3GPP TR 28.805 V16.1.0 (2019-12)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Telecommunication management;

Study on management aspects of communication services

(Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

.

Keywords

Management,communication, services

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [6](#__RefHeading___Toc27497532)

Introduction [7](#__RefHeading___Toc27497533)

1 Scope [8](#__RefHeading___Toc27497534)

2 References [8](#__RefHeading___Toc27497535)

3 Definitions of terms, symbols and abbreviations [8](#__RefHeading___Toc27497536)

3.1 Terms [8](#__RefHeading___Toc27497537)

3.2 Symbols [9](#__RefHeading___Toc27497538)

3.3 Abbreviations [9](#__RefHeading___Toc27497539)

4 Concepts and background [9](#__RefHeading___Toc27497540)

4.1 Types of communication services [9](#__RefHeading___Toc27497541)

4.2 Management aspects of communication services [10](#__RefHeading___Toc27497542)

4.2.1 Customer, service and resource views [10](#__RefHeading___Toc27497543)

4.2.2 Communication service management function [10](#__RefHeading___Toc27497544)

4.2.3 Lifecycle of communication service [11](#__RefHeading___Toc27497545)

4.2.4 Relation of CSI lifecycle to NSI lifecycle [12](#__RefHeading___Toc27497546)

4.2.4.0 Introduction [12](#__RefHeading___Toc27497547)

4.2.4.1 CSI LCM operation triggering NSI creation [12](#__RefHeading___Toc27497548)

4.2.4.2 CSI LCM operation triggering NSI modification [13](#__RefHeading___Toc27497549)

4.2.4.3 CSI LCM operation triggering NSI activation and deactivation [13](#__RefHeading___Toc27497550)

4.2.5 Performance assurance of communication services [13](#__RefHeading___Toc27497551)

4.3 Management layers [14](#__RefHeading___Toc27497552)

4.4 Management model [15](#__RefHeading___Toc27497553)

4.4.1 Introduction [15](#__RefHeading___Toc27497554)

4.4.2 Description [15](#__RefHeading___Toc27497555)

4.4.3 Communication services applied to network slicing [16](#__RefHeading___Toc27497556)

4.5 Communication services [17](#__RefHeading___Toc27497557)

4.5.1 Introduction [17](#__RefHeading___Toc27497558)

4.5.2 GSMA GST/NEST [17](#__RefHeading___Toc27497559)

4.6 SLS assurance [17](#__RefHeading___Toc27497560)

4.6.1 Description [17](#__RefHeading___Toc27497561)

4.6.2 Management cooperation with 5GC and NG-RAN [18](#__RefHeading___Toc27497562)

4.7 Service QoE [18](#__RefHeading___Toc27497563)

4.7.1 Description [18](#__RefHeading___Toc27497564)

4.7.2 Service QoE collection and service quality assurance [18](#__RefHeading___Toc27497565)

5 Potential use cases and requirements [19](#__RefHeading___Toc27497566)

5.1 Management data analytics and automated service assurance [19](#__RefHeading___Toc27497567)

5.1.1 Service quality assurance and optimization of the services [19](#__RefHeading___Toc27497568)

5.1.1.1 Description [19](#__RefHeading___Toc27497569)

5.1.1.2 Potential requirements [19](#__RefHeading___Toc27497570)

5.1.2 CSI monitoring [19](#__RefHeading___Toc27497571)

5.1.2.1 Description [19](#__RefHeading___Toc27497572)

5.1.2.2 Potential requirements [20](#__RefHeading___Toc27497573)

5.1.3 SLS monitoring for network slicing [20](#__RefHeading___Toc27497574)

5.1.3.1 Description [20](#__RefHeading___Toc27497575)

5.1.3.2 Potential requirements [20](#__RefHeading___Toc27497576)

5.1.4 MDA-Assisted network provisioning contributing to SLS assurance [21](#__RefHeading___Toc27497577)

5.1.4.1 Description [21](#__RefHeading___Toc27497578)

5.1.4.2 Potential requirements [21](#__RefHeading___Toc27497579)

5.2 Lifecycle management [21](#__RefHeading___Toc27497580)

5.2.1 Communication service instances realized in a single network slice instance [21](#__RefHeading___Toc27497581)

5.2.1.1 Description [21](#__RefHeading___Toc27497582)

5.2.1.2 Potential requirements [22](#__RefHeading___Toc27497583)

5.2.2 Remove a communication service instance from a network slice instance [22](#__RefHeading___Toc27497584)

5.2.2.1 Description [22](#__RefHeading___Toc27497585)

5.2.2.2 Potential requirements [22](#__RefHeading___Toc27497586)

5.2.3 Management aspects of NSIs utilized by multiple communication services [23](#__RefHeading___Toc27497587)

5.2.3.1 Description [23](#__RefHeading___Toc27497588)

5.2.3.2 Potential requirements [23](#__RefHeading___Toc27497589)

5.2.4 Obtaining an NSI as an NOP Internal to provide multiple CSIs [23](#__RefHeading___Toc27497590)

5.2.4.1 Description [23](#__RefHeading___Toc27497591)

5.2.5 Providing CSI management capability to vertical industries [23](#__RefHeading___Toc27497592)

5.2.5.1 Description [23](#__RefHeading___Toc27497593)

5.2.6 Create a Communication Service (CSI) [24](#__RefHeading___Toc27497594)

5.2.6.1 Description [24](#__RefHeading___Toc27497595)

5.2.6.2 Potential requirements [24](#__RefHeading___Toc27497596)

5.2.7 Activate a Communication Service (CSI) [24](#__RefHeading___Toc27497597)

5.2.7.1 Description [24](#__RefHeading___Toc27497598)

5.2.7.2 Potential requirements [24](#__RefHeading___Toc27497599)

5.2.8 De-activate a Communication Service (CSI) [24](#__RefHeading___Toc27497600)

5.2.8.1 Description [24](#__RefHeading___Toc27497601)

5.2.8.2 Potential requirements [25](#__RefHeading___Toc27497602)

5.2.9 Modify a Communication Service (CSI) [25](#__RefHeading___Toc27497603)

5.2.9.1 Description [25](#__RefHeading___Toc27497604)

5.2.9.2 Potential requirements [25](#__RefHeading___Toc27497605)

5.2.10 Terminate a Communication Service (CSI) [25](#__RefHeading___Toc27497606)

5.2.10.1 Description [25](#__RefHeading___Toc27497607)

5.2.10.2 Potential requirements [25](#__RefHeading___Toc27497608)

5.2.11 Management of multi-party communication service [25](#__RefHeading___Toc27497609)

5.2.11.1 Description [25](#__RefHeading___Toc27497610)

5.2.11.2 Potential requirements [26](#__RefHeading___Toc27497611)

5.3 Lifecycle management, data analytics and automated service assurance [26](#__RefHeading___Toc27497612)

5.3.1 Service management aspects of NSaaS [26](#__RefHeading___Toc27497613)

5.3.1.1 Description [26](#__RefHeading___Toc27497614)

5.3.1.2 Potential requirements [27](#__RefHeading___Toc27497615)

6 Potential solutions [27](#__RefHeading___Toc27497616)

6.1 Solution for communication service instances realized in a single network slice instance [27](#__RefHeading___Toc27497617)

6.2 Solution for translation of SLS into SLS requirements [28](#__RefHeading___Toc27497618)

6.3 Solution for communication service instance termination [29](#__RefHeading___Toc27497619)

6.3.1 Solution for the case that network slice used as resources [29](#__RefHeading___Toc27497620)

6.4 Solution for communication service instance modification [29](#__RefHeading___Toc27497621)

6.4.1 Solution for the case that network slice used as resources [29](#__RefHeading___Toc27497622)

6.5 Solution for communication service instance activation [30](#__RefHeading___Toc27497623)

6.5.1 Solution for the case that network slice used as resources [30](#__RefHeading___Toc27497624)

6.6 Solution for communication service instance de-activation [30](#__RefHeading___Toc27497625)

6.6.1 Solution for the case that network slice used as resources [30](#__RefHeading___Toc27497626)

6.7 Solution for MDA-Assisted SLS assurance [30](#__RefHeading___Toc27497627)

6.7.1 MDA-Assisted network optimization [30](#__RefHeading___Toc27497628)

6.8 Solution for providing management capability to vertical industries [32](#__RefHeading___Toc27497629)

6.9 Solution for management aspects of NSI utilized by multiple communication services. [33](#__RefHeading___Toc27497630)

6.9.1 Assignment of communication service to an existing NSI [33](#__RefHeading___Toc27497631)

6.9.2 Activation of CSI sharing NSI. [33](#__RefHeading___Toc27497632)

6.9.3 Termination of CSI sharing NSI. [33](#__RefHeading___Toc27497633)

7 Conclusions and recommendations [34](#__RefHeading___Toc27497634)

7.1 Conclusions [34](#__RefHeading___Toc27497635)

7.1.1 Introduction [34](#__RefHeading___Toc27497636)

7.1.2 Lifecycle management of communication services [34](#__RefHeading___Toc27497637)

7.1.3 Management data analytics [34](#__RefHeading___Toc27497638)

7.1.4 SLS assurance [34](#__RefHeading___Toc27497639)

7.2 Recommendations [35](#__RefHeading___Toc27497640)

7.2.1 Lifecycle management of communication services [35](#__RefHeading___Toc27497641)

7.2.2 SLS assurance solution [35](#__RefHeading___Toc27497642)

7.2.3 Management data analytics in the SON context [35](#__RefHeading___Toc27497643)

7.2.4 Management of MDAF [35](#__RefHeading___Toc27497644)

Annex A: Comparison table between 3GPP ServiceProfile attributes and GSMA GST attributes [36](#__RefHeading___Toc27497645)

Annex B: Change history [42](#__RefHeading___Toc27497646)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, certain modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" shall not to be used as substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

With the recent introduction of a service based management architecture for management of mobile networks [2], a service provider or network operator can manage 5G networks including network slicing, using management services. The next level of management is to manage the communication services provided by the network. The present document studies the use of a service based management architecture for management of communication services.

# 1 Scope

The present document specifies potential use cases, requirements and solutions (from the perspective of services based management architecture) for the management of communication services. The document provides conclusions and recommendations on the next steps in the standardization.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[3] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

[4] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[5] 3GPP TR 28.801: "Study on management and orchestration of network slicing for next generation network".

[6] 3GPP TR 23.791: "Study of Enablers for Network Automation for 5G".

[7] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[8] 3GPP TS 28.531: "Management and orchestration; Provisioning; Stage 1".

[9] TMN M.3010: "Principles for a telecommunications management network" M.3010 (02/00).

[10] 3GPP TS 28.404: "Telecommunication management; Quality of Experience (QoE) measurement collection; Concepts, use cases and requirements".

[11] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[12] GSMA Official Document NG.116 "Generic Network Slice Template Version 1.0 May 2019".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**communication services**: subset of 3GPP defined services. Examples of 3GPP services (e.g. 5G LAN) can be found in TS 22.261.

