp.org/tsg_sa/WG5_TM/Ad-hoc_meetings/Virtual-TMF-Align/S5vTMFa169.zip
[148] TR166 - Federated Information Framework - Concepts and Principles - v0.1.docx
[149] Fixed Mobile Convergence (FMC) Network Management – Federated Network Model (FNM) Umbrella, Version 1.2 JWG meeting in Budapest, April 4-6, 2011
[150] TM Forum MTOSI Release 2.1 (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[151] TM Forum Information Framework (SID) Suite; Release 9.5 (http://www.tmforum.org/Guidebooks/GB922InformationFramework/45046/article.html)
[152] TM Forum MTOSI Release 2.1: Supporting document SD2-5_Communication_Styles (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[153] JOSIF Guidebook (http://sourceforge.net/apps/mediawiki/openoss/index.php?title=JOSIF_Guidebook)
[154] OMG Unified Modeling Language (OMG UML), Superstructure, Version 2.3 (http://www.omg.org/spec/UML/2.3/Superstructure/PDF)
[155] TM Forum MTOSI Release 2.1: Supporting document SD0-2_Guidelines_BA (Business Agreement Guidelines) (http://www.tmforum.org/MTOSIRelease21/11998/home.html)
[156] TM Forum Business Process Framework (eTOM) Release 9 (http://www.tmforum.org/StandardsPacks/8175/home.html)
[157] NGMN TOP OPE Requirements Version 1.0
[158] NGCOR Consolidated Requirements V0.93
[159] CCITT Rec. X.733 specification
[160] CCITT Rec. X.210 | ISO/TR 8509
[161] CCITT Rec. X.710 | ISO/IEC 9595
[162] eTOM Release 9.0, GB921 Addendum D,, TM Forum, August 2010
[163] TM Forum TAM Release 4.5, TMF, April 2011
[164] SID Release 9.5, GB922 Concepts and principles, TMF, March 2011
[165] TM Forum TR143, eTOM and ITIL, Building Bridges
[166] NGMN Top OPE recommendations
[167] This concept is explained further in TM Forum document SD2-1, MTOSI Implementation Statement (see section 2.5.1, Publisher Notification Suppression).
[168] TM Forum Manage Resource Inventory - DDP BA, TMF518_MRI, Version 1.1, May 2008.
[169] TM Forum Manage Service Inventory - DDP BA, TMF518_MSI, Version 1.0, May 2008.
[170] OSS/J Inventory API, JSR-142 Overview, Release 1.0, TMF888, TM Forum Approved Version 1.3, January 2010
[171] TM Forum comparison study of OSS/J, MTOSI and 3GPP inventory interface approaches
[172] TMForum Interface Program, Inventory Interface, Progress Status at TAW Paris (Jan 2011).
[173] TM Forum Product, service and resource inventory retrieval for cloud and IT
[174] TM Forum Product, service and resource inventory update for cloud and IT
[175] in 3GPP TR 32.828 version 1.5.0
[176] 3GPP TS 32.341/2/6
[177] TMForum TR 146 Lifecycle Compatibility Release 1-0
[178] ITIL v3
[179] TM Forum, Catalog Management FDD v1.12
[180] 3GPP TS 32.171 Subscription Management

