|  |  |
| --- | --- |
| 3GPP TR 28.824 V18.0.0 (2023-06) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on network slice management capability exposure (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| 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 Specification 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. | |

|  |
| --- |
|  |
| ***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.  © 2023, 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 4

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview 6

4.1 General 6

4.1.1 Concepts related to network management capability exposure 6

4.1.2 Roles related to network management capability exposure 8

4.1.3 Types of interface for the exposure of network slice 8

4.1.4 Procedures related to consumption of exposed network management capabilities 11

4.2 Issues 17

4.2.1 Issue #1: Types of NSCs 17

4.2.2 Issue #2: Types of capabilities available for exposure 17

4.2.3 Issue #3: EGMF/MCEG 18

4.2.4 Issue #4: NSC-NSP service interaction 18

4.2.5 Issue #5: Relation to other SA5 work/study items 18

4.2.6 Issue #6: Network slice management capability exposure interface via OSS 19

4.2.7 Issue #7: Capability exposure ecosystem 19

5 Use cases for network management capability exposure 19

5.1 Exposed network slice management capability consumption 19

5.1.1 Description 19

5.1.2 Issue and gaps 20

5.2 Exposure of MnS for monitoring QoS of video application 20

5.2.1 Description 20

5.2.2 Potential issues and gaps 21

5.3 exposed MnS discovery service 21

5.3.1 Description 21

5.3.2 Potential issues and gaps 22

5.4 Exposure of network slice as a product 22

5.4.1 Description 22

5.4.2 Potential issues and gaps 26

5.5 Exposure of network slice as a service 26

5.5.1 Description 26

5.5.2 Potential issues and gaps 29

5.6 Exposure to application servers and application functions 29

5.6.1 Description 29

5.6.2 Issue and gaps 30

6 Potential requirements for network management capability exposure 30

6.1 Potential requirements related to exposed MnS discovery service 30

6.2 Potential requirements related to exposure interface via OSS 31

7 Possible solutions for network management capability exposure 31

7.1 Possible solution for “exposed MnS support to discovery systems” – Scenario 5.4 31

7.2 Possible solutions for exposed MnS discovery service 32

7.3 Potential solution for MnS discovery service for exposure 32

7.4 Potential solution for exposed MnS consumption via OSS interface 33

7.5 Solution for internal service order after receiving product order 35

7.6 Solution for external product order after receiving product order 36

7.7 Solution for external service order after receiving product order 37

7.8 Potential solution for product onboarding 37

7.9 Potential solutions for network slice management capability exposure via CAPIF 38

7.9.1 Exposure via CAPIF alternative 1 38

7.9.2 Exposure via CAPIF alternative 2 38

7.9.3 Exposure via CAPIF alternative 3 42

7.9.4 Evaluation 44

7.10 Possible solution for network slice management capability exposure 45

7.11 Potential solution for consumption of exposed MnS after service order completed 47

7.12 Possible solution for “Exposure to application servers and application functions” – Section 5.8 48

7.13 Possible solution for end-to-end handling of NSC requirements for network slice management capabilities exposure 49

8 Conclusion and Recommendation 50

8.1 Reference Architecture for network slice ordering, provisioning and assurance 50

8.1.1 Conclusion 50

8.1.2 Recommendation 52

8.2 Network slice management capability exposure via CAPIF 53

8.2.1 Conclusion 53

8.2.2 Recommendation 53

8.3 Filtering 53

8.3.1 Conclusion 53

8.3.2 Recommendation 54

8.4 Capability exposure ecosystem 54

8.4.1 Conclusion 54

8.4.2 Recommendation 54

# 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.

# Introduction

This report is to study on network slice management capability exposure.

# 1 Scope

The present document describes use cases, potential requirements and solutions for exposure of management services to external network slice consumers, e.g. verticals and service providers. The present document provides conclusions and recommendations on the next steps for 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] TM Forum TMF622 Product Order API REST Specification

[3] TM Forum TMF641 Service Ordering API

[4] TM Forum TMF652 Resource Order Management API

[5] 3GPP TS 28.531: "Management and orchestration; Concepts, use cases and requirements"

[6] 3GPP TS 28.202: "Charging management; Network slice management charging in the 5G System (5GS); Stage 2"

[7] 3GPP TR23.700-99 “Study on Network Slice Capability Exposure for Application Layer Enablement (NSCALE)”

[8] 3GPP TS23.434 “Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows.”

[9] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3"

[10] 3GPP TS 28.537: "Management and orchestration; Management capabilities"

[11] 3GPP TS 28.533: "Management and orchestration; Architecture framework"

[12] TM Forum TMF633 Service Catalogue Management API

[13] TM Forum TMF620 Product Catalogue Management API

[14] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

[15] 3GPP TS 28.532: "Management and orchestration; Generic Management Service"

[16] 3GPP TS 28.623: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions"

[17] 3GPP TS 28.622: " Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP) Information Service (IS)"

[18] 3GPP TS 28.201: "Charging management; Network slice performance and analytics charging in the 5G System (5GS); Stage 2"

[19] 3GPP TS 29.222: “Common API Framework for 3GPP Northbound APIs”.

[20] 3GPP TS 31.222: “Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs”.

[21] CAMARA: <https://github.com/camaraproject>

[22] GSMA Open Gateway, Feb 2023 [Online]. Link: <https://www.gsma.com/futurenetworks/gsma-open-gateway/>

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

BSS Business Support System

CSP Communication Service Provider

NOP Network OPerator

# 4 Overview

## 4.1 General

### 4.1.1 Concepts related to network management capability exposure

#### 4.1.1.1 Exposed Management Services

Exposed MnS represents the MnS that can be exposed by MnS producer to the external MnS consumer. Exposed MnS may rely on a dedicated MnF (e.g. EGMF defined in 3GPP or function defined in other standard like TMF) that manages the exposure aspects.

NOTE: Whether MnS is exposed to external MnS consumer via BSS or via an exposure platform depends on requirements from third parties’ applications and/or NSP’s policy.

#### 4.1.1.2 Exposure of Management Services

Exposure of management services supports the case that an external MnS consumer which is outside 3GPP management system can indirectly consume management capability offered by MnS producer within 3GPP management system. Even though the exposed MnS complies with the same Technical Specification as an MnS, the actual operational behaviour and managed data may be constrained by the network slice provider.

NOTE: The exposure of MnS data and MnSs to the external MnS consumer may incur additional charging which needs to studied further by 3GPP SA5 charging group.

#### 4.1.1.3 Exposure Governance

Perform access control including Filtering when external MnS consumer consume MnS from 3GPP management system.

To avoid unauthorised management capability consumption, management services should be subject to exposure governance before being exposed to different types of MnS consumers. As introduced in TS 28.533 [11], management capability exposure governance provides exposure governance (i.e. filtering) on basic elements of management function service based interface:

1) Management service component type A

2) Management service component type B

3) Management service component type C

Definitions and typical cases of filtering are given in the following subclauses.