**communication service instance:** run-time construct of a communication service for a defined group of users

**service level specification**: specification of the minimum acceptable standard of service

**SLA requirements**: service and network requirements derived from SLAs.

NOTE: A provider may add additional requirements not directly derived from SLA's, associated to provider internal [business] goals.

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CFCS Customer Facing Communication Service

CS Communication Service

CSC Communication Service Customer

CSMF Communication Service Management Function

CSP Communication Service Provider

NMF Network Management Function

NSaaS NetworkSlice as a Service

NSI Network Slice Instance

NSMF Network Slice Management Function

RFCS Resource Facing Communication Service

SLA Service Level Agreement

SLS Service Level Specification

# 4 Concepts and background

## 4.1 Types of communication services

Communication Service (CS) is offered by a communication service provider to its customers to fulfil their requested communication service requirements. The types of communication service customers include B2B, B2C, B2H and B2B2X, see clause 4.1.2 of TS 28.530 [3]. A communication service can be provided as an end-user service or as a business service [3].

Communication services offered by Communication Service Providers (CSPs) to Communication Service Customers (CSCs) are of various categories. Communication services can be classified from different dimension views according to the purpose of classification.

To investigate different business models or different roles involved from business models perspective, using types of service consumers as the service classification criteria, communication services can be classified as business to consumer (B2C) services, business to business (B2B) services, business to household (B2H) services and business to business to everything (B2B2X) services, see clause 4.1.2 of TS 28.530 [3]. Two business models as "Network Slice as a Service (NSaaS)" and "Network Slices as NOP internals" are documented in clauses 4.1.6 and 4.1.7 of TS 28.530 [3].

Examples of the categories of communication services from performance requirements perspective, are eMBB, URLLC and MIoT, see clause 4.1.4 of TS 28.530 [3].

- EMBB service type aims at supporting performance requirements of high data rates and high traffic densities, see Table 7.1-1 "Performance requirements for high data rate and traffic density scenarios" of TS 22.261 [4].

- URLLC service type aims at supporting performance requirements of low-latency and high-reliability, see Table 7.2.2-1 "Performance requirements for low-latency and high-reliability services" of TS 22.261 [4].

- MIoT service type aims at supporting performance requirements of large number and high density of IoT devices, see clause 4 of TS 22.261 [4].

## 4.2 Management aspects of communication services

### 4.2.1 Customer, service and resource views

A communication service can be described from the perspective of a customer that orders and consumes the communication service and from the perspective of a CSP that offers and provides the communication service.

A communication service can be realized by the instantiation of a communication service, based on communication service description(s) with the information applicable to the communication service instance. The communication service information is mapped to resource information to realize the communication service.

### 4.2.2 Communication service management function

The CSMF is described in [5] and involves provisioning and management of communication service instances. Part of his role is to request the necessary resources to realize the communication service instances. The request for the resources includes service specific instance information to be used by the resource management to realize the communication service instance.

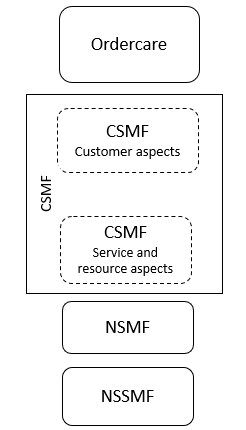


Figure 4.2.2.1: Customer aspects as well as, service and resource aspects regarding CSMF

The CSMF is split into two parts where one of them is related to customer aspects and the other is related to the service and resource aspects. Figure 4.2.2.2 depicts the CSMF functionalities.

Service Design

Service SLA

Input/Translation

Service

Catalogue

Capability Exposure

CFCS

CSI Resource Inventory

CSI LCM

Fault Supervision of CSI

Performance Assurance of CSI

RFCS

CSMF

Ordercare

CSC

Figure 4.2.2.2: CSMF functionalities

CFCS aspect provides the following functions and services:

- **Service Design**: It defines parameters for service provisioning, including parameter name, parameter type, allowed value and range of the service parameters and so on.

- **Service SLA Input and Translation**: It receives service SLA from CSC and translates the SLA into resource aspect related requirements, e.g. service profile for the instantiation of network slice instance.

- **Service Catalogue**: It stores the service profile information which represents the communication service type and capability.

- **Capability exposure**: It handles exposure of communication service management capability to CSC, e.g. communication service instance performance monitoring.

RFCS aspect manages the resource aspects of the communication service instance (CSI). RFCS aspect provides the following functions and services:

- **CSI resource inventory**: It stores the identifications of the CSI resources (e.g. CSI ID, NSI ID), including those that are currently in use, and those that are available to be allocated. It also stores the mapping relationship between the CSI and the resource e.g. NSI, as well as the real time communication service resource availability and capability information according to the feedback or notification from NSMF. CSIs are allocated, modified and deallocated, and the corresponding network resource information is updated during CSI life cycle management. It maintains the CSI resource availability status.

- **CSI LCM**: It manages CSI lifecycle e.g. through requesting NSMF to allocate/deallocate/modify network resources for the CSI. It also does the feasibility check for a new CSI request. The NSMF notifies CSMF the network resource LCM status so that the CSI can update the CSI resource inventory accordingly.

- **Fault Supervision of CSI**: It collects CSI level fault supervision information. The closed loop management should be operated through interaction between CSMF and other OAM functions e.g. NSMF, MDAF.

- **Performance Assurance of CSI**: It collects CSI level performance measurement information and supports SLS assurance. CSMF needs to collaborate with other OAM functions, e.g. NSMF, MDAF, for this purpose.

### 4.2.3 Lifecycle of communication service

Lifecycle of a communication service instance (CSI) includes the following phases:

**- Preparation phase:**

Providing a communication service instance (CSI) starts with preparation of CSI, which includes service design, pre-planning, feasibility check, i.e., checking the attainable service quality from both resource and service aspects, negotiation of the service attributes, preparing service and network requirements derived from SLA.

**- CSI commissioning phase:**

Once the CSI is prepared, it can be established by converting the communication service requirement for the CSI to network requirements and creation of the CSI. When the CSI is created, it is deployed on the network resources and ready to be activated.

**- CSI operation phase:**

After the commissioning phase, the CSI is activated. An activated CSI allows run-time operation of the communication service, e.g., quality assurance, data exposure, CSI modification. Optimization of CSI utilization may continue during the operation phase of the CSI.

**- CSI decommissioning phase:**

When the CSI is no longer needed, after being de-activated, lifecycle of the CSI ends with CSI termination.



Figure 4.2.3.1: Lifecycle of a communication service instance

### 4.2.4 Relation of CSI lifecycle to NSI lifecycle

#### 4.2.4.0 Introduction

Resource facing aspects of CSI lifecycle involve interactions with NSI lifecycle. It is to be noted that except for certain situations when a CSI LCM operation triggers a NSI LCM operation, CSI-NSI lifecycles are independent. The following clauses show the cases when a CSI LCM operation triggers a NSI LCM operation.

#### 4.2.4.1 CSI LCM operation triggering NSI creation

During the "CSI commissioning" phase the provider of the communication service may run a trail for instance before the SLA (including SLS) is agreed. The trial period may be needed to allow the shared network slice resources to learn and adapt the resource allocation and configuration to changed traffic flows associated with the CSIs and their target KPI's.

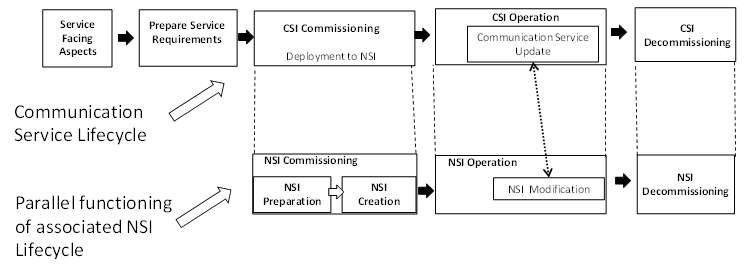


Figure 4.2.4.1.1: NSI is exclusively used for CSI

#### 4.2.4.2 CSI LCM operation triggering NSI modification

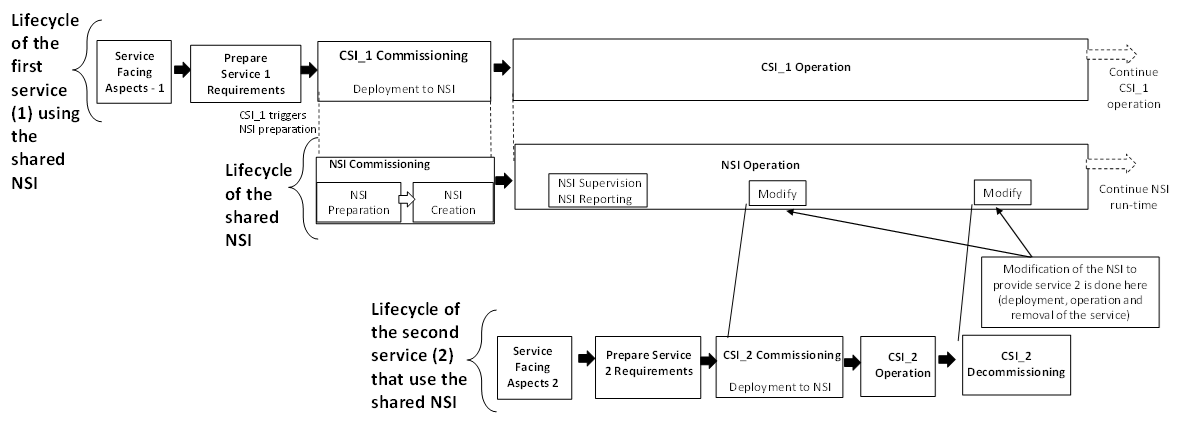


Figure 4.2.4.2.1: CSI LCM operation triggering modification of a NSI shared by two CSIs

The modification step may necessitate a trial being performed to allow for learning and adapting the resource allocation and configuration to shared NSI.

#### 4.2.4.3 CSI LCM operation triggering NSI activation and deactivation

The LCM operation of an NSI is independent of the LCM operation of CSIs using the NSI. When CSIs share an NSI there is no constraints on the termination of the CSIs. For example, CSI\_1 is created before CSI\_2: CSI\_1 could then be terminated first, or CSI\_2 could be terminated first, both options are possible. Even more options are possible if CSI\_3… to CSI\_N are added.