11 APPENDIX

11.1 Glossary and Abbreviations

Abbreviation	Meaning & Terms	Further explanation
2G/3G/LTE	Standards for mobile communication network and devices capabilities	
3GPP	3rd Generation Partnership Project	http://www.3gpp.org
3GPP SA5	Telecom Management group within 3GPP	http://www.3gpp.org/SA5-Telecom-Management
AAA	Authentification and Authorization & Accounting	Function providing a network service related to billing & charging system
ABR	Asynchronous Batch Response	Is a message exchange pattern. This is a multiple response pattern. The response of the first invocation returns an acknowledgement. The result set will then be sent in chunks to the service consumer (via the call back receptacle) as the data becomes available in the service producer. The consumer usually has control over the size of the chunks specified in the initial call.
ADSL	Asynchronous Digital Subscriber Line	
AFB	Asynchronous (File) Bulk Response	Is a message exchange pattern. The initial request is non-blocking and the service consumer gets notified when the transfer is completed.
AFI	Automonic Future Internet	ETSI's pre-standardization body
AKA	also known as	
AN	Asynchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
ANR	Automatic Neighbourhood Relation	
API	Application Programming Interface	
ARPU	Average Revenue Per User	Commercial KPI used in business plan
ARR	Asynchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
ASCII	American Standard Code of Information Interchange	ASCII
ASN.1	Abstract Syntax Notation One	
ASP	Application Service Provider	
ATM	Asynchronous Transfer Mode	ATM technology
B2B	Business-To-Business	
BA	Business Agreement (TM Forum)	Requirements and usage scenario specification.
BBF	Broadband Forum	http://www.broadband-forum.org
BER	Bit Error Ratio	Is the number of bit errors divided by the total number of transferred bits during a studied time interval.
BNG	Broadband Network Gateway	It's an evolution of the existing BRAS the Gatway for Fixed Access Network
BSS	Business Support Systems	Business Support Systems
CAPEX	Capital Expenditures	costs to set up/ change a network
CBE	Common Business Entity	TMF SID term

Abbreviation	Meaning & Terms	Further explanation
CCV	Common Communications Vehicle	A communication infrastructure connecting Operations Systems (e.g., CORBA platform, JMS platform)
CDR	Call Details Records	
CFS	Customer Facing Service	TMF SID term
CFSS	Customer Facing Service Specification	TMF SID term
CI	Configuration Item	ITIL term
close loop	Autonomous Operated SON Function	
CM	Configuration Management	
CMDB	Configuration Management Data Base	ITIL term
CMIP	Common Management Information Protocol	CMIP is a protocol for network management.
CMS	Configuration Management System	ITIL term
CN	Core Network	
CORBA	Common Object Request Broker Architecture	CORBA
CORBA	Common Object Request Broker Architecture	CORBA is a standard defined by the Object Management Group (OMG) that enables software components written in multiple computer languages and running on multiple computers to work together.
COTS	Commercial Off the Shelf	COTS
CPE	Customer Premises Equipment	
CRUD	Create, Read, Update, Delete	
csv	Comma Separated Value	
CTK	Compliance Test Kit	Part of TM Forum interface specification.
DDP	Document Delivery Package	The MTOSI interface specification is structured in DDPs based on eTOM level 2/3 processes.
DSLAM	Digital Subscriber Line Access Multiplexer	
DT	Deutsche Telekom (Operator)	
e2e	end-to-end	
EM	Element Management	EM
EMS	Element Management System	EMS
eNB	Enhanced NodeB	
EPC	Evolved Packet Core	Mobile Core Network for 4G
eTOM	Enhanced Telecommunication Operations Map	eTOM
ETSI	European Telecommunications Standards Institute (SDO)	
FAB	Fullfillment, Assurance and Billing	
FCAPS	Fault, Configuration, Assurance, Performance	FCAPS
FDD	Feature Description Document	TMF concept
FIM	Federated Information Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Information Model part of these models contains the static data; i.e., the object classes with their attributes and the content of the notifications."