##### 4.1.1.3.1 Filtering

Definition: The exposure access control on certain information elements (i.e. granular access) of MnS component type A, type B and/or type C according to the consumer’s authorization level. For example, the permission of Read, write, the acquisition of notification for certain MnSs.

Typical case 1: Assuming the management service X is a provisioning MnS with operations createMOI, getMOIAttributes, modifyMOIAttributes and deleteMOI as MnS component type A, the filtering on management service X could be that only a subset of original MnS is exposed to MnS consumer, e.g. only operation getMOIAttributes, is exposed to management service consumer.

Typical case 2: Assuming the management service Y is a provisioning MnS with NRM MOIs as the component type B, the filtering on management service Y could be that only a subset of original MnS is exposed to MnS consumer, e.g. only part of the attributes of the NRM MOI, is exposed to management service consumer.

To implement the filtering on MnS, attribute mnsScope of IOC MnsInfo, see further details in TS 28.622 [17], may be used to provide information about the management scope of a Management Service. The management scope is defined as the set of managed object instances that can be accessed (as filtering) using the Management Service.

#### 4.1.1.4 Exposure via BSS

##### 4.1.1.4.1 General

Exposure of service data to companies that are external to the operator are regulated by contracts. Different customers may have access to different management capabilities. It may differ on what attributes/policies/intents are allowed to be changed, which value ranges changes are allowed, and which performance metrics are allowed to be exposed.

The network slice data with the ServiceProfile is located in the Network Management Layer.

Even if the external interface always goes via BSS, there are different scenarios for how a customer, e.g. vertical, can influence the ServiceProfile.

The capabilities required by a Vertical have to be the same on the interface between NOP Network Management Layer and CSP Service manager. The external interface is external to the administrative domain of the operator, while the internal interface is inside the administrative domain of the operator.

##### 4.1.1.4.2 Exposure scenarios

See clause 5.4.1 for detailed description of exposure scenarios/use cases via BSS.

#### 4.1.1.5 Exposure via OSS

##### 4.1.1.5.1 General

Exposure of service data to companies that are external to the operator are regulated by contracts. The exposure usually goes through BSS, as explained in clause 4.1.1.3. However, based on specific contract, the customer may interact with the Operator via OSS. There are different scenarios for how a customer having such contract interacts with Operator for the network slice management capability exposure.

##### 4.1.1.5.2 Exposure scenarios

See clause 5.5.1 for detailed description of exposure scenarios/use cases via OSS.

### 4.1.2 Roles related to network management capability exposure

#### 4.1.2.1 Exposed MnS

The roles related to network management capability exposure are the exposed MnS consumer and exposed MnS producer with the interface for the exposed MnS. The roles and interface are shown in Figure 4.1.2.1.1



Figure 4.1.2.1.1 Roles related to network management capability exposure

#### 4.1.2.2 Exposed MnS consumer

The logical entity consuming management capability offered by an Exposed MnS producer is called an Exposed MnS consumer. An exposed MnS consumer is equivalent to an MnS consumer with the difference that it is outside the trust domain of the CSP or NOP. An exposed MnS consumer is owned by an external customer (e.g. vertical such as Industry, Internet Company, etc) which may take the role of a CSC or NSC. The external customer usually has specific service requirements on a 5G network.

#### 4.1.2.3 Exposed MnS producer

The logical entity offering management capability that can be consumed by an Exposed MnS consumer is called Exposed MnS producer. An exposed MnS producer is owned by a service provider which may take the role of a CSP or NSP.

### 4.1.3 Types of interface for the exposure of network slice

#### 4.1.3.1 Introduction

Different types of interfaces may be used during the whole lifecycle of network slice, including ordering, provisioning, operation phases. These interfaces can be categorized as:

- Inter-organization interfaces (represented East-West):

- Between the organizational entity playing the Network Slice Customer (NSC) role, named Company V here, and the organizational entity playing the Network Slice Provider (NSP) role, named Company A here:

- Interface Type-A to:

- create a product (network slice) order,

- retrieve information concerning a product (network slice) order,

- update a product (network slice) order,

- delete a product (network slice) order;

Candidate APIs for Interface Type-A include, but are not limited to, TMF API 622 (Product ordering).

Interface Type-A is not in the scope of 3GPP.

- Between the organizational entity playing the Network Slice Provider (NSP) role, named Company A here, and the two organizational entities playing the Communication Service Provider (CSP) role, acting as ‘partners’ and named Company X and Company Y respectively here

- Interface Type-X to:

- create a product order,

- retrieve information concerning a product order,

- update a product order,

- delete a product order;

Candidate APIs for Interface Type-X include, but are not limited to, TMF API 622 (Product ordering).

Interface Type-X is not in the scope of 3GPP.

- Intra-organization interfaces (represented North-South), internal to the organizational entity playing the Network Slice Provider (NSP) role:

- Between its BSS and its OSS/SML

- Interface Type-1 to:

- create a service order,

- retrieve information concerning a service order,

- update a service order,

- delete a service order;

Candidate APIs for Interface Type-1 include, but are not limited to, TMF API 641 (Service ordering).

Interface Type-1 is not in the scope of 3GPP.

- Between its OSS/SML and its OSS/NML

- Interface Type-2 to:

- create a network slice / network slice subnet,

- retrieve information concerning a network slice / network slice subnet,

- update a network slice / network slice subnet,

- delete a network slice / network slice subnet,

- collect PM and FM data concerning a network slice / network slice subnet;

Candidate APIs for Interface Type-2 include, TS 28.531, TS 28.532, TS 28.545, TS 28.550.

Interface Type-2 is in the scope of 3GPP/SA5.

The following clauses describe a non-exhaustive set of use cases.

In case of additional use cases, new types of interfaces may be needed.

#### 4.1.3.2 Use case No.1: simple case

In this use case, Company-V (as the NSC) chooses a product from Company-A product offerings and sends a request to Company-A to order the product which is a network slice via Interface Type-A.

As Company-A can satisfy Company-V’s requirements by itself, it doesn’t have to count on partners.

In this use case, Interface Type-A, Type-1 and Type-2 are involved.