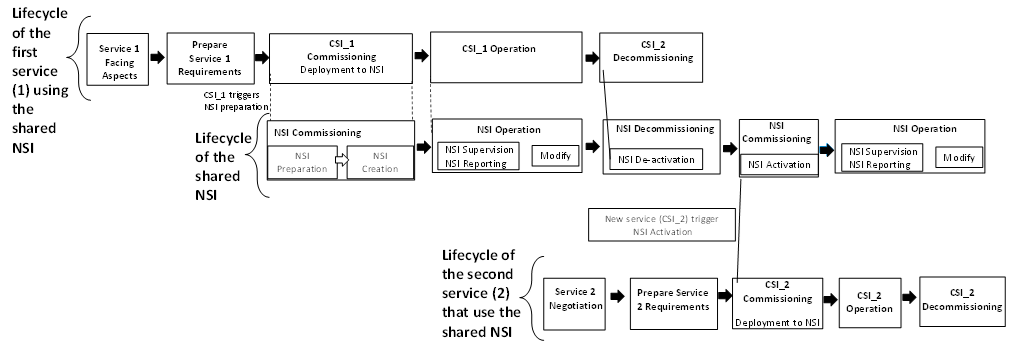


Figure 4.2.4.3.1: CSI LCM operation triggering activation/deactivation of a NSI shared by two CSIs

### 4.2.5 Performance assurance of communication services

Performance assurance of communication services includes the following aspects:

- Performance monitoring of communication services;

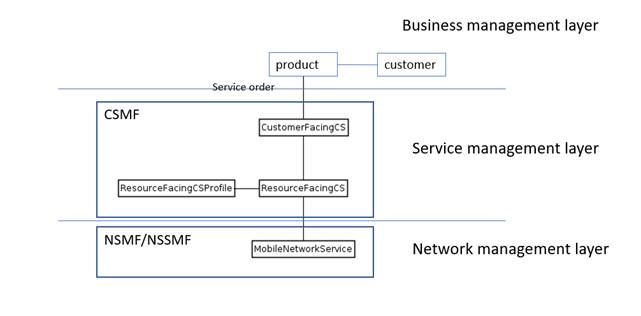
- Performance analytics of communication services;

- Performance guarantee of communication services.

These aspects are responsible for restoring the communication service performance for customers to a level specified in the SLS or other service KQI descriptions as soon as possible.

## 4.3 Management layers

The high-level view of management layers is provided by ITU-T and can be found in M.3010 [8]. Figure 4.3.1 shows the relation between the communication service model and the business, service and network management layer specified in [8].



NMF

Figure 4.3.1: Management model for management of communication services

The customers of a service provider (a subscriber or an enterprise) are not directly connected to the CFCSs. The customer is connected via the products in the portfolio of the service provider (a product is offered to the customers of a service provider). One of the aspects on the business management layer is the definition of the products, the product characteristics and their relation to a customer. For example, a CSP agrees on requirements and documents them in a Service Level Specification (SLS) with the customer. The SLS requirements can be part of a product definition to allow the CSP e. g. to offer same product definition to other customers. This relationship belongs to the business management layer and is not subject to standardization.

A service order to provide a communication service comes from the business management layer to the service management layer. The order contains information about the communication service to be provided to the customer. The information includes service specific information, i.e. attributes and values that are needed to configure the communication service, and customer specific information, i.e. attributes and values that are needed to configure the service for a specific customer (for example endpoints, coverage, and QoS, QoE attributes).

The information from a CFCS is mapped or converted to RFCS information and depending on the type of service additional attributes may be needed for the configuration of an RFCS. The RFCSProfile describes a specific RFCS type that can be instantiated with a new service order.

The service order for provisioning of a new communication service is converted to a request to the network management layer (NMF) to allocate a network slice [8] and allocate or configure the associated network slice subnets [8]. Depending on the communication service requirements the network management layer either creates a new network slice for the request or modifies, an existing network slice and let the new communication service use the existing network slice. The procedures for network slice allocation and network slice subnet allocation and configuration are described in TS 28.531 [8].

**NSaaS**

Network slice as a Service is specified in TS 28.530 [8] and used in a number of use cases. The NSaaS aspects are managed on the service management layer while the resource aspects are managed on the network management layer. The request for NSaaS comes to the service management layer and will be translated into one or more resource requests on the network management layer. The associated service profile(s) [7] specifies the network attributes that need to be configured for the customer to use the network slice as a service. In this scenario the CSMF layer receives the request for NSaaS from the business management layer including the service management requirements derived from the SLS.

## 4.4 Management model

### 4.4.1 Introduction

A CSP has to administrate communication services both from the view of the customer and from the view of the resource. The administration from the view of the customer is about information in relation to the business agreement for example address, SLA information, etc. The administration of a communication service from the view of the resources is about information on the relation between the communication service and the resources being used, the behaviour of the resources and how this impacts the users of the communication service.

NOTE: The meaning of SLA information in the context of the present document is as follows: A CSP and a CSC have a business agreement of which the SLA is a part of. The service and network requirements are derived from an SLA/SLS (for example performance management metrics for eMBB on delay and latency).

### 4.4.2 Description

The administration of a customer facing communication service (CFCS) and the administration of a resource facing communication service (RFCS) are the responsibility of different organisations within a CSP, Administration of CFCSs includes the administration of the business aspects between the CSP and the CSC. For example, what actions the CSP is to take in case an SLA is breached. This interaction takes place northbound of the customer facing part of the CSMF which maintains the relationship between the customer and the communication service(s). Not meeting the SLS (as part of the SLA) may result in concrete actions to be performed towards the resources, this interaction takes place between the RFCS and the resources.

The entities and the relationship are shown in Figure 4.4.2.1. a more detailed description is provided below Figure 4.4.1.

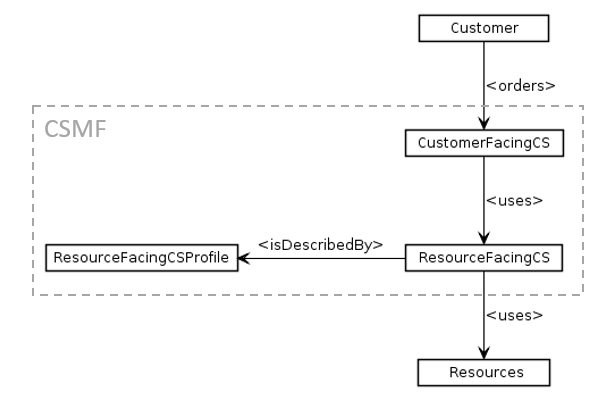


Figure 4.4.2.1: Example of relationships shown between different entities

A CSP receives an order or request from a customer to provide a communication service. With the reception and acceptance of the order, the administration and management of communication services begins. The order from the customer is processed and mapped to a Customer Facing Communication Service (CFCS).

The CSCF is what the customer will see and recognize, which is not the same as which resources are configured and used to provide the communication service to the customer.

The CFCS uses the RFCS, the RFCS represents a communication service instance for a specific customer. A customer may have multiple RFCS (for example eMBB#1, eMBB#2 and mIoT#1). An RFCS uses resources or uses resource services. An example of a resource service is the NSaaS, an example of resources is a RAN resource, CN resources or TN resources.

The provisioning of a RFCS can be done using a set of parameters that are applicable to each instance of an RFCS. This set of parameters is called the RFCS profile. Multiple RFCS profile can be supported depending on the different types of RFCS that can be supported by the resources. The RFCS profile holds all information that is needed to describe the capabilities of an RFCS. The management function creates a new RFCS when a request is received, the parameters from the RFCS profile are added to the new RFCS with the values of the parameters populated with information from the request.

### 4.4.3 Communication services applied to network slicing

In a network slicing scenario, the resources used by an RFCS are captured by the network slicing model. The CSP could have different types of RFCS where each type is described by a ResourceFacingServiceProfile consisting of a pre-defined set of attributes. A request for an RFCS involves the creation on an instance of an RFCS using the attributes of the selected ResourceFacingServiceProfile with the information from the request.

The RFCS instance uses an NSI, the RFCS instance is bound to an NSI instance at instantiation time. The management system needs to allocate an appropriate NSI to support the RFCS. Depending on the NSI capabilities many RFCS may use a single NSI. The NSI capabilities are described by the set of ServiceProfiles it supports. A single RFCSProfile maps to a single ServiceProfile supported by the NSI.

The communication service always uses resources from the RAN, CN and TN domain otherwise there would not be a connection for the Communication Service to use. The top-level NSSI aggregates the resources of the domain NSSI's, and through 1:1 relationship with the NSI the top-level NSSI does not require an association with any profile, this information is already captured by the ServiceProfiles supported by the NSI.

The lower level or domain NSSI's as per slicing model in TS 28.541 [7] may be associated with one or more SliceProfiles.

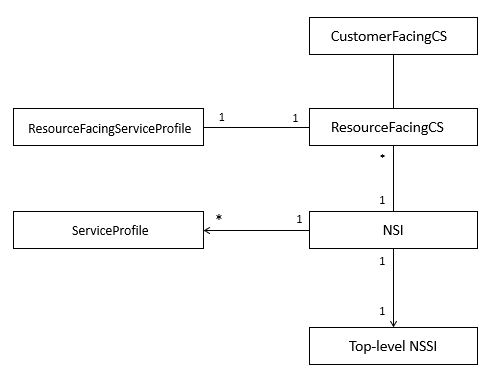


Figure 4.4.3.1: Example of relationships shown between different entities

## 4.5 Communication services

### 4.5.1 Introduction

Various organizations are involved in the specification of information that is relevant for B2B customers of a CSP. The information can be used between CSP and CSC to agree on the characteristics of service using network slices. This clause captures the concept from GSMA.

### 4.5.2 GSMA GST/NEST

The Generic Network Slice Template (GST) is a set of attributes that can characterise a type of network slice. One or more NSIs (Network Slice Instance) can be created out of the same type based on the requirements. GST is generic and is not tied to any specific network deployment, see GST defined in GSMA [12]. Some of GST attributes are embodied as some attributes of ServiceProfile [7], for example, GST attribute "Isolation level" [12] is mapped to ServiceProfile attribute "resourceSharingLevel" [7].

The NEtwork Slice Type (NEST) is a GST filled with values. Some of NEST attributes are embodied as some attributes of ServiceProfile [7] filled with values, for example, NEST attribute "Isolation level" with value = 0 [12] is mapped to ServiceProfile attribute "resourceSharingLevel" [7] with value = shared.

Figure 4.x.2-1, as an example, shows the mapping relation of 3GPP ServiceProfile and GSMA GST/NEST in context of the network slice lifecycle. Network Slice Customer (NSC) acts as CSC (see Figure 1 of GST [12]), CSMF acts as CSP, and NSMF prepares NSIs based on attributes values of ServiceProfile [7] which is a mapping of GST/NEST.



Figure 4.5.1.1: Mapping of 3GPP ServiceProfile and GSMA GST/NEST  
 in context of the network slice lifecycle

## 4.6 SLS assurance

### 4.6.1 Description

The NOP needs to take into account their customers' requirements in planning, provision and optimization phases of the network, which may include:

- Receive the service request from the customer.

- Identify which SLS that management system could guarantee with the network management capabilities.

- Identify what other information except the management data may be needed to support management decision.

### 4.6.2 Management cooperation with 5GC and NG-RAN

Coordination may be needed between the management, 5GC and NG-RAN domains as shown in the figure 4.6.2.1. The management domain provides the SLS assurance from the management perspective. Core and RAN contribute to the fulfilment of network slice SLS from the control plane and user plane perspective.