Abbreviation	Meaning & Terms	Further explanation
FM	Fault Management	Fault Management
FMC	Fixed Mobile Convergence	http://en.wikipedia.org/wiki/Fixed-mobile_convergence
FOM	Federated Operations Model	A Federated Model is the aggregation of all models used in the Fixed Mobile Converged (FMC) environment. The Operations Model part of these models contains the dynamics; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the FIM through the management interfaces.
FRU	Field Replaceable Unit	
FT IRP	File Transfer Integration Reference Point	
GDMO	Guidelines for the Definition of Managed Objects	GDMO is a specification for defining managed objects of interest to the Telecommunications Management Network for use in CMIP.
GEN	Generic Next Generation Operational Requirements	
GPON	Gigabit-capable Passive Optical Network	
GWCN	Gateway Core Network	A variant of core network sharing model
HLR	Home Location Register	
HO	handover	
HSS	Home Subscribe Server	It's an evolution of the current HLR used as a location server for 2G/3G networks
HTTP	Hyper Text Transfer Protocol	
HW	Hardware	Hardware
IA	Information Agreement (TM Forum)	UML model specification
IDL	Interface Definition Language	OMG IDL
IETF	Internet Engineering Task Force (SDO)	IETF
IIS	Interface Implementation Specification (TM Forum)	Protocol specification; e.g., using XML or CORBA
IM	Information Management	
IMS	IP Multimedia Subsystem	http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem
InvM	Inventory Management	
IP	Internet Protocol	http://en.wikipedia.org/wiki/Internet_Protocol
IPR	Intellectual Property Rights	
IRP	Integration Reference Point (3GPP term)	3GPP 32.103
ISG	Industry Specification Group	ETSI's pre-standardization instrument
ITIL	Information Technology Infrastructure Library	
itSMF	IT Service Management Forum	
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector (SDO)	ITU-T
JMS	Java Message Service	JMS is a Java Message Oriented Middleware API for sending messages between two or more clients.
JPA	Java Persistence API	JPA is a Java programming language framework managing relational data in applications using a Java Platform.
JVT	Java Value Types	
LCC	Lower Camel Case	An approach to indicate word boundaries using medial

Abbreviation	Meaning & Terms	Further explanation
		capitalization, thus rendering "two words" as "twoWords". This convention is commonly used in Java.
LTE	Long Term Evolution	http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution
MEF	Metro Ethernet Forum (SDO)	MEF
MEP	Message Exchange Pattern	The combination of a communication pattern and a communication style which fully identifies the messages and the choreography (sequencing and cardinality) of messages through a management interface.
MME	Mobility Management Entity	
MMS	Multimedia Messaging Service	
MO	Managed Object	Managed_object
MOCN	Multi-Operator Core Network	Model of Network sharing which does not share the Core Networks
MOM	Message Oriented Middleware	
MORAN	Multi-Operator Radio Access Network	A model of Network sharing at Radio access level
MPLS	Multi Protocol Label Switching	MPLS
MRI	Manage Resource Inventory	
MSI	Manage Service Inventory	
MT	Modelling and Tooling	Project sub stream of NGCOR
MTNM	Multi Technology Network Management	
MTOSI	Multi Technology OS interface	TM Forum interface product. It is an XML-based Operations System (OS)-to-OS interface suite. The Network Management System-to-Element Management System communication is also covered as a special case.
MVNE	Mobile Virtual Network Environment	
MVNO	Mobile Virtual Network Operator	
MW	Management World	TM Forum event
MW	TM Forum Management World	
NE	Network Element	Network_element
NBI	Northbound Interface	Interface between EMS and NMS
NGCOR	Next Generation Converged Operations Requirements	NGMN project
NGMN	Next Generation Mobile Network	http://www.ngmn.org
NGN	Next Generation Network	http://en.wikipedia.org/wiki/Next_Generation_Networking
NGOSS	Next Generation Operation Systems and Software	
NM	Network Management	Network_management
NMS	Network Management System	Network_management_system
NOC	Network Operation Centre	
NRM	Network Resource Model (3GPP)	Contains the static data of an interface specification.
O	Orange (Operator)	
OA&M	Operation, Administration & Maintanance	OA&M
OC	Operating Committee (NGMN)	