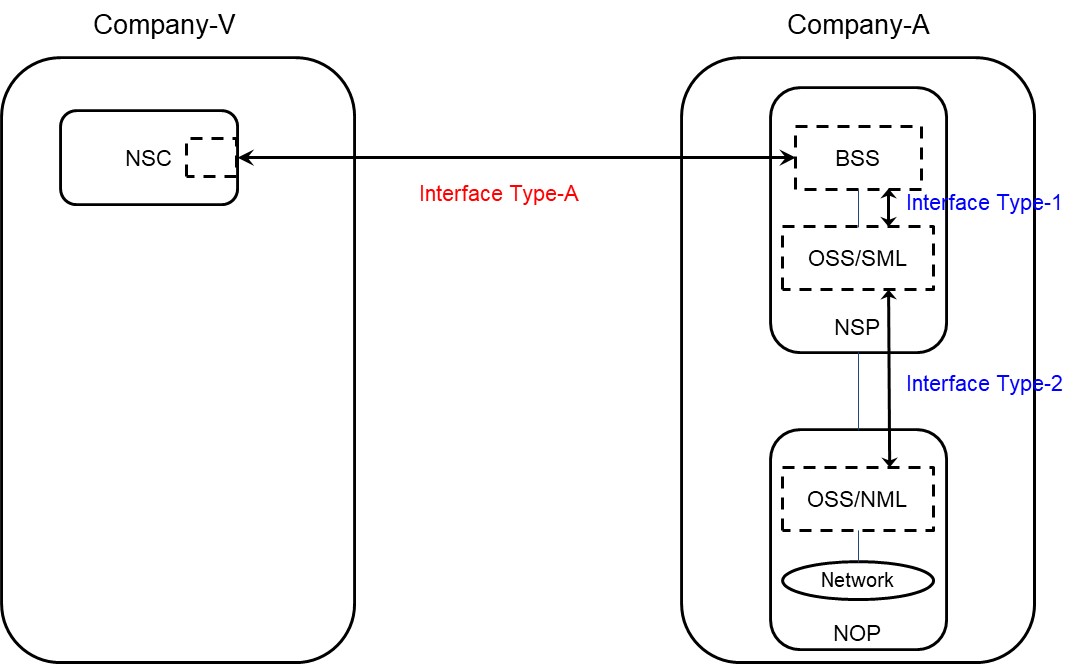


Figure 4.1.3.2.1 Use case No.1: simple case

#### 4.1.3.3 Use case No.2: partners involved

In this use case, Company-V (as the NSC) chooses a product from Company-A product offerings and sends a request to Company-A to order the product which is a network slice via Interface Type-A.

As Company-A can’t satisfy Company-V’s requirements by itself, it has to count on partners (Company-X and Company-Y), e.g. to provide RAN coverage in their respective countries.

In this use case, Interface Type-A, Type-1, Type-2 and Type-X are involved.

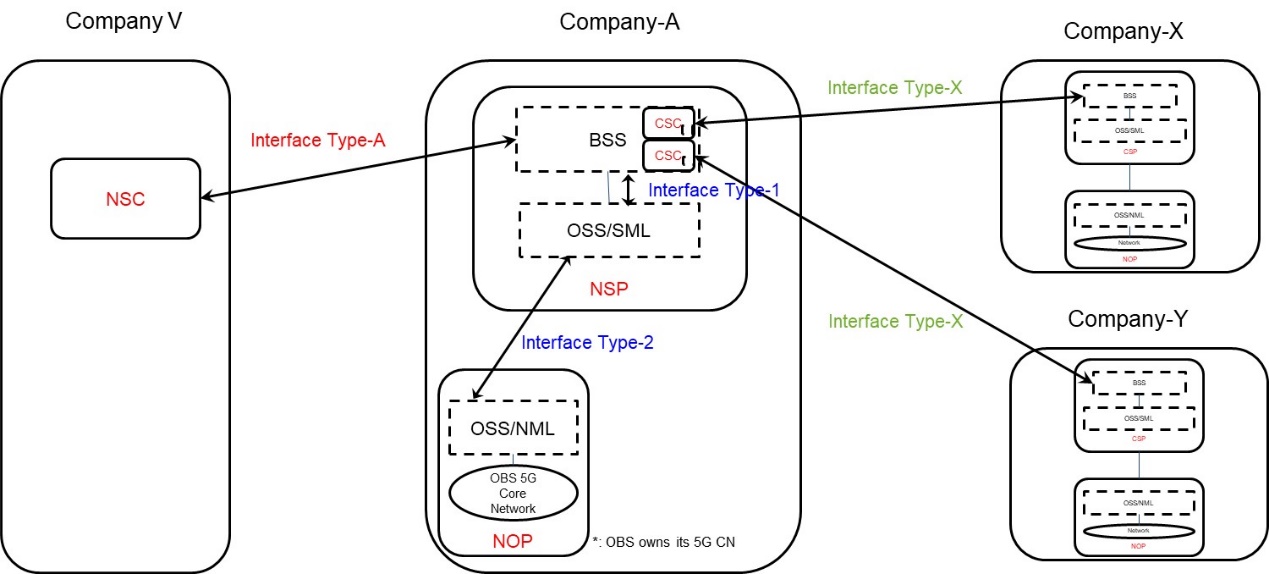


Figure 4.1.3.3.1 Use case No.2: partners involved

### 4.1.4 Procedures related to consumption of exposed network management capabilities

#### 4.1.4.1 Introduction

When an NSP receives an order from an NSC for a network slice enabled product, the order is decomposed by the NSP’s BSS. Depending on whether the NSP employs services from 3rd party CSP’s different procedures may apply for the same order. The different procedures applicable to the same order may be invoked asynchronously and treated as independent procedures, however it may not result in loss of traceability between the original order and the orders that are created as result of decomposition. The following procedures have been identified:

- Procedure invoking internal service order after receiving product order from NSC

- Procedure invoking external product order after receiving product order from NSC

- Procedure invoking external service order after receiving product order from NSC

- Procedure for create product

- Procedure for consumption of exposed MnS after service order is completed

#### 4.1.4.2 Procedure invoking internal service order after receiving product order from NSC

The procedure for invoking a service order internal to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.2.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.2.1 are described in the subsequent paragraphs.

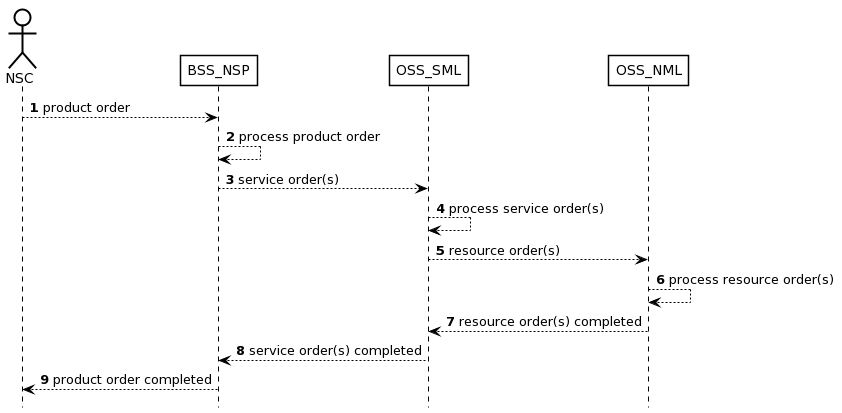


Figure 4.1.4.2.1 Procedure invoking internal service order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

2) The BSS processes the product order and when applicable converts it to appropriate service order(s) for the OSS Service Management Layer. This is internal to BSS and there are no interface requirements.

3) The OSS Service Management Layer receives a service order from the BSS. The interface between the BSS of the NSP and the OSS\_SML of the NSP is used.

4) The OSS Service Management Layer processes the service order and when applicable converts it to appropriate request(s) for the OSS Network Management Layer as requests for management and orchestration of resources. This is internal to the OSS Service Management Layer and there are no interface requirements.