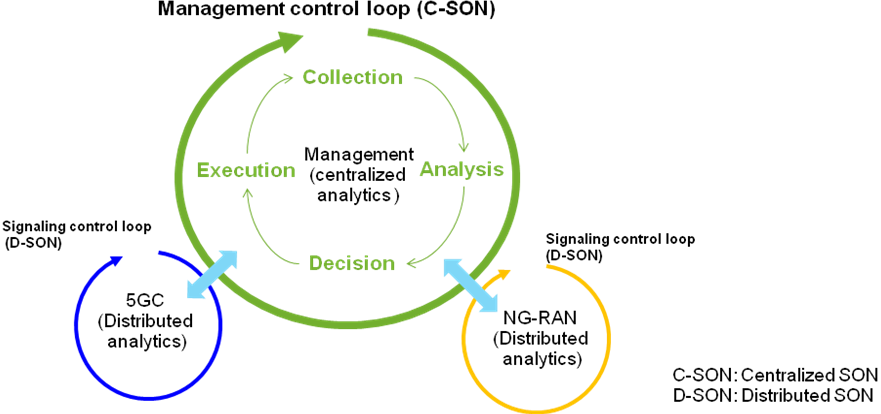


Figure 4.6.2.1: Cooperation between management,  
 5GC and NG-RAN domains following Hybrid-SON

## 4.7 Service QoE

### 4.7.1 Description

The QoE information is information collected by the end user application in the UE. The QoE information can be also collected by a collection centre for analysis and/or KPI calculations [10].

Service QoE is analytics data from QoE information of user related to CSI. How to analyse collected QoE information and calculate the result of Service QoE may be defined by NOP or CSP/CSC. For example, the Service QoE can be a weighted average experience of multiple user applications using CSI. Percentage of users satisfied in a given CSI may also be the analytics result and can be used as Service QoE for the CSI.

Service QoE may be used for supporting SLS fulfilment.

### 4.7.2 Service QoE collection and service quality assurance

If there is no methodology model to map end user QoE requirements into resource aspect related requirements, the end user service QoE information cannot be deduced from performance measurements in the network. There are two types of methods for service QoE collection:

- For DASH and MTSI user services in TS 28.404 [10], user QoE information is measured and collected by the user application in the UE. A collection centre collects user QoE information for a specified user service/user service type either from UEs in a specified area or a specific UE in UMTS and LTE. For 5G network MDAS may collect and analyse the user QoE information. Service QoE of given CSI is an analytic result of user QoE information.

- For other user services, user QoE information is measured or collected by the application server of CSC or CSP. In TS 23.288 [11] the NWDAF collects data from applications and provides analytics data services. The management system may get analytic results by consuming the analytics data services provided by NWDAF. The analytic result from NWDAF may be used as Service QoE.

In the case of Network Slices as NOP internal, the Service QoE may help the management system to optimize the resources of CSI and guarantee the performance.

In the case of Network Slice as a Service, the Service QoE of CSIs which is using NSI may help the management system for SLS assurance.

# 5 Potential use cases and requirements

## 5.1 Management data analytics and automated service assurance

### 5.1.1 Service quality assurance and optimization of the services

#### 5.1.1.1 Description

The goal of the use case is to enable service quality assurance and optimization for the set of services provided by the network to certain group (category) of the UEs. For example, the set can include the services provided via certain NSI(s) or to IoT devices in certain area.

It is assumed that the relevant NFs are deployed and active in NG-RAN and 5GC. The group of NG-RAN and 5GC nodes, which are essential for the set of E2E services, provide provisioning and PM management services. It is also assumed that the providers of the related NSI / NSSI provisioning and PM management services are deployed and active.

The management system is consuming above management services either directly or through proxy nodes that re-exposure the management services; the management system is aware of the performance requirements imposed on the set of services.

The management system is collecting the network data and monitoring the performance indicators related to the targeted services. Analytics hosted by the MDAF may be utilized for processing of the network data to derive and analyse the performance indicators. If the service quality assurance and optimization function detects performance degradation or potential for improvement of the targeted performance indicators, it modifies the configuration parameters in the corresponding NG-RAN and 5GC nodes and NSI(s)/NSSI(s), using the NG-RAN, 5GC, and NSI(s)/NSSI(s) (where relevant) provisioning services, and continues monitoring the performance.

If the network performance does not recover / improves, the management system may adjust the modifications, for example roll back to previous configuration. In any case it continues collection of the network data and monitoring of the performance indicators.

#### 5.1.1.2 Potential requirements

**REQ-CSM\_SAO-CON-01** The network management system shall have the capability to be configured with the target communication service performance indicators for a set of communication services supplied to a group or category of UEs.

**REQ-CSM\_SAO-CON-02** The network management system shall have the capability to collect network data and analyse performance indicators related to the set of communication services supplied to a group or category of UEs.

**REQ-CSM\_SAO-CON-03** The network management system shall have the capability to modify the configuration parameters in the NG-RAN and 5GC nodes and NSI(s)/NSSI(s), related to the set of communication services supplied to a group or category of UEs

### 5.1.2 CSI monitoring

#### 5.1.2.1 Description

After the CSI provisioning, the 3GPP management system monitors the KPIs of CSI resource part, i.e. SLA related performance metrics. According to the KPIs of CSI resource part, the 3GPP management system can evaluate SLA fulfilment by ensuring that service requirements are fulfilled by the CSI resource part.

The 3GPP management system may provide the KPIs of CSI resource part to the CSI to authorized CSI service provider or CSI service consumer to let them check whether the service SLA requirements are met.

#### 5.1.2.2 Potential requirements

**REQ-CSM\_CSI-MON-01** The 3GPP management system shall have the capability of monitoring CSI resource part and evaluating SLA fulfilment.

**REQ-CSM\_CSI-MON-02** The 3GPP management system shall have the capability of providing KPIs of CSI resource part to authorized CSI service provider or CSI service consumer.

### 5.1.3 SLS monitoring for network slicing

#### 5.1.3.1 Description

An SLS will contain information that will be broken down to service requirements that are conveyed to the CSP by the CSC. The service requirements may be used to provision a network slice instance.

After the network slice provisioning, the CSP and /or CSC may need to monitor the SLS status of the NSI to make sure whether its service requirements are achieved. In the service based management architecture, subscribe-notify and request-response style interactions between the communication services management function and network slice management function can be utilized. Network slice management function reports the SLS related network slice level KPIs and end user traffic level QoS/QoE parameters. The reporting can be periodic, or event based. Communication services management function may also invoke the SLS monitoring related APIs provided by the network slice management function. Network slice management function collects network slice domain specific operating data from the constituent network slice subnet management functions. Aggregating, analysing and processing the data into E2E network slice level operating parameters and presents them to the communication services management function.

A new slice may be created with dedicated 5GC resource e.g. dedicated SMF/UPF/PCF. Usually 5GC resource is enough while NG RAN is the bottleneck. In the radio access network, QoS of user traffics and cell KPIs may be degraded due to many factors such as congestion, coverage issues, interference, shortage of radio resources etc. In such cases, there is a risk to guarantee the E2E SLSs of one or more network slice instances for all the UEs from the CSC all the time.

The networks outside of the 3GPP operators are out of control of the 3GPP operators and may be exceptional for the SLA negotiation, e.g. the outside transport networks or DCs of third parties and the applications etc.

The number users of the network slice (customers of the CSC) is slowly increased while the network slice resources adapt to changing traffic characteristics. What slice customer care is, how many subscribers (e.g. 1 million) can be served by the slice and the Service Experience statistics per application (e.g. average Service MOS 4.0 for Application X for the slice customer) and how many percent (e.g. 90 % for Application X) UEs' service experience satisfy per application ID, see clause 6.32 of TR 23.791 [6]. Therefore, the CSPs may need to monitor the SLS status of the NSI for those aspects.

When a performance degradation impacts the service requirements the management system reconfigures the resources to resolve the performance degradation, in case the degradation cannot be resolved the management system may restrict the total number of active users.

During the runtime phase of network slice, as consequence of SLS monitoring the management system may adjust reserved resources for the network slice to improve service experiences and ensure SLS according to the activity prediction of users provided by NWDAF, as well as resource adjustment recommendation provided by MDAF.

#### 5.1.3.2 Potential requirements

**REQ-CSM\_SLS-CON-01** The 3GPP management system shall have the capability monitoring the performance metrics related to the SLA.

**REQ-CSM\_SLS-CON-02** The 3GPP management system shall have the capability consuming the data related to QoE provided by for example an NWDAF.

**REQ-CSM\_SLS-CON-03** The 3GPP management system shall have the capability evaluating the QoE data provided by an NWDAF to trigger actions if the network slice performance requirements are not met.

**REQ-CSM\_SLS-CON-04** The 3GPP management system shall have the capability configuring reserved resources in RAN potentially to be used for a new network slice instance.

**REQ-CSM\_SLS-CON-05** The 3GPP management system shall have the capability to consume activity prediction of the users from, for example, historical data in NWDAF.

**REQ-CSM\_SLS-CON-06** The 3GPP management system shall have the capability to consume the Management Data Analytics Service for the purpose of SLS assurance.

### 5.1.4 MDA-Assisted network provisioning contributing to SLS assurance

#### 5.1.4.1 Description

The 5G network can support different services with various QoS parameters. The QoS parameters are maintained by the system during the lifetime of the network.

Utilizing MDAF to provide big data analytics in order to help the management system functions to derive suitable network topology (e.g. VNF chains, network configurations etc.) to guarantee the service assurance given by the vertical customers from the network provisioning aspect. After the network is setup with the suitable configurations, the control plane and user plane could do further adjustment (e.g. with UE session control etc.) to improve the individual user experiences.

In this case, management system needs to identify which service requirements that are related to the network management system for the purpose of network or network slice deployment, and which type of information that could be provided to MDAF for the analytics.

For communication service provisioning, CSMF translates customer level SLA into communication service requirements, and analyses the network capability to determine whether to map the CSI to an existing NSI or a new NSI. This operation is performed in the CSI or NSI planning phase. MDAF can be utilized to assist such planning. MDAF may get SLS requirements as input from CSMF and provide analytical information which may include network performance data and recommended network configuration settings to help the management system functions to derive the suitable configuration parameters.

For example, communication service SLS requirements such as E2E latency, bandwidth, service area, user capacity, user QoE requirements etc. may be used as input to MDAF. . Information from 5GC and NG-RAN, such as performance measurements of 5GC NFs, performance measurements of gNBs and en-gNBs, QoE measurement etc., may be used as input also to MDAF. The output data provided by MDAF may include performance data and recommended configuration settings.

#### 5.1.4.2 Potential requirements

**REQ-CSM\_MDA-CON-01** The communication services management system shall have the capability providing the communication service requirements related to network to the management data analytics service provider.