Abbreviation	Meaning & Terms	Further explanation
OCL	Object Constraint Language	OCL is a declarative language for describing rules that apply to Unified Modeling Language (UML) models.
OPE	Operational Efficiency	Requirements specification from NGMN.
OPEX	Operational Expenditures	Costs of running a network
OS&R	Operation, Support and Readiness	Is a Level 1 process grouping of the Business Process Framework. OS&R contains processes for ensuring operational readiness in the fulfillment, assurance and billing areas.
OSA	Open Services Access	
OSS	Operations Support System	Operations_support_system
OSSJ	OSS through Java	
PBB-TE	Provider Backbone Bridges - Traffic Engineering	
PCC	Policy Charging and Control	
PCRF	Policy and Charging Rules Function	It's a functional block in the EPC network architecture for charging & Policy
PDF	Portable Document Format	
PDH	Plesiochronous Digital Hierarchy	
PM	Performance Management	http://en.wikipedia.org/wiki/FCAPS
PT	Portugal Telecom (operator)	
QoS	Quality of Service	QoS
RAM	Resource Alarm Management	Used as an abbreviation for the FM Interface specification workstream of the TMForum
RAN	Radio Access Network	http://en.wikipedia.org/wiki/Radio_access_network
RAT	Radio Access Technology	
RFS	Resource Facing Service	
RFSS	Resource Facing Service Specification	
RI	Reference Implementation	Part of TM Forum interface specification.
Rinv	Resource Inventory	
RM	Resource Mangement	
RM&O	Resource Management & Operations	
RPC	Remote Procedure Call	RPC is an inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction.
SACM	Service Asset and Configuration Management	
SDH	Synchronous Digital Hierarchy	SDH technology
SDO	Standards Developing Organisation	All committes, fora and partnerships that create standards, recommendations and technical reports.
SecM	Security Management	
SFB	Synchronous (File) Bulk Response	Is a message exchange pattern. The service consumer requests a response set to be uploaded to a storage server and the blocking call returns when the transfer is complete.
S-GW	Serving Gateway	

Abbreviation	Meaning & Terms	Further explanation
SI&P	Strategy, Infrastructure & Product	
SID	Shared Information & Data model (TM Forum)	http://www.tmforum.org/InformationFramework/1684/home.html
SIT	Synchronous Iterator	Is a message exchange pattern. This is a multiple response pattern. This is the classical Iterator design pattern. The response of the first invocation returns a partial data set as well as a pointer to an Iterator interface. The service consumer will then invoke the Iterator to receive the subsequent result data set partitions. The consumer has control of the flow, the service provider needs to maintain the state related to the pending Iterator.
SLA	Service Level Agreement	KPI describing user requirements tro be translated into QOS objective at operator side within an agreement
SM	Security Management	http://en.wikipedia.org/wiki/FCAPS
SM&O	Service Management &Operations	
SN	Synchronous Notification	Is a message exchange pattern. It facilitates the dissemination of notifications.
SNMP	Simple Network Management Protocol	SNMP is an "Internet-standard protocol for managing devices on IP networks"
SOA	Service Oriented Architecture	Service-oriented_architecture
SOAP	Simple Object Access Protocol	
SON	Self Organizing Network	
SONET	Synchronous Optical Network	SONET
SP	Service Provider	Company, which provides access to telephone and related communications services
SPR	Subscription Profile Repository	It's a data base for user profiles
SQM	Service Quality Management	eTOM definition: "SQM encompasses monitoring, analyzing and controlling the performance of the service perceived by customers"
SRR	Synchronous Request/Reply	Is a message exchange pattern. This is a simple response pattern involving a request/reply with a single result message.
SuM	Subscription Management	
SW	Software	Software
TA	Tracking Area	
TAM	Telecom Appplications Map	TMF term
TMF	TM Forum	www.tmforum.org
TWG SC	Technical Working Group Steering Committee	NGMN group
UCC	Upper Camel Case	An approach to indicate word boundaries using medial capitalization, thus rendering "two words" as "TwoWords". This convention is commonly used in Java.
UDC	User Data Convergence	Evolution of unified data bases
UE	User Equipment	
UML	Unified Modelling Language	UML
UMTS	Universal Mobile Telecommunication System	UMTS
USIM	Universal Subscriber Identity Module	
VF	Vodafone (operator)	