5) The OSS Network Management Layer receives a request from the OSS Service Management Layer. An interface between the OSS Service Management Layer and OSS Network Management Layer may be used.

6) The OSS Network Management Layer processes the request and when applicable converts it to appropriate request(s) for the network. An interface between the OSS Network Management Layer and Network Layer (not shown) may be used.

7) The OSS Network Management Layer notifies the OSS Service Management Layer that the resource order(s) have been completed. An interface between the OSS Service Management Layer and the Network Layer may be used.

8) The OSS Service Management Layer notifies the BSS that the service order has been completed. The interface between the OSS Service Management Layer and the BSS is used.

9) The BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order. The interface between the NSC and the BSS is used.

#### 4.1.4.3 Procedure invoking external product order after receiving product order from NSC

The procedure for invoking a product order external to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.3.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.3.1 are described in the subsequent paragraphs.

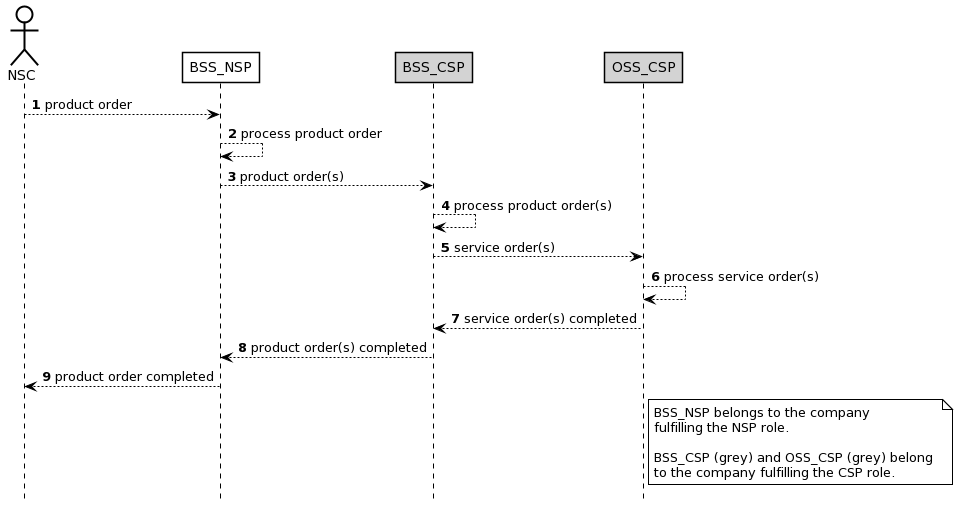


Figure 4.1.4.3.1 Procedure invoking external product order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

2) The NSP BSS processes the product order and when applicable converts it to appropriate product order(s) towards a 3rd party CSP BSS. This is internal to BSS and there are no interface requirements.

NOTE: When the BSS\_NSP receives a product order, the BSS\_NSP splits the product order into service orders. A service order that can be fulfilled by the NSP will be processed by the NSP\_OSS\_SML (see also Figure 4.1.4.2.1) while a service order that cannot be fulfilled by NSP will be ordered from the CSP through a product order.

3) The CSP BSS receives a product order from the NSP BSS. The interface between the BSS of the CSP and the BSS of the NSP is used.

4) The CSP BSS processes the product order and when applicable converts it to appropriate service order(s) for the CSP OSS. This is internal to the BSS and there are no interface requirements.

5) The CSP OSS receives a service order from the CSP BSS. The interface between the BSS and the OSS both belonging to the CSP is used.

6) The CSP OSS processes the service order until the service order is completed.

7) The CSP OSS notifies the CSP BSS that the service order has been completed. The interface between the OSS and the BSS both belonging to the CSP is used.

8) The CSP BSS notifies the NSP BSS that the product order has been completed. The interface between the BSS of the CSP and the BSS of the NSP is used.

9) The BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order.

#### 4.1.4.4 Procedure invoking external service order after receiving product order from NSC

The procedure for invoking a service order external to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.4.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.4.1 are described in the subsequent paragraphs.

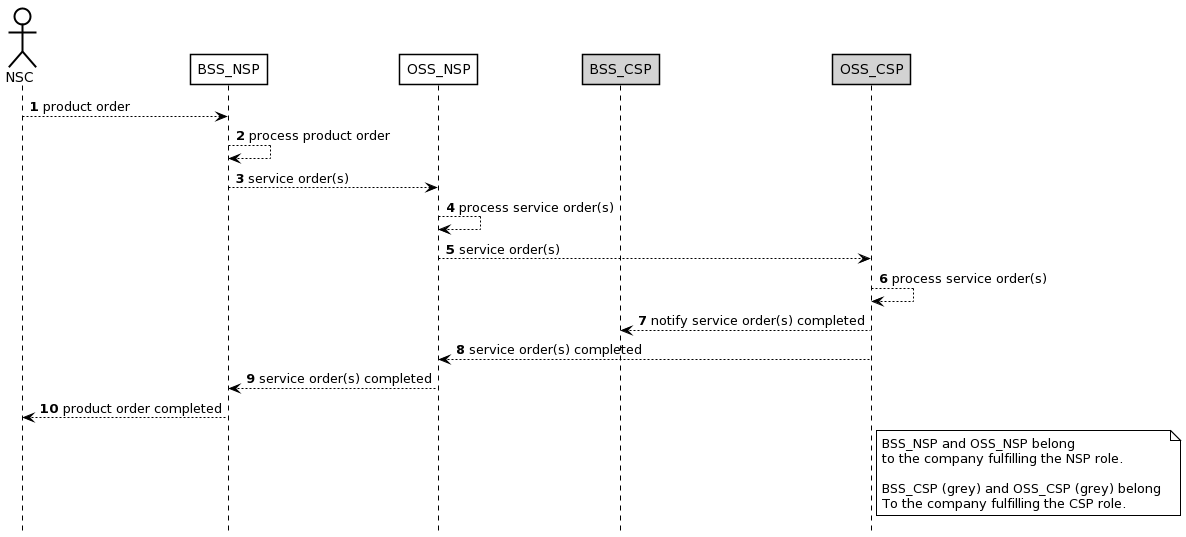


Figure 4.1.4.4.1 Procedure invoking external service order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

2) The NSP BSS processes the product order and when applicable converts it to appropriate service order(s) for the OSS producer. This is internal to BSS producer and there are no interface requirements.

3) The NSP OSS receives a service order from the NSP BSS. The interface between the OSS and the BSS, both belonging to the same NSP, is used.

4) The OSS processes the service order and when applicable converts it to appropriate service order(s) for a 3rd party CSP OSS. This is internal to the OSS producer and there are no interface requirements.

5) The CSP OSS receives a service order from the NSP OSS producer. The interface between the OSS of the CSP and the OSS of the NSP is used.

6) The CSP OSS processes the service order until the service order is completed. This is internal to the OSS producer and there are no interface requirements.

7) The CSP OSS notifies the CSP BSS that the service order has been completed. The interface between the OSS and the BSS, both belonging to the same CSP, is used.