**REQ-CSM\_MDA-CON-02** The management data analytics service provider shall have the capability getting the network management data from network management service provider.

**REQ-CSM\_MDA-CON-03** The management data analytics service provider shall have the capability allowing its authorized consumer to request recommendation for the purpose of network provisioning.

**REQ-CSM\_MDA-CON-04** The management data analytics service provider shall have the capability providing information which may include performance data and recommended configuration settings for communication service planning.

## 5.2 Lifecycle management

### 5.2.1 Communication service instances realized in a single network slice instance

#### 5.2.1.1 Description

A CSP offers a portfolio of communication services to the market (CSC). CSC selects a suitable product and orders communication service by inputting some service requirements e.g. SLA requirements information.

The CSP receives a request from a customer to realize a communication service instance:

- The CSP checks the communication service catalogue to find communication services with the communication service description which matches the request. The CSP performs feasibility check, i.e., checking the attainable service quality from both resource and service aspects.

- The CSP translates the service SLS into parameterized E2E network slice template information. In order to achieve this purpose, interactions between the CSP and NOP or some manually network design and planning process are needed. The CSP provides the service profile to the NOP for network resources allocation. The NOP checks the network slice inventory to find a network slice instances which matches the request.

- The network slice instance to be used will be checked whether there is sufficient capacity available to support the new communication service instance. If there is enough capacity available, the communication service instance will be assigned to the network slice instance. The mapping between the communication service instance and the network slice instance will be maintained by both the CSP and NOP.

The communication service instance has been realized.

#### 5.2.1.2 Potential requirements

REQ-CSM\_LCM-CON-01 The 3GPP management system shall provide a management service, which offers the capability to receive and process a request to realize a communication service instance.

REQ-CSM\_LCM-CON-02 The 3GPP management system shall provide management service, which offers the capability to ensure that the list of realized communication service instances are up to date.

REQ-CSM\_LCM-CON-03 The 3GPP management system shall provide a management service, which offers the capability to find a communication service description based on a request.

REQ-CSM\_LCM-CON-04 The 3GPP management system shall provide a management service, which offers the capability to assign a communication service instance to an existing network slice instance.

### 5.2.2 Remove a communication service instance from a network slice instance

#### 5.2.2.1 Description

A Communication Service Provider (CSP) is informed by a CSC that a realized communication service instance will cease to exist.

The CSP checks the communication service inventory to find the network slice instance that is used to realize the communication service instance. The communication service instance is unassigned from the network slice instance and the network slice instance is modified or terminated to reflect the changed requirements.

The communication service instance has been removed.

#### 5.2.2.2 Potential requirements

**REQ-CSM\_LCM-CON-05** The 3GPP management system shall have the capability to remove an existing instance of communication service according to the request from a CSC to remove a communication service instance.

**REQ-CSM\_LCM\_CON-06** The 3GPP management system shall have the capability to request the network slice management function to modify or terminate the existing NSI which supports the CSI to be removed.

### 5.2.3 Management aspects of NSIs utilized by multiple communication services

#### 5.2.3.1 Description

Network slices and network slice subnets can be shared by different communication services as described in clause 4.1.3 of TS 28.530 [3]. Also, same NSI can be utilized to provide communication services to different customers. In both cases, multiple CSIs may share a single NSI. In this use case, a communication service provider uses a network slice to provide multiple CSIs, i.e. network provider performs service-based sharing of the network slice among its customers.

On the contrary to the cases where a single NSI is utilized for a single CSI, the network management system is responsible for maintaining QoS guarantees for each service or customer over the resource facing aspects of a single NSI. For service-based sharing, the customer provides service requirements. Therefore, the NSI resources are shared based on service requirements to satisfy SLS requirements. In this case, the network provider determines the policies and rules about how the network resources are utilized. In other words, the network itself is transparent to the customer of the CSI service. Therefore, the network management system can utilize a database including available services.

While utilizing NSIs with sharing, effect of all services on that NSI and its constituent should be considered. Effects of loads of services can be evaluated using historical data and analysis provided by MDAF, as a part of feasibility check for provisioning CSIs. Similarly, for modifications on NSIs and NSSIs with sharing, effect of the modification on all services are considered.

#### 5.2.3.2 Potential requirements

**REQ-CSM\_LCM-CON-07** The 3GPP management system shall have the capability to assure the QoS guarantees for each service when a network slice is utilized by multiple services.

### 5.2.4 Obtaining an NSI as an NOP Internal to provide multiple CSIs

#### 5.2.4.1 Description

CSI is defined in Clause 3.1 as a run-time construct of a communication service for a defined group of users. For example, what a vertical customer or an enterprise customer receives from a network operator is a CSI which can be used to provide PDU sessions to its end users.

A consumer of an NSI as a NOP Internal may use the NSI to offer multiple CSIs to its customers. One example case is a CSP obtains an IOT network slice instance for a generic home monitoring service and offer it to multiple customers who run different kind of home monitoring services such as electric meter monitoring or alarm monitoring. Another example is that the CSP receives a NSI for a certain application and provides the same services to multiple customers using multiple CSIs.

Depending on the CSC requirements, CSC may obtain certain service management capabilities such as session admission control or dynamic adjustment of priorities so that it can manage the CSI services it provides to its customers.

In certain scenarios, the CSI consumers (e.g. vertical customers) may also obtain service management components such as service data handling and related actions, subscriber data handling, service and use policy establishment (user priority, user allowed services etc.) for managing the end user devices.

### 5.2.5 Providing CSI management capability to vertical industries

#### 5.2.5.1 Description

When a CSI is provided to a vertical industry or enterprise, the vertical customer may want to get certain service management capabilities.

The vertical customer is authorized to obtain the allowed management capability from CSI service provider according to the pre-defined agreements between the CSI service provider and the CSI service consumer. Level of management capability exposure has been agreed upon between the CSI service provider and the CSI service consumer.

These management capabilities may include the ability to limit or allow the traffic originated from certain end users, the ability to limit or allow traffic related to specific applications by applying priority, policy changes configuration setting which are related to session admission control.

### 5.2.6 Create a Communication Service (CSI)

#### 5.2.6.1 Description

A communication service provider (CSP) receives a request to provide a communication service to a CSC.

Based on the request the CSP checks the list of CS profiles for a matching profile, creates a new instance of the profile, adds information from the request to this profile and stores it with a unique identity (CSI Id), this is followed by a request to an NMF (Network Management Function) to allocate resources (available and assigned) (for example an NSI) that can support the characteristics of the requested CSI. Once the NMF confirms the resources have been allocated to provide the CSI, the CSP informs the CSC that the CSI has been created. The case when no matching profile can be found is not further investigated in the present document.

#### 5.2.6.2 Potential requirements

**REQ-CSM\_LCM-CON-08** The 3GPP management system shall support capabilities to create a communication service instance according to the request from a CSC.

### 5.2.7 Activate a Communication Service (CSI)

#### 5.2.7.1 Description

A communication service provider (CSP) receives a request to activate provided to a CSC.

Based on the request the CSP checks the CSI inventory and locates the CSI that is requested to be activated. The resources needed for the CSI have been allocated (assigned and available) before the activation request. From the inventory the CSP will know which resources (for example which NSI) are used for the CSI and sends an activation request to the NMF (Network Management Function) to allow the CSI to use the allocated resources. A positive response to the activation request will immediately allow the CSI to use the allocated resources. Once the NMF confirms that the CSI can use the allocated resources, the CSP informs the CSC that the CSI has been activated.

NOTE: In some cases when a trial is being performed to allow for learning and adapting the resource allocation and configuration to the shared NSI, in such case an activation request may allow a group of subscribers to use the communication service instead of the target number of subscribers (maximum number of subscribers allowed to use the NSI).

#### 5.2.7.2 Potential requirements

**REQ-CSM\_LCM-CON-09** The 3GPP management system shall support capabilities to activate a communication service instance provided to a CSC.

### 5.2.8 De-activate a Communication Service (CSI)

#### 5.2.8.1 Description

A communication service provider (CSP) receives a request to de-activate a communication service provided to a CSC.

Based on the request the CSP checks the inventory to locate the CSI that is requested to be de-activated. From the inventory the CSP will know which resources are used for the CSI and sends a de-activation request to the NMF (Network Management Function) to disallow the CSI to use the allocated (assigned and available) resources. Once the NMF confirms that the CSI cannot use the allocated resources, the CSP informs the CSC that the CSI has been de-activated.

#### 5.2.8.2 Potential requirements

**REQ-CSM\_LCM-CON-10** The 3GPP management system shall support capabilities to de-activate a communication service instance provided to a CSC.

#### 5.2.9 Modify a Communication Service (CSI)

#### 5.2.9.1 Description

A communication service provider (CSP) receives a request to modify a communication service provided to a CSC.

Based on the request the CSP checks the inventory to find the CSI that is requested to be modified. In some cases a modification request may necessitate a trial being performed to allow for learning and adapting the resource allocation and configuration to the shared resources. From the inventory the CSP will know which resources (for example an NSI) are used for the CSI and sends a modification request to the NMF (Network Management Function) to modify the allocated resources (available and assigned) a modification can result in adding or removing resources, or changes of properties of the resources within the scope of the service definition). Once the NMF confirms that the modification has been completed, the CSP informs the CSC that the CSI has been modified.

#### 5.2.9.2 Potential requirements

**REQ-CSM\_LCM-CON-11** The 3GPP management system shall support capabilities to modify a communication service instance provided to a CSC.

### 5.2.10 Terminate a Communication Service (CSI)

#### 5.2.10.1 Description

A communication service provider (CSP) receives a request to terminate a communication service provided to a CSC.

Based on the requirements from the request the CSP checks the inventory to find the CSI that is requested to be terminated. If the status of the CSI is active, the CSP has to de-activate the CSI before the CSI can be terminated. When the status of the CSI is in-active the CSP can terminate the CSI. The CSP will know which resources (for example an NSI) are used for the CSI and sends a de-allocation request to the NMF (Network Management Function) to de-allocate the allocated resources. Once the NMF confirms that the resources allocated to the CSI have been de-allocated, the CSP informs the CSC that the CSI has been terminated.

#### 5.2.10.2 Potential requirements

**REQ-CSM\_LCM-CON-12** The 3GPP management system shall support capabilities to terminate a communication service instance provided to a CSC.

### 5.2.11 Management of multi-party communication service

#### 5.2.11.1 Description

A Vertical Industry customer deploys IoT devices in a specific geographical area supported by a communication service provided by a CSP. The customer decides to venture into new geographical areas and request the CSP to extend the agreement to cover other geographical areas. The new requirement includes geographical areas where the CSP does not have mobile network coverage. The CSP makes an agreement with an Access Network (AN) provider that can provide the required additional coverage for the customer. To improve the latency the CSP decides to extend its CN resources to be located near or with the CN resources of the AN provider. The CSP provides the additional CN resources and integrates the CN resources into the CSP's existing CN as well as into the AN from the provider. The CSP offers the customer a seamless communication service spanning the coverage areas required by the enterprise

This description identifies the following roles involved in the use case:

- CSC is the Vertical Industry customer looking for coverage of new geographical areas for IoT devices and therefore has a request to increase the current coverage

- CSP providing communication service to CSC

- NOP#1 providing RAN, CN services to the CSP

- NOP#2 providing RAN services, for different area, to CSP

- VISP providing virtualization infrastructure (e.g. data centre) and management services to NOP#2

The use case involves the following steps and interactions as sketched:

- CSP provides a communication service to an CSC. The RAN and CN resources that realize the communication services are provided by NOP#1

- CSC wants to extend the communication service to areas that are not covered by CSP.