Abbreviation	Meaning & Terms	Further explanation
WDM	Wavelength Division Multiplexing	WDM
WiMax	Worldwide Interoperability for Microwave Access	WiMAX
WLAN	Wireless Local Area Network	WLAN
WS	Web Service	Web Services
WSDL	Web Service Description Language	WSDL
XMI	XML Metadata Interchange	http://en.wikipedia.org/wiki/XMI
XML	Extensible Markup Language	XML
Xpath	XML Path Language	XPATH is a query language for selecting nodes from an XML document.
XSD	XML Schema	XSD
	alarm interface	An interface which transports alarm - informations between OSS systems
	Business Services	These are the operations in TM Forum terminology.
	Business Use Case	High level uses case driven by a business scenario.
	common architecture	All interfaces should be part of a common architecture
	Common Core Network	Business architecture Scenario
	Common Information Model	This term is used to reference information models like TMForum SID
	Communication Partners	OSS systems, which exchange information
	Converged Framework Model	Harmonised design guidelines for tooling.
	cross-domain	Cross mobile and fixed domains
	cross-domain	Cross mobile and fixed domains
	Domain	Related to the partioning of the network
	Dynamic Requirement	Requirements which describe the operations part of the management interface.
	Element Management Layer	EMS level in layering architecture
	Element Manager	Element_Manager
	EMS (server)	The SW component which implements the interface in the OSS systems, which delivers a service to other OSS systems
	EMS-OSS layer	Summary of all OSS systems which deliver an EMS functionality
	eNodeB	Base Station for LTE
	entity	An entity is some tangible or conceptual thing , entity word is typically used when presenting things without a real name name or label. Entities are characterized by attributes and relationships.
	EPC Network	Mobile Core Network for 4G
	federated information / data model	See sub-task MT
	Federated Model	see Operations Model
	Federated Network Resource Model	see Operations Model
	femtoCell	Home NodeBB (Base Station deployed in the Home)
	implementation technology	Technology used to implement a functionality
	Infrastructure Domain	

Abbreviation	Meaning & Terms	Further explanation
	Interfacing / Integration	
	inventory component	An instance of the objects in an inventory database
	logical resource	Logical resources are e.g., subnetwork connection, topological link, termination point etc..
	management architecture	Defines the architecture between Operations Systems and the between Operations Systems and the network.
	management area	These are e.g., alarm management, inventory, performance management etc..
	Management Interface	An instance of an interface between two OSes used for management.
	Management Model	Generic term for information model and operations model.
	management operation	Operations executed via the management interface.
	management recommendations	ITU-T standards are called Recommendations.
	management workflows	Specific sequence of operations executed via the management interface.
	multi-domain network	Domains are e.g., access, metro, backhaul, core.
	multi-technology network	Technologies are e.g., ATM, OTN, SDH, Ethernet, DSL, LTE, 2G, 3G, HSPA.
	Network Abstraction Layer	A logical layer between the network and the management layer which relay an abstracted view (from management point of view) of the network.
	network data	Data which describes - from management point of view - the underlying network in an abstract way. This data can be used by all different management areas.
	Network Level Interface	An interface which is able to provide an end-to-end view of the underlying network.
	network level management	A management function which is able to manage an end-to-end view of the underlying network.
	Network Operator	Company, which provides access to telephone and related communications services
	Network Resource Model	Data model representing the equipment of a network. It's 3GPP terminology
	network technology	For Mobile , it means 2G, 3G or 4G
	network type	The type of the network (e.g. UMTS- Radio, DWH, IP, etc. ..)
	NGOSS concepts	Concepts (like eTOM, SID, etc…) which are summarized within the "Next Generation Operation Support Systems" - concept of the TMForum
	NMS (client)	The SW component which implements the interface in the OSS systems, which requests a service from another OSS system.
	OA&M functional domain	It refers to ITU-T "FCAPS"
	open loop	Operator controlled SON function
	Operations Model	Contains the dynamic part of the model; i.e., operations (and their parameters) grouped in service interfaces which allow the transport of the data defined in the information model through the management interfaces.
	Operator	Role, responsible for the management of a network and/or service
	operator-wide OSS application	Applications developed by the operator to ensure FM, PM, CM,