8) The CSP OSS notifies the NSP OSS producer (may occur at the same time as or before step 7) that the service order has been completed. The interface between the OSS of the CSP and the OSS of the NSP is used.

9) The NSP BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order.

#### 4.1.4.5 Procedure for product onboarding

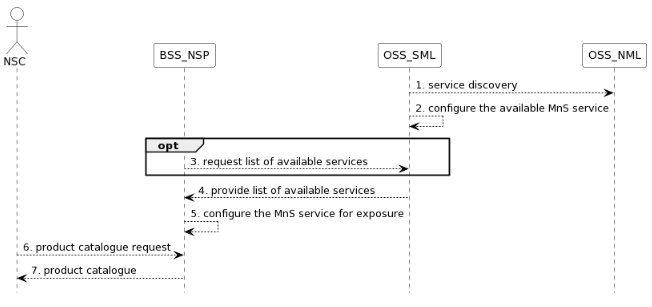


Figure 4.1.4.5.1 Procedure related to product onboarding

1) OSS\_SML obtains 3GPP management services in the network through management service discovery;

2) OSS\_SML governs the rules and policies of MnS and configures the available MnS (e.g. exposed MnS) to BSS\_NSP. For example, if the RAN NE is dedicated to external customers, the performance monitoring service of a RAN NE should be exposed. Otherwise, it should not be exposed;

3) Optionally, the BSS\_NSP may send information to request the list of available services from OSS\_SML;

4) OSS\_SML provides the list of available services to BSS\_NSP;

5) BSS\_NSP configures (groups or package the services into a product) the services from OSS\_SML such that they can be exposed to NSC;

6) NSC should request the product catalogue from BSS\_NSP.

7) BSS\_NSP provides product catalogue to NSC.

#### 4.1.4.6 Procedure for consumption of exposed MnS after service order is completed

The procedure for consumption of an exposed MnS after the product and service orders are completed is shown in figure 4.1.4.6.1. The MnS is produced by the MnS producer located in the OSS of the NSP.

An MnS may already be produced before CAPIF 1 service is requested. The CAPIF 2/2e service is a filtered, enriched and/or converted version of the MnS. The transformation, filtering, enrichment, or conversion of MnS APIs into service APIs is optional. The details of how this transformation, filtering and/or enrichment are to be done are out of scope of SA5.

Editor’s Note: There exist initiatives such as CAMARA [21] which are working in this translation.

Filtering is removing of information elements (attributes and classes), enrichment is adding information elements from other MnSs or other sources outside OAM, and converting is changing information elements through for example combining or mapping information elements. The CAPIF 2/2e service is provided by the API\_Provider\_domain\_function and consumed by the NSC\_Application. The API\_Provider\_domain\_function uses the MnS(s) produced to provide the CAPIF 2/2e service.

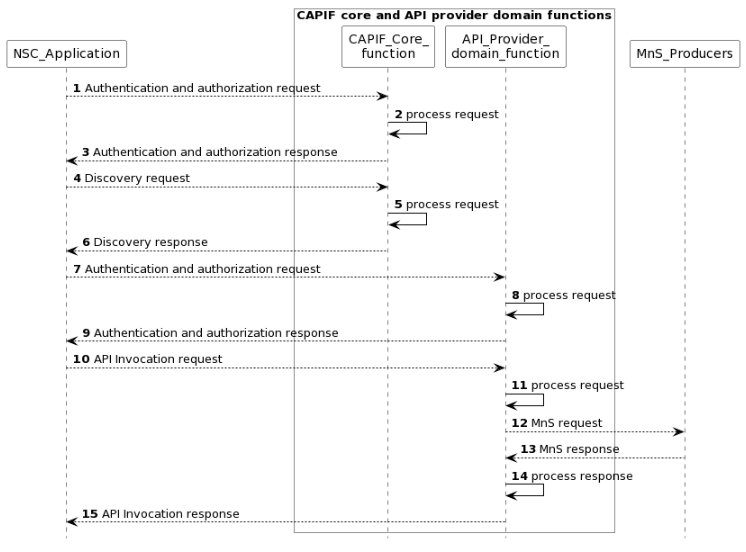


Figure 4.1.4.6.1 Procedure for consumption of exposed MnS after service order is completed

NOTE1: For simplicity reasons the CAPIF Core function and API Provider domain function defined in TS 23.222 [14] are combined and any communication between them is also not included.

NOTE2: The procedure is only applicable to “Exposure via CAPIF alternative 1” described in clause 7.9.1.

1) The CAPIF\_Core\_function receives an authenticating and authorization request from the NSC\_Application based on the identity and other information required for authentication and authorization of the NSC\_Application.

2) The CAPIF\_Core\_function processes the authentication and authorization request.

3) The CAPIF\_Core\_function provides the response with the result of the authentication and authorization to the NSC\_Application.

4) The CAPIF\_Core\_function receives a request for the discovery of service APIs information.

5) The CAPIF\_Core\_function processes the discovery request.

6) The CAPIF\_Core\_function provides the appropriate response to the NSC\_Application.

7) The API\_Provider\_domain\_function receives an authentication and authorization request from the NSC\_Application based on the identity and other information required for authorization of the NSC\_Application.

8) The API\_Provider\_domain\_function processes the authorization request.

9) The API\_Provider\_domain\_function provides the response with the result of the authentication and authorization to the NSC\_Application.

10) The API\_Provider\_domain\_function receives a request for the invocation of the service API(s) from the NSC\_Application.

11) The API\_Provider\_domain\_function processes (and optionally may enrich and/or convert) the invocation request.

12) The MnS\_Producers receive requests from the API\_Provider\_domain\_function for MnS.

13) The MnS\_Producers provide the appropriate responses to the API\_Provider\_domain\_function.

14) The API\_Provider\_domain\_function processes (and optionally may filter, enrich and/or convert) the response from the MnS\_Producers.

15) The API\_Provider\_domain\_function provides the appropriate response to the NSC\_Application.

NOTE: Each response in the steps does not always need to trigger the next request.

## 4.2 Issues

### 4.2.1 Issue #1: Types of NSCs

The problem of network slice capability exposure is mostly relevant for B2B/B2B2C market, where Network Slice as a Service (NSaaS) [1] model applies. In this regard, different types of NSCs can be found.

- Baseline vertical customer: it corresponds to a NSC which is only interested in monitoring the network slice, to verify it behaves as expected, according to the SLA. This NSC does typically have no telco experience, and is associated to a network slice that is entirely deployed on a PLMN. The capabilities offered to a baseline vertical customer includes the ability for this NSC to receive information on subscribed items, including network slice status (e.g. active, inactive) and subscribed management data (e.g., KPIs, events/logs, trace data, etc.). The profile of this NSC type is a ‘passive NSC’.