- CSP wants to provide the CSC with the same service agreement level when outside the current CSPs coverage area.

- CSP asks the NOP#1 to provide resources (e.g. RAN resources for additional area) that enable the CSP to extend the currently provided communication service to additional coverage areas.- NOP#1 requests to NOP#2 management exposure to enable creation and configuration of additional RAN resources.

- NOP#1 deploys its own CN resources on VISP using the management services exposed.

- NOP#1 connects CN resources to the AN of NOP#2 using the management services exposed by NOP#2.

- NOP#1 extends its CN with the CN resources connected to Access Network of NOP#2.

- The CSP extends the currently provided communication service to include the additional requested coverage areas provided by NOP#2.

- NOP#1 manages the resources, including its CN resources connected to the NOP#2 Access Network.

- CSP manages the extended communication service.

#### 5.2.11.2 Potential requirements

REQ-FNS\_CON-01: The 3GPP management system shall support capabilities to provide management services that allow the integration of 3GPP resources in another operator's network to allow seamless provisioning and management of communication services.

REQ-FNS\_CON-02: The 3GPP management system should support capabilities to provide management services that allow the management of 3GPP resources in another operator's network.

## 5.3 Lifecycle management, data analytics and automated service assurance

### 5.3.1 Service management aspects of NSaaS

#### 5.3.1.1 Description

5G networks with slicing provides a variety of communication services, including NSaaS as discussed in clause 4.1.6 of TS 28.530 [3]. NSaaS consumer may provide multiple communication service instances (CSIs) using the obtained NSI. In this case, it is assumed that the NSI is provided so as to satisfy the network resource requirements provided by the NSaaS consumer. The management system of the NSaaS consumer and the NSaaS provider are responsible for maintaining QoS guarantees for each CSI using the NSI.

In this case, the customer's CSMF should convert NSI resource capability to service provisioning capabilities. Whenever a new CSI added to the NSI, the NSaaS consumer should ensure the NSI is capable of supporting the new CSI. The NSaaS provider has to satisfy the policies and rules about how the NSaaS consumer needs to utilize the network resources. In other words, the network is exposed to the customer based on necessity.

The MDAS of the customer may assist for the conversion of resource capability into service capability, or the customer may request services and analysis from the MDAS of the NSaaS provider. Note that in the former case, the CSMF of the NSaaS consumer needs to obtain resource information and then perform the conversion. The NSI resource capability can be evaluated using historical data and analysis provided by MDAS of the NSaaS consumer. This information can be used by the NSaaS customer for provisioning and quality assurance of CSIs utilizing the obtained NSI.

When obtaining analysis from the MDAS of the service provider, the network management system of the service provider may prepare a database including service requirements conversion to network resource requirements and/or service capacity boundaries that can be supported by the network resources available to NSaaS consumer. When the conversion is readily available, CSMF of the NSaaS consumer do not need to make the conversion, and is used for service and customer aspects.

#### 5.3.1.2 Potential requirements

**REQ-CSM\_MDA-CON-05** The communication service provider, as the NSaaS provider, shall have the capability to provide data analytics to an NSaaS consumer.

# 6 Potential solutions

## 6.1 Solution for communication service instances realized in a single network slice instance

The customer provides service requirements. The NSI resources are shared based on service requirements (in case of sharing the same slice for different services). Note that this assumes the case where the network itself is transparent to the CSI provider at this point, i.e., only service and customer facing aspects of CSMF are considered. Differently than a non-shared NSI, the mutual effects of different services, as well as different requirements and policies of several customers need to be considered while determining the feasibility of provisioning the requested service.

Detailed explanation of steps are as follows.

1) CSMF receives an intent or request for service allocation.

2 If CSMF is not already provided with network resource information converted to service capabilities, it may request the service capabilities from the NSI provider.

a) If some network components are obtained by another provider, service requirements may be given to this provider and service capabilities can be obtained.

b) CSMF receives the analysis report.

3) CSMF sends the list of services to MDAF and other service information that may be required for MDAF analysis, e.g. service policies and requirements.

a) MDAF may use historical analysis of services sharing the NSI and also collects information about the current situation of the network, e.g. by querying RAN and CN traffic load analysis and policies.

b) CSMF obtains information from MDAF without interacting with other management functions at the lower layers, such as NSMF and NSSMF.

4) CSMF evaluates the feasibility of adding the requested service by using service-level analysis and predictions.

5) CSMF makes a decision on whether to assign the CSI, or not.

6) The customer receives response.

a) If the service is feasible, the CSI is assigned for the service. The customer receives acknowledgement along with necessary information about CSI, e.g. the identifier and so on.

b) If the service is not feasible, the response includes reasons for rejection. Rejection reasons may be provided depending on the exposure to the customer.

## 6.2 Solution for translation of SLS into SLS requirements

A service-level agreement (SLA) specification (SLS) is an agreement between two or more parties, where one is the customer and the others are service providers. In this case, CSC is the consumer of the communication services, CSMF is the service provider of communication services management.

Therefore, CSMF needs to convert the received SLAs from CSC to SLA requirements, i.e. the service and network requirements derived from SLAs, see figure 6.2.1.

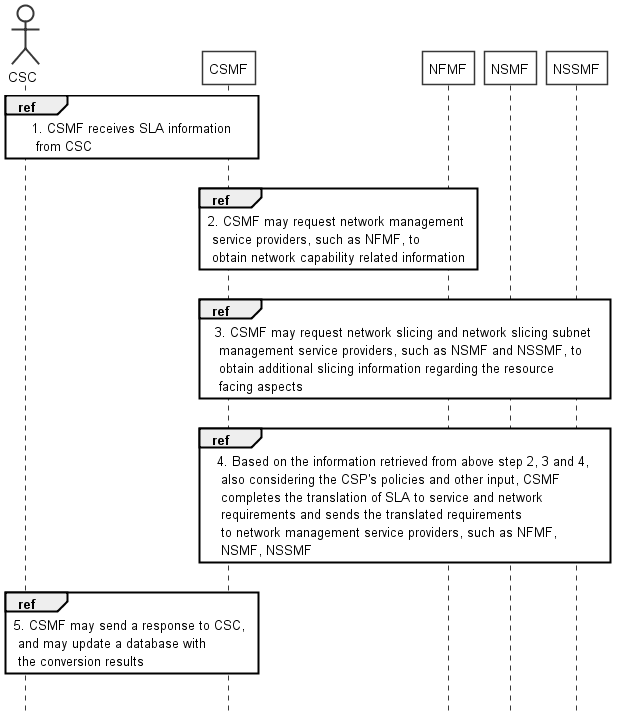


Figure 6.2.1: Translation of SLA into SLA requirements

1) CSMF receives SLA information from CSC.

2) CSMF may request network management service providers (e.g. NFMF) to obtain network capability related information.

3) CSMF may request network slicing and network slicing subnet management service providers (e.g. NSMF and NSSMF) to obtain additional slicing information regarding the resource facing aspects, if needed.

4) Based on the information retrieved from above step 2, 3 and 4, also considering the CSP's policies and other input (e.g. service profile information stored in service catalogue), CSMF completes the translation of SLA to communication service requirements and network requirements and then sends the translated requirements to network management service providers (e.g. NSMF, NSSMF, NFMF)

a) In case of network slicing, NSMF fills the dataType ServiceProfile which represents the properties of network slice related requirements that should be supported by the network slice instance with the translated requirements.

1) If the conversion between CSMF and CSC is done upon a request, CSMF may send a response to CSC, and may update a database with the conversion results.

## 6.3 Solution for communication service instance termination

### 6.3.1 Solution for the case that network slice used as resources

1) The CSC sends a request to the CSP for service termination.

2) If the status of the CSI is active, the CSP has to de-activate the CSI before the CSI can be terminated.

a) The CSP decides on whether to decommission the related NSI(s) and NSSI(s), or modify them. This decision can be based on current and prospective services to utilize these NSI(s) and NSSI(s), e.g. MDAS may provide prediction on prospective demand.

b) If the CSC has access to management exposure interfaces, the CSC may be involved in decommissioning. The management exposure interface is disabled before the termination of the service.

3) CSP manages the required modifications with NSMF and NSSMF via the resource facing interface of CSMF.

4) An acknowledgement may be received by the CSP and CSC indicating that the CSI termination is completed, and the exposure interfaces are disabled.

a) The CSP may decide to terminate the SLA with the CSC upon receiving the acknowledgement.

## 6.4 Solution for communication service instance modification

### 6.4.1 Solution for the case that network slice used as resources

After all NSIs for a customer's CSI are prepared and provisioned, CSMF of the customer request the activation of the CSI so that CSI's runtime begins (except in Exposure E2, the customer may not need to request activation).

1) The CSC sends a request to the CSP for service modification.

a) Based on the request the CSP may check an inventory to find the CSI that is requested to be modified.

b) CSP checks the feasibility of the modification request. The modification may necessitate a trial being performed to allow for learning and adapting the resource allocation and configuration. If the request is not feasible, CSC and CSP may negotiate to agree on a feasible modification option.

c) Alternatively, if CSC has information about estimated service capacities as provided by CSP, CSC may directly request a feasible modification.

d) An update on the SLA may also be negotiated.

2) After CSP evaluates the required changes on the CSI, CSP performs or request for the necessary operations on the related NSI(s) and NSSI(s) via the resource facing aspect of CSMF, NSMF, and NSSMF.

a) Service and resource facing aspects of the CSMF of the CSP may be partially exposed to the CSC for monitoring and supervision. In this case, CSC may utilize these interfaces for required operations.

3) Once the NMF confirms that the modification has been completed, the CSP informs the CSC that the CSI has been modified.

## 6.5 Solution for communication service instance activation

### 6.5.1 Solution for the case that network slice used as resources

The resources needed for the CSI have been allocated (assigned and available) before the activation request. From the inventory the CSP will know which resources (for example which NSI) are used for the CSI.

1) The CSC sends a request to the CSP for service activation.

a) Based on the request the CSP may check the CSI inventory and locate the CSI that is requested to be activated.

b) Alternatively, the request from the CSC may include a CSI indicator.

2) Prepared CSIs are deployed in this stage.

a) CSP is responsible for CSI deployment to NSI, which means that CSI is allowed to use the allocated resources.

b) If CSC has access to management interfaces, CSC may initiate deployment.