Abbreviation	Meaning & Terms	Further explanation
	OSS application	An application which delivers a capability dedicated to the OSS domain
	OSS environment	
	OSS Interface	Interface between OSS systems
	physical resource	Physical resources are e.g., network elements, cables, fibres etc..
	primitive	Simplest element provided by a programming language
	resource	Resource is any physical or virtual component of a telecommunications network
	Resource Configuration Management	TMForum TAM definition: "The Resource Configuration Management application generates a resource plan to fulfill a resource order."
	Resource Fault Management	TMForum TAM definition: "Fault Management applications are responsible for the management of faults, or troubles, associated with the service provider's resources. "
	resource management layer	Covers all Resource Management processes as defined in the TM Forum Business Process Framework (eTOM) "Resource Management & Operations" (RM&O) layer within the operations & support, fulfillment, and assurance verticals. This process grouping maintains knowledge of resources (application, computing and network infrastructures) and is responsible for managing all these resources.(e.g. networks, IT systems, servers, routers, etc.) utilized to deliver and support services required by customers.
	service catalogue	Storage of all service specifications and instances
	service configuration and activitation	Operator process dealing with delivery
	Service Inventory	TMForum TAM definition: Service Inventory represents the applications which contain and maintain information about the instances of services in a telecom organization
	service management layer	Covers all Service Management processes as defined in the TM Forum Business Process Framework (eTOM) "Service Management & Operations" (SM&O) layer within the operations & support, fulfilment, and assurance verticals. This process grouping focuses on the knowledge of services (Access, Connectivity, Content, etc.) and includes all functionalities necessary for the management and operations of communications and information services required by customers.
	service platform	A resource, which delivers a telecommunication service
	service type	The type of a service (e.g. MMS or SMS - Service)
	shared network	Generic term which includes different model sharing (at core, access network)
	type acceptance	Type Acceptance is the process of verifying that a certain product has passed performance tests and quality assurance tests or qualification requirements stipulated in contracts, regulations, or specifications.
	Umbrella Model	Part of the model containing artefacts that can be used/inherited in both wireline and wireless network models.
	Usage Scenario	TMF term for "use case"; are defined for each required operation
	Use Case	It refers to Business architecture scenarios and Generic & Basic architecture scenarios

11.2 The NGCOR Requirements and their Addressees

The following chapters summarize the requirements that have been elaborated and collected per substream of the NGCOR project and show the addressees of these requirements.

11.2.1 Generic Requirements

GEN	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-GEN (1)	X	X	X
REQ-GEN (2)	X		
REQ-GEN (3)	X		
REQ-GEN (4)	X		
REQ-GEN (5)	X		
REQ-GEN (6)	X		
REQ-GEN (7)	X		
REQ-GEN (8)	X		
REQ-GEN (9)	X		
REQ-GEN (10)	X		
REQ-GEN (11)	X		
REQ-GEN (12)	X		
REQ-GEN (13)	X		
REQ-GEN (14)	X		
REQ-GEN (15)	X		
REQ-GEN (16)	X	X	X
REQ-GEN (17)	X	X	X
REQ-GEN (18)	X		
REQ-GEN (19)	X		
REQ-GEN (20)	X	X	X
REQ-GEN (21)	X	X	
REQ-GEN (22)	X		