- Advanced vertical customer: it corresponds to an NSC which requests (to the NSP) a dedicated network slice for the provision of PNI-NPN services. In this scenario, a portion of the network slice is deployed within the NSC premises (e.g., RAN, UPF) and the other portion (e.g., 5GC control plane functions) is hosted by one or more PLMN nodes. Unlike the baseline vertical customer, this new NSC does typically have (yet limited) telco knowledge, and wants to retain certain control over the allocated network slice. The capabilities offered to an advanced vertical customer might include (i) monitoring capabilities, i.e. the same capabilities offered to a baseline vertical customer and (ii) device configuration capabilities, i.e. provision of parameters for battery, mobility and communication patterns associated to the device, (iii) edge discovery/selection, e.g. in case the vertical wants to deploy workloads on the telco edge cloud.

- Hyperscaler: it corresponds to a NSC which requests (to the NSP) a dedicated network slice to provide a service-tailored connectivity pipe to a NSC’s customer. With some enterprises (i.e., NSC’s customer) starting to migrate workloads towards hyperscaler nodes, it is necessary for the hyperscaler (i.e., NSC) to provide SLA guarantees to these enterprises, especially for critical processes/services. However, the hyperscaler does not have network resources between its cloud nodes and customer premises, and therefore has to ask the mobile network operator (i.e., NSP) to set up a network slice between these endpoints. The capabilities offered to a hyperscaler might include (i) monitoring capabilities, i.e., the same capabilities offered to a baseline vertical customer; (ii) quality on demand, i.e. dynamic QoS and bandwidth management; (iii) policy control.

- Mobile (Virtual) Network Operator.

NOTE 1: In all the above cases, the NSP role is assumed to be played by an MNO.

NOTE 2: The capabilities mentioned above are neither exhaustive nor accurate, but examples to motivate the need for considering different NSC types.

The NSC types within the scope of FS\_NSCE should be use case driven.

### 4.2.2 Issue #2: Types of capabilities available for exposure

When referring to the capabilities a NSC might be interested to consume, we have three big groups of capabilities that a NSP can make available for consumption:

- Application layer capabilities, not in the scope of the present document.

- Management layer capabilities.

- Network layer capabilities, not in the scope of the present document.

There is the need to have one single exposure layer to make all the capabilities available for NSCs. This exposure layer should integrate network layer capabilities (@NEF), management layer capabilities (@MCEG), application layer capabilities (@SEAL), together with non-3GPP capabilities (e.g. cloud related capabilities). Otherwise, if 3GPP starts defining different exposure fabrics, (i) the likelihood of encountering incompatibilities/duplicities across these specific solutions is high; (ii) the operators may come up with increased integration efforts, which ultimately may make their systems very hard to build and maintain.

### 4.2.3 Issue #3: EGMF/MCEG

The Exposure Governance Management Function (EGMF) was originally defined in TS 28.533 [11] as an MnF providing management capability exposure governance (MCEG). However, the current definition needs more elaboration on the following questions:

- The functional scope of management capability exposure governance, and its relationship with the access control and with existing API GW solutions in carrier networks.

- The impact of management capability exposure governance on the Network Slice NRM fragment. Is it within the scope of SA5 or not? If in-scope, then:

- what NSC related information (e.g., NSC id, NSC granted capabilities) does the NSP send to the NOP?

- how does the NOP manage this information in relation to the existing NetworkSlice and NetworkSliceSubnet IOCs?

- The need to standardize EGMF. Does 3GPP really need to define this MnF? Doesn’t this approach mean moving away from producer centric model of 3GPP, i.e., focus on service producers rather than MnFs?

- If EGMF standardization is within the scope of 3GPP, then does 3GPP need to provide details on EGMF internals? Does 3GPP need to decide whether the EGMF is positioned on the Network Management Layer (NML), or the Service Management Layer (SML), or BSS layer?

### 4.2.4 Issue #4: NSC-NSP service interaction

The NSC-NSP service interactions work (i.e., APIs made available by the NSP, for consumption by the NSCs) is out of the 3GPP scope. Based on the proposal #2, which argues in favour of having one single exposure layer integrating 3GPP capabilities and non-3GPP capabilities, together with the fact that a high number of NSCs are not familiar with 3GPP models, it makes sense to let these interactions be covered in other industry fora.

Editor's note: The potential group to provide the single exposure layer is FFS.

### 4.2.5 Issue #5: Relation to other SA5 work/study items

The work conducted in the FS\_NSCE is related to other Rel-17 SI/WIs, including:

- MSAC (Management Service Access Control), on the access control aspects inherent to exposure to 3rd parties. NSP shall expose capabilities to NSCs in a controlled, secure and auditable way.

- OAM\_NPN (Management of Non-Public Networks), when the network slice is used for the provisioning of a PNI-NPN. In this case, the modes 1b defined in [3] applies.

- eMEMTANE (Management of enhanced tenant concept), on the need to associate tenants to different NSCs, and manage the corresponding information in the NRM.

- 5GDMS (Discovery of management services in 5G), on the need for NSCs to discover capabilities available for consumption.

The work in FS\_NSCE is to leverage outcomes from the Rel-17 study/work items which are listed above. It seems these study/work items provides most (if not all) the ingredients for the network slice capability exposure topic, so the mission of FS\_NSCE should be to find out the recipe to combine them and provide overall exposure picture.

### 4.2.6 Issue #6: Network slice management capability exposure interface via OSS

Scenarios regarding exposure interface via OSS have been introduced in clause 4.1.1.4. NSC can make contract with the NSP or CSP regarding exposure via BSS. Upon the completion of the contact, the NSC can directly get access to the OSS within the NSP or CSP for access the exposed MnS. Several key issues exist for the use cases. For example, how does the NSC identify the address of MnS producer for the exposed MnS within the OSS and how to consume the exposed MnS directly from OSS needs to be addressed.

### 4.2.7 Issue #7: Capability exposure ecosystem

Capability exposure paves the way for transforming telco networks into programmable service platforms that can be easily accessed by 3rd parties, including application developers, aggregator marketplaces and enterprise customers, through APIs. This new paradigm, referred to Network-as-a-Service (NaaS), enables these 3rd parties (and their applications) to consume exposed telco capabilities, tapping into them to provide enhanced user experiences and contribute to service innovation with new use cases.

The development of NaaS requires a collaborative workspace that bring together incumbent telco standards bodies with IT and cloud communities, industry associations and open-source projects. An effective collaboration among organizations needs to be based on a clear demarcation on their scope of work, avoiding that participating organizations run overlapping activities or duplicate efforts; otherwise, NaaS may risk ending up with a fragmented ecosystem. With this goal in mind, GSMA Open Gateway initiative [22] has defined a reference NaaS framework built on three main organizations:

**- Linux Foundation’s** **CAMARA**: it represents the “exposure” doctrine, i.e., how capabilities are exposed for external consumption via 3rd party facing APIs. CAMARA defines these APIs, and is responsible for their hosting and release management. Third-party facing APIs are user-friendly (semantics tailored to the service needs of 3rd parties) and open (following Apache2.0 license).