3) CSI operation can begin after this stage.

a) CSC receives acknowledgement indicating that the CSI is activated.

## 6.6 Solution for communication service instance de-activation

### 6.6.1 Solution for the case that network slice used as resources

1) The CSC sends a request to the CSP for service de-activation.

a) Based on the request the CSP may check the CSI inventory and locate the CSI that is requested to be de-activated.

b) Alternatively, the request from the CSC may include a CSI indicator.

2) CSP makes necessary changes with the resource facing aspects of CSMF to disallow CSI from using the resources of the associated NSI(s).

3) CSI is de-activated and CSI cannot use the NSI resources after this stage.

a) Further decisions on NSI lifecycle are taken by the CSP.

4) CSP sends an acknowledgement indicating the de-activation of the CSI to the CSC.

a) SLA between the CSP and CSC may be re-negotiated.

## 6.7 Solution for MDA-Assisted SLS assurance

### 6.7.1 MDA-Assisted network optimization

To enable SLS assurance within certain region area to UEs or certain group (category) of UEs, NSMF, NSSMF and NFMF use MDAF which provides MDAS to help network optimization, see figure 6.7.1.1.

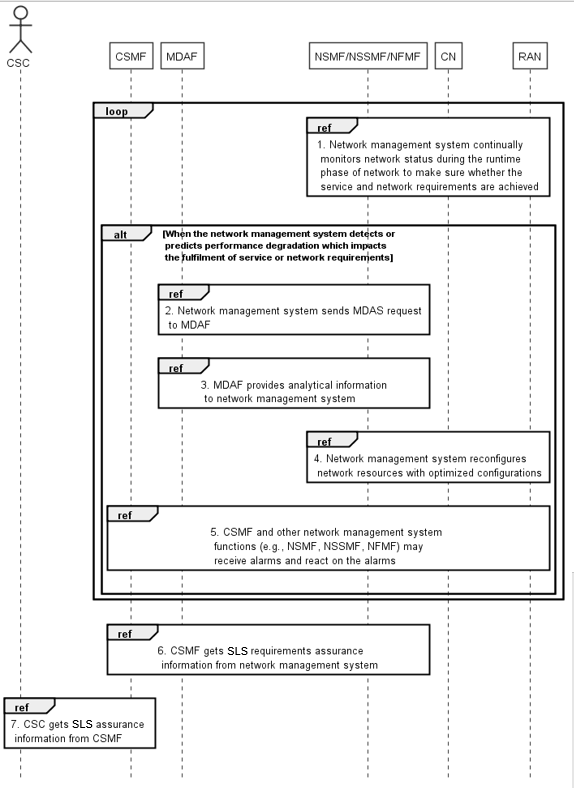


Figure 6.7.1.1: MDA-Assisted network optimization contributing to SLS assurance

1) Before network initial setting, there is fine tuning of configurations and algorithms during a trial phase of provisioning.

2) After network initial setting, NSMF, NSSMF and NFMF continually monitor network status during the runtime phase of network to make sure whether the service and network requirements are achieved. Information from 5GC and NG-RAN, such as alarms or performance measurements of 5GC NFs, alarms or performance measurements of gNBs and en-gNBs, QoE measurement, high level KPIs, etc., need to be collected frequently or on demand by the NSMF, NSSMF and NFMF.

3) When the NSMF, NSSMF and NFMF detect performance degradation which impacts the fulfilment of service or network requirements, the NSMF, NSSMF and NFMF send MDAS request to MDAF. There may be one or several instances of MDAF depending on the actual deployment.

4) MDAF may use historical analysis result and also collects information (e.g. by querying NG-RAN and 5GC traffic load and policies) about the current situation of the network to provide MDAS response which may include network performance data and recommended network reconfiguration settings to the NSMF, NSSMF and NFMF to help them reconfigure the resources to resolve the performance degradation. SON function may be requested to trigger network optimization.

5) The NSMF, NSSMF and NFMF reconfigure network resources with optimized configurations to minimize resource consumption for goal fulfilment.

6) During the runtime phase of network, CSMF, NSMF, NSSMF and NFMF may receive alarms, e.g., a KPI is not satisfied, or it is predicted that a KPI may not be satisfied in the near future, or the under-utilization of service capacity. SON function may be requested to perform fault handling such as fault locating, and by the assistance of MDAS, triggers self-healing operation.

- If the alarm is related to the insufficiency of resources, CSMF requests increasing service capacity via resource-facing aspects.

- If the alarm is related to under utilization of service capacity, CSMF requests decreasing service capacity via resource facing aspects.

- If the alarm is related to unexpected and high demand from one of the services, CSMF facilitates load balancing, e.g., by updating service priorities.

- If the alarm is due to faults in the network, e.g., malfunction of network equipment, NSMF, NSSMF and NFMF request alternative resources.

7) CSMF gets SLS requirements assurance information from NSMF, NSSMF and NFMF, e.g., whether or not the SLS requirements are assured.

8) CSC gets SLS assurance information from CSMF, e.g., whether or not the SLA is assured.

## 6.8 Solution for providing management capability to vertical industries

When a CSI is provided to a vertical industry or enterprise, the vertical customer may want to get certain service management capabilities.

The vertical customer is authorized to obtain the allowed management capability from CSI service provider according to the pre-defined agreements between the CSI service provider and the CSI service consumer. Level of management capability exposure has been agreed upon between the CSI service provider and the CSI service consumer.

The management model shown in Figure 4.4.2.1 shows how a CSI has a CFCS part and a RFCS part, the RFCS part represents the CSP's internal view of a CSI, while the CFCS is the external view of a CSI towards the customer from a vertical industry. The CFCS can also expose the management capabilities required by the customer from the vertical industry without having to expose all CSP internal management capabilities.

Management capabilities for communication services include observation of the performance of the communication services, exposure of analytics services and providing custom designed capabilities to CSC.

## 6.9 Solution for management aspects of NSI utilized by multiple communication services.

### 6.9.1 Assignment of communication service to an existing NSI

1) The CSP receives the request, with CS requirements, from CSC and create a new CSI.

2) CSP using the resource facing interface of CSMF.

a. Translates the service requirements into resource facing requirements

b. Communicates the resource facing requirements to the NSMF for the allocation of an NSI

3) NSMF may create a new NSI or assign an existing NSI by performing a feasibility check including the following.

a. An isolation requirement check will be performed to ensure that the target NSI is shareable.

b. The target NSI should be able to satisfy the resource facing requirements received from CSMF.

c. The total projected/expected NSI performance, maybe evaluated using MDAF and NWDAF, should meet the predefined requirements (e.g. total expected load of NSI shall not be exceeding a predefined threshold).

4) Depending on the feasibility check, some NSI modification procedures (e.g. scaling) may be required during the CSI Commissioning.

### 6.9.2 Activation of CSI sharing NSI.

On receiving a CSI activation request a feasibility check should be initiated in which the current performance (e.g. current load) of the assigned NSI should be considered to confirm if the NSI will be able to satisfy the CSI requirements. Based on the result of the feasibility check the NSI modification (e.g. scale-out/up) procedure may be initiated before activating the CSI.

1. The CSP receives the request for a CSI activation.

2. CSP evaluates the projected/expected NSI performance (e.g. NSI load information) maybe using the network analytics function e.g. MDAF, NWDAF.

3. Considering the projected/expected NSI performance and the CS requirements, the CSP may either activate the CSI or initiate the NSI modification procedure, via the resource facing interface of CSMF, before activating the CSI.

### 6.9.3 Termination of CSI sharing NSI.

1. The CSC sends a request to the CSP for communication service termination.

2. CSP, via CSMF, initiate CSI Decommissioning.

3. If the status of the CSI is active, the CSP has to de-activate the CSI before the CSI can be terminated.

4. CSP, via CSMF, terminates the CSI.

5. CSMF identifies the NSI associated to the CSI and request NSMF to perform NSI related modification or termination operation. Before initiating the NSI termination, CSMF checks if there are current and prospective communication services utilizing this NSI. The analytics functions e.g. NWDAF, MDAF can be used to get this information.

6. In case there are multiple communication services utilizing the NSI, CSMF does the modification feasibility check, in collaboration with NSMF, to see the required level of scale-in/down to be performed as a consequence of the terminated CSI. This will include CSMF constructing the new set of resource facing requirements for the NSI and doing the feasibility check based on those requirements.

7. Based on the modification feasibility check, NSMF then decides whether to modify the NSI or to terminate it. If the NSI need to be scale-in/down at a percentage more than a predefined threshold (e.g. 70% virtual resource reduction) then the NSI may be terminated. Which will further require CSMF to relocate the current CSI(s), in collaboration with NSMF, to an existing NSI i.e. re-allocating existing NSI to active CSI(s). This is done in order to keep the number of NSI to a manageable figure and to efficiently use the capabilities of existing NSIs.

NOTE: In order to relocate the CSI, CSMF first has to de-activate the CSI detaching it from the NSI. CSMF will then initiate CSI activation procedures to allocate an existing NSI to the CSI(s).

8. CSMF may then execute the NSI termination with NSMF and NSSMF.

# 7 Conclusions and recommendations

## 7.1 Conclusions

### 7.1.1 Introduction

The study has identified use cases, requirements and solutions for management of communication services. The study has extended the existing concepts for network slicing to include management of communication services.

The use cases and requirements address lifecycle management of communication services and management data analytics as well as automated service assurance.

### 7.1.2 Lifecycle management of communication services

The study has identified that a communication service includes both customer facing aspects and resource facing aspects,

The study has identified use cases and requirements for a management object that represents all the network resources that are used by a communication service instance. In the study the name used for this representation is RFCS.

The study has identified that an RFCS has a <uses> relationship to an NSI in case the mobile network is partitioned in network slices.

The study has identified that the NSaaS can be considered a CFCS that maps directly to an NSI. The NSaaS (CFCS) is exposed to a B2B customer (e.g. enterprise) while the NSI is never exposed to a B2B customer.

### 7.1.3 Management data analytics

The study has identified use cases and requirements for the use of management data analytics to support service level specification agreed between an operator and a B2B customer (e.g. vertical).

The study has identified that interaction between an MDAF/S, other management functions, RAN and 5GC is needed for management of communication services, to ensure that the consumers of communication services experience an optimal service.

The study has identified that further work is needed to understand deployment, roles, responsibilities and management of MDAFs.

The application of management data analytics in context of SON has not been evaluated

### 7.1.4 SLS assurance

The study has identified that a management solution is needed to address the use case "How to ensure that slice SLA is guaranteed" documented as key issue 14 in TR 23.791 [6].

## 7.2 Recommendations

### 7.2.1 Lifecycle management of communication services

It is recommended that business level information is not standardized in Rel-16 timeframe.

### 7.2.2 SLS assurance solution

It is recommended to start normative work on the specification of an SLS assurance solution in Rel-16.

### 7.2.3 Management data analytics in the SON context

It is recommended to come up with an additional study which covers the application of management data analytics in the SON context.