Table 11-1: Generic Requirements - Whom these requirements are addressed to

11.2.2 CON Requirements

CON	Addressee / Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-CON (1)	X	X	
REQ-CON (2)	X	X	
REQ-CON (3)	X	X	
REQ-CON (4)	X	X	
REQ-CON (5)	X	X	
REQ-CON (6)			X
REQ-CON (7)	X		
REQ-CON (8)			X
REQ-CON (9)	X		
REC-CON (10)	X		

Table 11-2: Converged Operations Requirements - Whom these requirements are addressed to

11.2.3 MT Requirements

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (1)	X		
REQ-MT (2)	X		
REQ-MT (3)	X		
REQ-MT (4)	X		
REQ-MT (5)	X		
REQ-MT (6)	X		
REQ-MT (7)	X		
REQ-MT (8)	X		
REQ-MT (9)	X		
REQ-MT (10)	X	X	X
REQ-MT (11)	X		
REQ-MT (12)	X		
REQ-MT (13)	X		
REQ-MT (14)	X		
REQ-MT (15)	X	X	X
REQ-MT (16)	X		
REQ-MT (17)	X		
REQ-MT (18)	X		
REQ-MT (19)	X		
REQ-MT (20)	X		
REQ-MT (21)	X		
REQ-MT (22)	X		
REQ-MT (23)	X		
REQ-MT (24)	X		
REQ-MT (25)	X		
REQ-MT (26)	X		
REQ-MT (27)	X		
REQ-MT (28)	X		
REQ-MT (29)	X		
REQ-MT (30)	X		
REQ-MT (31)	X		
REQ-MT (32)	X		
REQ-MT (33)	X		
REQ-MT (34)	X		
REQ-MT (35)	X		
REQ-MT (36)	X		
REQ-MT (37)	X		
REQ-MT (38)	X		
REQ-MT (39)	X		
REQ-MT (40)	X		
REQ-MT (41)	X	X	X
REQ-MT (42)	X	X	X

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (43)	X		
REQ-MT (44)	X		
REQ-MT (45)	X	X	X
REQ-MT (46)	X		
REQ-MT (47)	X		
REQ-MT (48)	X		
REQ-MT (49)	X		
REQ-MT (50)	X		
REQ-MT (51)	X		
REQ-MT (52)	X	X	X
REQ-MT (53)	X		
REQ-MT (54)	X		
REQ-MT (55)	X		
REQ-MT (56)	X		
REQ-MT (57)	X		
REQ-MT (58)	X		
REQ-MT (59)	X		
REQ-MT (60)	X		
REQ-MT (61)	X		
REQ-MT (62)	X		
REQ-MT (63)	X		
REQ-MT (64)	X		
REQ-MT (65)	X		
REQ-MT (66)	X		
REQ-MT (67)	X		
REQ-MT (68)	X		
REQ-MT (69)	X		
REQ-MT (70)	X		
REQ-MT (71)	X		
REQ-MT (72)	X		
REQ-MT (73)	X		
REQ-MT (74)	X		
REQ-MT (75)	X		
REQ-MT (76)	X		
REQ-MT (77)	X		
REQ-MT (78)	X		
REQ-MT (79)	X		
REQ-MT (80)	X		
REQ-MT (81)	X	X	X
REQ-MT (82)	X	X	X
REQ-MT (83)	X	X	X
REQ-MT (84)	X	X	X
REQ-MT (85)	X	X	X
REQ-MT (86)	X	X	X
REQ-MT (87)	X	X	X
REQ-MT (88)	X	X	X

MT	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-MT (89)	X	X	X
REQ-MT (90)	X	X	X
REQ-MT (91)	X	X	X
REQ-MT (92)	X	X	X
REQ-MT (93)	X	X	X
REQ-MT (94)	X	X	X
REQ-MT (95)	X	X	X
REQ-MT (96)	X	X	X
REQ-MT (97)	X	X	X
REQ-MT (98)	X	X	X
REQ-MT (99)	X	X	X
REQ-MT (100)	X	X	X
REQ-MT (101)	X	X	X
REQ-MT (102)	X	X	X
REQ-MT (103)	X	X	X
REQ-MT (104)	X	X	X
REQ-MT (105)	X	X	X
REQ-MT (106)	X	X	X
REQ-MT (107)	X	X	X
REQ-MT (108)	X	X	X
REQ-MT (109)	X	X	X
REQ-MT (110)	X	X	X