**- GSMA Open Gateway**: it represents both the “technical” doctrine, i.e., how third-party facing APIs are to be supported by underlying telco capabilities, and “business” doctrine, i.e. definition of templates for agreements between operators and 3rd parties, ensuring a consistent commercial framework for exposing services. GSMA conducts the technical work through OPG/OPAG (Operator Platform Group / Operator Platform API Group), and the commercial work through WAS (Wholesale Agreement Services).

**- TM Forum**: it represents the “operational” doctrine, i.e., how to manage capabilities throughout the entire NaaS lifecycle. This includes the registration/onboarding of 3rd parties, service fulfilment (e.g., provisioning, activation and modification), service assurance (e.g., incident management, service status, service performance) and billing.

# 5 Use cases for network management capability exposure

## 5.1 Exposed network slice management capability consumption

### 5.1.1 Description

A use case of exposed network slice management capability consumption can be described as follows:

1. In order to enable the consumption of network slice related exposed MnS, an NSC firstly makes a contract with the NSP, which contains the agreement and conditions for consuming an exposed MnS. The condition can be a certain constraint of exposed MnS consumption based on the contract, e.g. the usage quota of certain exposed MnS, the usage frequency of certain exposed MnS, etc. The NSC negotiates its specific requirements for the network slice management capability consumption with the NSP. Based on the contract, NSP selects the MnS that can be exposed externally and decides on exposure policies that shall be applied to the MnS when it is exposed externally. For example, NSP may decide to disallow certain operations, limit the Managed Object Instances that may be managed, or aggregate/anonymize sensitive data.

2. The BSS may interact with the OSS in order to complete certain configuration (i.e. permission regarding what exposed MnS, optionally under what condition, can be consumed) regarding the consumption of exposed MnS based on the customized requirement from the NSC.

3. The MnS can be exposed directly or NSP applies any policies before exposing the resulting functionality as an MnS.

4. NSP publishes the MnS in a service directory so that the NSC is able to discover the exposed MnS.

5. NSP authenticates NSC to consume the exposed MnS as defined in the contract, and provides the relevant authorization keys to NSC.

6. After successful authorization verification, NSC requests to access the exposed MnS. The MnS can be exposed originally as it is for internal consumption or NSP applies any constrains before exposing the limited functionality as a MnS. The access may need the interaction with BSS (e.g. through Service Catalogue) or the access can directly go through OSS.

### 5.1.2 Issue and gaps

#### 5.1.2.1 Issues

How to publish MnS which can be exposed to BSS to a suitable MnS producer for network management capability exposure is not specified in existing 3GPP management system.

NSC needs to apply for the access of network slice management capability through BSS. However, there is no discussion and agreement on whether an exposed MnS is exposed transparently through the BSS or being processed through a dedicated exposure platform before exposing to the NSC.

The definition and the format of permission (authorization) for the consumption of network slice related exposed MnS and its potential impact on internal interface with BSS is not discussed in current SA5 work.

5.1.2.1 Gaps

1) How to publish a MnS.

2) How an external consumer can discover the available MnS;

3) And, how to define exposure policies that shall be applied when an MnS is accessed by an external consumer is not specified in existing 3GPP management standards.

## 5.2 Exposure of MnS for monitoring QoS of video application

### 5.2.1 Description

A use case of exposure of MnS for monitoring QoS of video application can be described as follows:

1. A live concert with high-resolution video application service is provided with service provider A (i.e. associate to exposed MnS consumer). A local hosting network (e.g. SNPN) is available and provides localized services for high-resolution video service of the concert. The local hosting network is managed by the service provider A. The high-resolution video streaming service of the live concert is available from both the local hosting network and PLMN. Service provider A and the provider of PLMN (i.e. associate to exposed MnS provider) are two different parties.

2. The service provider A of the local hosting network can have an offer from the Operator of PLMN before identifying the correct MnS for exposure through BSS (e.g. by using Product Catalog). The BSS may obtain the information of MnS that is allowed to be exposed using a MnS service for exposure provided by OSS. The contract may contain the agreement on the exposure of MnSs for consuming certain management MnS related to QoS. According to the contract, the service provider A can have the permission to use the MnS for consuming certain performance MnS related to QoS for the PLMN. The performance MnS can be related to NR and 5GC, e.g. Average DL UE throughput in gNB. For the hosting network, the service provider may have contract with the Network Operator which can offer network management service for the hosting network. The network management service may be offered by a management system that belongs to a service platform of the Network Operator. Due to the contract, the service provider can access the management system directly without going through BSS.

3. Once the offer has been accepted, the corresponding exposure governance management service within the 3GPP management system (of the Operator of PLMN) is configured with permission rule through the interface between BSS and OSS. The permission rule defines that the provider of the local hosting network can have the right to access certain management MnS regarding QoS.

4. Through obtaining the measurement MnS using exposure capability, the provider of the local hosting network can determine the situation when PLMN cannot support the high-resolution video service with satisfied QoS. In this case, the service provider A can notify its customers about the local hosting network that may improve the QoS of the high-resolution video application.

### 5.2.2 Potential issues and gaps

#### 5.2.2.1 Issues

Whether and how to expose MnS directly from OSS is not specified in existing 3GPP management system.

The definition and the format of the permission rule (authorization) for the network management capability exposure regarding NR and 5GC related performance MnS is not specified in existing 3GPP management system.

Whether and how to publish MnS which can be exposed to an external party from a suitable MnS service producer for the exposure of performance MnS regarding NR and 5GC is not specified.

#### 5.2.2.2 Gaps

If there is a need to publish MnS, then the exposure of performance MnS regarding NR and 5GC is not specified in 3GPP management system.

## 5.3 exposed MnS discovery service

### 5.3.1 Description

An exposed MnS should be allowed to register to a trusted discovery service entity (e.g. a discovery MnS producer or an authorized supported discovery system) such that interested authorized consumers (within or external to the operator) are able to discover it. This implies that the exposed MnS is only exposed to a discovery service entity where a pre-existing contract allows for such an exposure.

A use case of exposed MnS discovery service is described as follows:

1. MNO A provides exposed MnSs from 3GPP management system for external customers and these exposed MnSs go through BSS/OSS for exposure.

2. In order to provide such discovery service to external customer, MNO A registers its exposed MnS to a trusted discovery service entity. MNO A configures the exposed MnS with the discovery entity’s address and the exposed MnS is registered at the discovery service entity with the appropriate level of exposure.

3. MNO A performs changes in its management system that impacts the information exposed by the exposed MnS. The changed information is automatically updated in the discovery service entity.

4. In case the relationship between MNO A and a discovery service entity (especially for the discovery system) ends, which implies the discovery service entity is no longer trusted, MNO A deregisters its exposed MnS to the discovery service entity. MNO A removes the configuration of the discovery entity’s address for exposed MnS and the exposed MnS is deregistered at the discovery service entity before the trusted discovery service entity becomes a no longer trusted entity.

### 5.3.2 Potential issues and gaps

#### 5.3.2.1 Issues

Study is needed whether the exposed MnS discovery service is to be provided by the MnS discovery service producer, by a dedicated exposed MnS discovery service producer (e.g. EGMF) or by a trusted discovery system.