### 7.2.4 Management of MDAF

It is recommended to come up with an additional study which covers the management of MDAF in general and for example in relation to roles, responsibilities, and deployments.

Annex A:  
Comparison table between 3GPP ServiceProfile attributes and GSMA GST attributes

In context of the network slice lifecycle, comparison table between 3GPP ServiceProfile attributes and GSMA GST attributes is listed in below table A-1. The table can be extended to include more information for GST/NEST mapping.

**Table A-1: Comparison between 3GPP ServiceProfile attributes and GSMA GST attributes**

| **GST attribute name**  **in GSMA NG.116 Generic Network Slice Template v1.0** | **GST attribute definition**  **in GSMA NG.116 Generic Network Slice Template v1.0** | **ServiceProfile attribute**  **in 3GPP TS 28.541** |
| --- | --- | --- |
| Availability | Void | availability |
| NOTE: This attribute is not documented in this version of the GST [12] | | |
| Coverage | This attribute specifies the coverage area of the network slice - the area where the terminals can access a particular network slice. | coverageAreaTAList |
| Delay tolerance | Provide the NSC with service delivery flexibility, especially for the vertical services that are not chasing a high system performance. For instance, the service will be delivered once the mobile system has sufficient resources or during the off-peak hours. For this type of traffic, it is not too critical how long it takes to deliver the amount of data, e.g. within hours, days, weeks, etc. | FFS |
| Deterministic communication | This attribute defines if the network slice supports deterministic communication for periodic user traffic. Periodic traffic refers to the type of traffic with periodic transmissions.  Availability: This parameter describes if the network slice supports deterministic communication.  Periodicity: This parameter provides a list of periodicities supported by the network slice. | FFS |
| Downlink throughput per network slice | Is the achievable data rate of the network slice in downlink that is available ubiquitously across the coverage area of the slice.  Guaranteed downlink throughput (M) Maximum downlink throughput (C) | areaTrafficCapDL in Perf for eMBB of ServiceProfile  trafficDensity in Perf for URLLC of ServiceProfile |
| Downlink throughput per UE | Guaranteed downlink throughput: This attribute describes the guaranteed data rate supported by the network slice per UE (User Equipment) in downlink, which is required to achieve a sufficient quality experience (dependent on the selected service type) and can be seen as a guaranteed throughput. If the value is 0, best effort traffic is expected where no minimum throughput is guaranteed. | expDataRateDL in Perf for eMBB of ServiceProfile  expDataRate in Perf for URLLC of ServiceProfile |
| Maximum downlink throughput | This attribute describes the maximum data rate supported by the network slice per UE in downlink. These parameters could be used to offer different contract qualities like gold, silver and bronze. | FFS |
| Energy efficiency | This attribute describes the energy efficiency of the network slice, i.e. the ratio between the performance indicator, in terms of data volume (DV), and the energy consumption (EC) when assessed during the same time frame [26].  Network slice energy efficiency Time frame of the measurement | FFS |
| Group communication support | This parameter describes which type of group communication is provided by the network slice. | FFS |
| Isolation level | Isolation is one of the key expectations of network slicing. A network slice instance may be fully or partly, logically and/or physically, isolated from another network slice instance [24]. This attribute describes different types of isolation:  • Physical – network slices are physically separated (e.g. different rack, different hardware, different location, etc.)  • Logical – network slices are logically separated. | resourceSharingLevel |
| Location based message delivery | This attribute describes the delivery of information in a particular geographic region. | FFS |
| Maximum supported packet size | This attribute describes the maximum packet size supported by the network slice and may be important for URLLC (Ultra-Reliable Low Latency Communication) and MIoT (Massive IoT), or to indicate a supported maximum transmission unit (MTU). | payloadSize in Perf for URLLC of ServiceProfile |
| Mission critical support | Mission-critical (MC) leads to a priority of the network slice relative to others, for C-plane (Control Plane) and U-plane (User Plane) decisions. This is relative to a customer provider relationship and to a PLMN (Public land Mobile Network). | FFS |
| MMTel support | This attribute describes whether the network slice supports IP Multimedia Subsystem (IMS) and Multimedia Telephony Service MMTel. This parameter describes whether the GSMA PRD IR.92 [22] compliant MMTel deployment is supported in the network slice. | FFS |
| Network Slice Customer network functions | A NSC can own some Network Functions (e.g. User Plan Function (UPF), User Data Management, UDM). This attribute provides a list of network functions to be provided by the NSC. If the list is empty, the NSC is not expected to provide any network function relevant for the network slice instance. | FFS |
| Number of connections | This attribute describes the maximum number of concurrent sessions supported by the network slice. | userDensity and activityFactor in Perf for eMBB of ServiceProfile  connDensity and serviceAreaDimension in Perf for URLLC of ServiceProfile |
| Number of terminals | This attribute describes the maximum number of terminals supported by the network slice. | maxNumberofUEs |
| Performance monitoring | This attribute provides the capability for NSC and NOP to monitor Key Quality Indicators (KQIs) and Key Performance Indicators (KPIs). KQIs reflect the end-to-end service performance and quality while KPIs reflect the performance of the network.  Availability: This parameter contains a list of KQIs and KPIs available for monitoring. If the list is empty this attribute is not available in the network slice and the other parameters might be ignored.  Monitoring sample frequency  This parameter describes how often the KQIs and KPIs are monitored. | FFS |
| Performance prediction | This attribute defines the capability to allow the mobile system to predict the network and service status. Predictive QoS (Quality of Service) can be done for various Key Quality Indicators (KQIs) and Key Performance Indicators (KPIs). KQIs reflect the end-to-end service performance and quality, while KPIs reflect the performance of the network. The prediction is done for a specific point of time in the future and for a specific geolocation. Note: Only the KQIs of communication services offered by the NSP can be predicted. For over the top services, the NSP is not able to access the KQIs.  Availability: This parameter contains a list of KQIs and KPIs available for prediction. If the list is empty the attribute is not available in the network slice and the other parameters might be ignored.  Prediction frequency: This parameter describes how often KQIs and KPIs prediction values are provided. | FFS |
| Positioning support | This attribute describes if the network slice provides geo-localization methods or supporting methods.  Availability: This parameter describes if this attribute is provided by the network slice and contains a list of positioning methods provided by the slice.   Prediction frequency: This parameter describes how often location information is provided. This parameter simply defines how often the customer is allowed to request location information.   Accuracy: This parameter describes the accuracy of the location information. Accuracy depends on the respective positioning solution applied in the network slice. | FFS |
| Radio spectrum | Defines the radio spectrum supported by the network slice. This is important information, as some terminals might be restricted in terms of frequencies to be used. | FFS |
| Reliability |  | FFS |
| NOTE: This attribute is not documented in this version of the GST [12] | | |
| Root cause investigation | Root cause investigation is the capability provided to NSC to understand or investigate the root cause of network service performance degradation or failure. | FFS |
| Session and Service Continuity support | The attribute defines the continuity of a Protocol Data Unit (PDU) session. The following three Session and Service Continuity (SSC) modes are specified [1]: • SSC mode 1 - the network preserves the connectivity service provided to the UE (the IP address is preserved) • SSC mode 2 - the network may release the connectivity service delivered to the UE and release the corresponding PDU Session (the network may release IP address(es) that had been allocated to the UE) • SSC mode 3 - changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity service (the IP address is not preserved in this mode when the PDU Session Anchor changes) • None – UE loses the connectivity service | FFS |
| Simultaneous use of the network slice | This attribute describes whether a network slice can be simultaneously with other network slice and if so, which group the network slice belongs to. | FFS |
| Slice quality of service parameters | This attribute defines all the QoS relevant parameters supported by the network slice. For some of these parameters 3GPP has already defined standard values [1]. By preselecting a 5G QoS Identifier (5QI) these parameters will automatically be filled out with the standardised values.  Functional + operational  - 3GPP 5QI - Resource Type - Priority level - Packet Delay Budget - Packet Error Rate - Jitter - Maximum Packet Loss Rate | latency  e2eLatency and jitter in Perf for URLLC of ServiceProfile |
| Support for non-IP traffic | This attribute provides non-IP Session support (Ethernet session and forwarding support) of communication devices | FFS |
| Supported access technologies | This attribute defines which access technologies are supported by the network slice. | FFS |
| Supported device velocity | Maximum speed supported by the network slice at which a defined QoS and seamless transfer between TRxPs (Transmission Reception Point(s)), which may belong to different deployment layers and/or radio access technologies (multi-layer /-RAT), can be achieved. | uEMobilityLevel  uESpeed in Perf for eMBB of ServiceProfile |
| Synchronicity | This attribute provides synchronicity of communication devices. Two cases are most important in this context:  • Synchronicity between a base station and a mobile device and  • Synchronicity between mobile devices.   Availability Accuracy | FFS |
| Terminal density | This attribute describes the maximum number of connected and/or accessible devices per unit area (per km2) supported by the network slice. | userDensity in Perf for eMBB of ServiceProfile  connDensity in Perf for uRLLC of ServiceProfile |
| Uplink throughput per network slice | The achievable data rate of the network slice instance in uplink that is available ubiquitously across the coverage area of the network slice.  Guaranteed uplink throughput Maximum uplink throughput | areaTrafficCapUL in Perf for eMBB of ServiceProfile  trafficDensity in Perf for URLLC of ServiceProfile |
| Uplink throughput per UE | Guaranteed uplink throughput This attribute describes the guaranteed data rate supported by the network slice per UE in uplink, required to achieve a sufficient quality experience (dependent on the selected service type). If the value is 0, best effort traffic is expected where no minimum throughput is guaranteed.  Maximum uplink throughput This attribute describes the maximum data rate supported by the network slice per UE in uplink. These parameters could be used in order to offer different contract qualities like gold, silver and bronze. | expDataRateUL in Perf for eMBB of ServiceProfile  expDataRate in Perf for URLLC of ServiceProfile |
| User management openness | This attribute describes the capability for the NSC to manage their users or groups of users' network services and corresponding requirements. For instance, if NSC Y orders a network slice which is capable to support X users of Y, then Y should be capable to decide which X users could use this network slice. Hence, Y could manage the users, in terms of add, modify or delete users to receive network services provided by the specific network slice. | FFS |
| User data access | Data access: The attribute defines how the network slice (or mobile network) should handle the user data.   Tunnelling mechanism The attribute defines the tunnelling mechanism; how the user data can be delivered to the external private data network. | FFS |
| V2X communication mode | This parameter describes if the V2X communication mode is supported by the network slice. | FFS |

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-09 | SA#85 |  |  |  |  | Change control version | 16.0.0 |
| 2019-09 | SA#86 | SP-191168 | 0005 | - | F | Correct faulty implementation of figure 4.4.3.1 | 16.0.0 |
| 2019-09 | SA#86 | SP-191168 | 0006 | - | F | Implement Edithelp comments | 16.1.0 |
| 2019-09 | SA#86 | SP-191168 | 0007 | - | F | Solutions for Editor's notes | 16.1.0 |