Table 11-3: Modelling & Tooling Requirements - Whom these requirements are addressed to

11.2.4 FM Requirements

FM	Addressee/ Receiver of Requirement		
	SDOs & Organisations	Equipment Vendors	OSS Vendors
REQ-FM (1)	X		
REQ-FM (2)	X		
REQ-FM (3)	X		
REQ-FM (4)	X		
REQ-FM (5)	X		
REQ-FM (6)	X		
REQ-FM (7)	X	X	
REQ-FM (8)	X		X
REQ-FM (9)	X	X	X
REQ-FM (10)	X	X	
REQ-FM (11)	X	X	X
REQ-FM (12)	X	X	
REQ-FM (13)	X		X

Table 11-4: Fault Management Requirements - Whom these requirements are addressed to

11.2.5 InvM Requirements

InvM	Addressee / Receiver of Requirement		
	SDOs & Organsations	Equipment Vendors	OSS Vendors
REQ-InvM (1)			X
REQ-InvM (2)			X
REQ-InvM (3)			X
REQ-InvM (4)			X
REQ-InvM (5)			X
REQ-InvM (6)			X
REQ-InvM (7)			X
REQ-InvM (8)			X
REQ-InvM (9)			X
REQ-InvM (10)	X	X	X
REQ-InvM (11)	X	X	X
REQ-InvM (12)	X		X
REQ-InvM (13)	X		X
REQ-InvM (14)	X		X
REQ-InvM (15)			X
REQ-InvM (16)	X		X
REQ-InvM (17)	X		X
REQ-InvM (18)	X		X
REQ-InvM (19)	X		X
REQ-InvM (20)	X		X
REQ-InvM (21)	X	X	X
REQ-InvM (22)	X		X
REQ-InvM (23)	X		X
REQ-InvM (24)	X		X
REQ-InvM (25)	X		X
REQ-InvM (26)	X		X
REQ-InvM (27)	X		X
REQ-InvM (28)	X		X
REQ-InvM (29)	X		X
REQ-InvM (30)	X		X
REQ-InvM (31)	X		X
REQ-InvM (32)	X		X
REQ-InvM (33)	X		X
REQ-InvM (34)			X
REQ-InvM (35)			X
REQ-InvM (36)			X
REQ-InvM (37)	X		X
REQ-InvM (38)	X	X	X
REQ-InvM (39)	X		X
REQ-InvM (40)		X	X
REQ-InvM (41)			X
REQ-InvM (42)	X		X

REQ-InvM (43)			X
REQ-InvM (44)			X
REQ-InvM (45)			X
REQ-InvM (46)			X
REQ-InvM (47)	X		X
REQ-InvM (48)	X		X
REQ-InvM (49)			X
REQ-InvM (50)	X		X
REQ-InvM (51)	X		X
REQ-InvM (52)	X		X
REQ-InvM (53)			X
REQ-InvM (54)			X
REQ-InvM (55)	X	X	X
REQ-InvM (56)	X	X	X
REQ-InvM (57)	X	X	X
REQ-InvM (58)	X		X
REQ-InvM (59)	X		X
REQ-InvM (60)			X
REQ-InvM (61)			X
REQ-InvM (62)			X
REQ-InvM (63)	X		X
REQ-InvM (64)	X		X
REQ-InvM (65)			X
REQ-InvM (66)			X
REQ-InvM (67)			X
REQ-InvM (68)			X
REQ-InvM (69)		X	X

Table 11-5: Inventory Management Requirements - Whom these requirements are addressed to