Study is needed on whether the MnS data as defined in TS 28.533 [11] can also be re-used for exposed MnS data, or if any extensions are necessary.

Study is needed on figuring out differences if the discovery system is external or internal to the operator.

Discovery of service and consumption of a discovered service can be completely separated. However, there may be an issue with managing which consumers have access to the discovery system and could theoretically consume the management service when authorization rules are not respected.

There is an issue with authentication and authorization between the three parties i.e. MnS producer/operator, MnS consumer/customer and discovery system owner.

#### 5.3.2.2 Gaps

To limit issues the exposure from a discovery system of the operator may only provide “read” permissions (w.r.t the exposed MnS) without authentication and authorization. To execute the discovered exposed MnS the consumer still needs to be authenticated and authorized by the management system. Therefore, there is a gap in the difference in exposure for consumption, and exposure for discovery which needs to be solved.

Editor’s Note: Whether or not the issue with a third-party discovery system should be solved only for MnSs or for any 3GPP exposed service is FFS.

## 5.4 Exposure of network slice as a product

### 5.4.1 Description

This use case involves the following roles:

- NSP: Network Slice Provider

- NSC: Network Slice Customer

- NOP: Network Operator

- CSC: Communication Service Customer

- CSP: Communication Service Provider

, and the following systems:

- BSS: Business Support System

- OSS: Operations Support System, made up of the two following sub-systems:

- SML: Service Management Layer

- NML: Network Management Layer (for sake of simplicity, network management and network element / function management are both in the NML).

#### 5.4.1.1 Sub-use case 1: NSP and NOP played by the same organization

In this scenario, the following organizations play aforementioned roles as follows:

- Company-V plays the role of NSC

- Company-A plays the role of NSP and NOP

- As NSP, it has:

- a BSS, e.g. to manage its customers, products, contracts, and

- a SML, to manage the services that support its products

- As NOP, it has:

- its own 5G network (RAN + core). In this sub-use case, Company-A owns the whole set of network resources used by the service required to support the product ordered by Vertical V

- a NML, to manage the network resources used by services

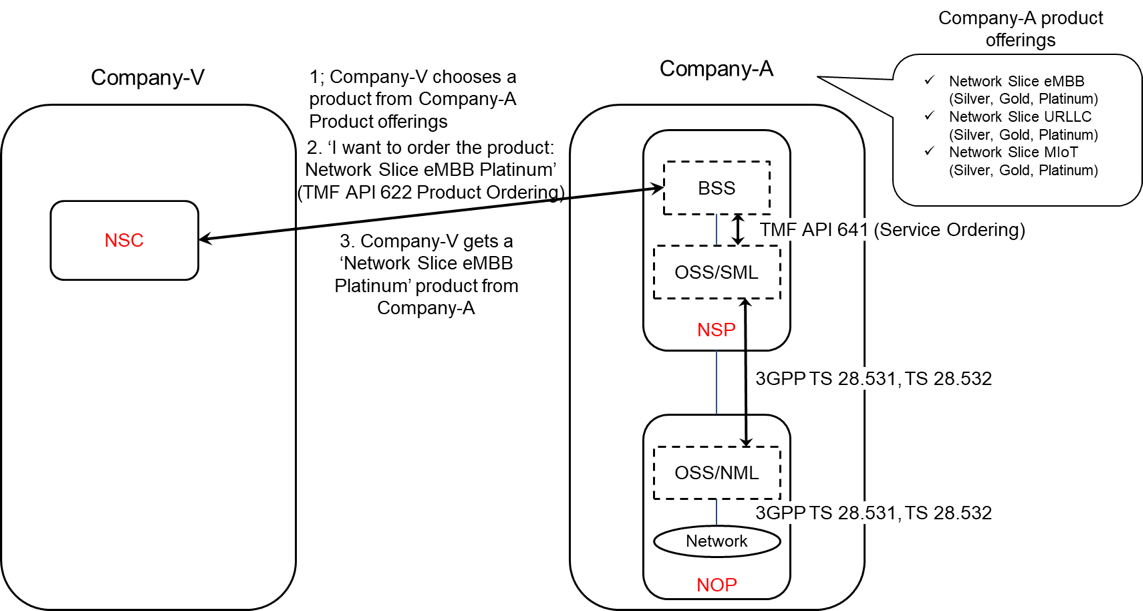


Figure 5.4.1.1-1: Sub-use case 1 - NSP and NOP played by the same organization

Company-A product catalogue proposes the following product offerings:

- Network Slice eMBB with different flavours: Silver, Gold, Platinum

- Network Slice URLLC with different flavours: Silver, Gold, Platinum

Network Slice MIoT with different flavours: Silver, Gold, Platinum.

In this sub-use case 1:

1. Company-V (as the NSC) chooses a product from Company-A product offerings

2. Company-V sends a request to Company-A (as the NSP) to order the product ‘Network Slice eMBB Platinum’. To achieve this, a candidate API is TMF API 622 (Product Ordering)

2.1 Company-A BSS determines which service supports the product being ordered by Company-V and issues a request to its OSS/SML to order this service. This service can be e.g. a network slice. To achieve this, a candidate API is TMF API 641 (Service Ordering)

2.2 OSS / SML determines which network resources support the service being ordered and issues a request to the OSS / NML to allocate required network resources, e.g. network slice subnet(s), network functions, etc. To achieve this, candidate APIs are from TS 28.531 and TS 28.532

2.3 OSS / NML allocates network resources required to support the service and informs OSS / SML back about the characteristics of the network resources being allocated

2.4 OSS / SML associates the allocated network resources to the service and informs its BSS back about the characteristics of the service supporting the product

3. Company-A (as the NSP) sends a reply to Company-V to inform that the product ordered is now available to Company-V.

NOTE: in this use case, aspects related to Transport Network(s) are not addressed as they are out of 3GPP scope.

#### 5.4.1.2 Sub-use case 2: NOP role played simultaneously by different organizations

In this scenario, the following organizations play aforementioned roles as follows:

- Company-V plays the role of NSC

- Company-A plays the role of NSP and NOP

- As NSP, it has:

- a BSS, e.g. to manage its customers, products, contracts, and

- a SML, to manage the services that support its products

- As NOP, it has:

- its own 5G core network. In this sub-use case, Company-A owns the whole set of 5G core network resources used by the service required to support the product ordered by Vertical-V

- a NML, to manage the 5G core network resources used by services

As Company-A has no RAN in all requested areas, it relies on external organizations, namely Company-X and Company-Y, to provide RAN coverage in the US and in Spain respectively. Therefore:

- Company-A plays the role of Communication Service Customer (CSC) wrt. Company-X and Company-Y who both play the role of Communication Service Provider (CSP)

- Both Company-X and Company-Y have their own catalogue of products to offer RAN coverage in their respective countries

- Both Company-X and Company-Y play the role of CSP (for their respective product offerings) and NOP (for their respective RAN).

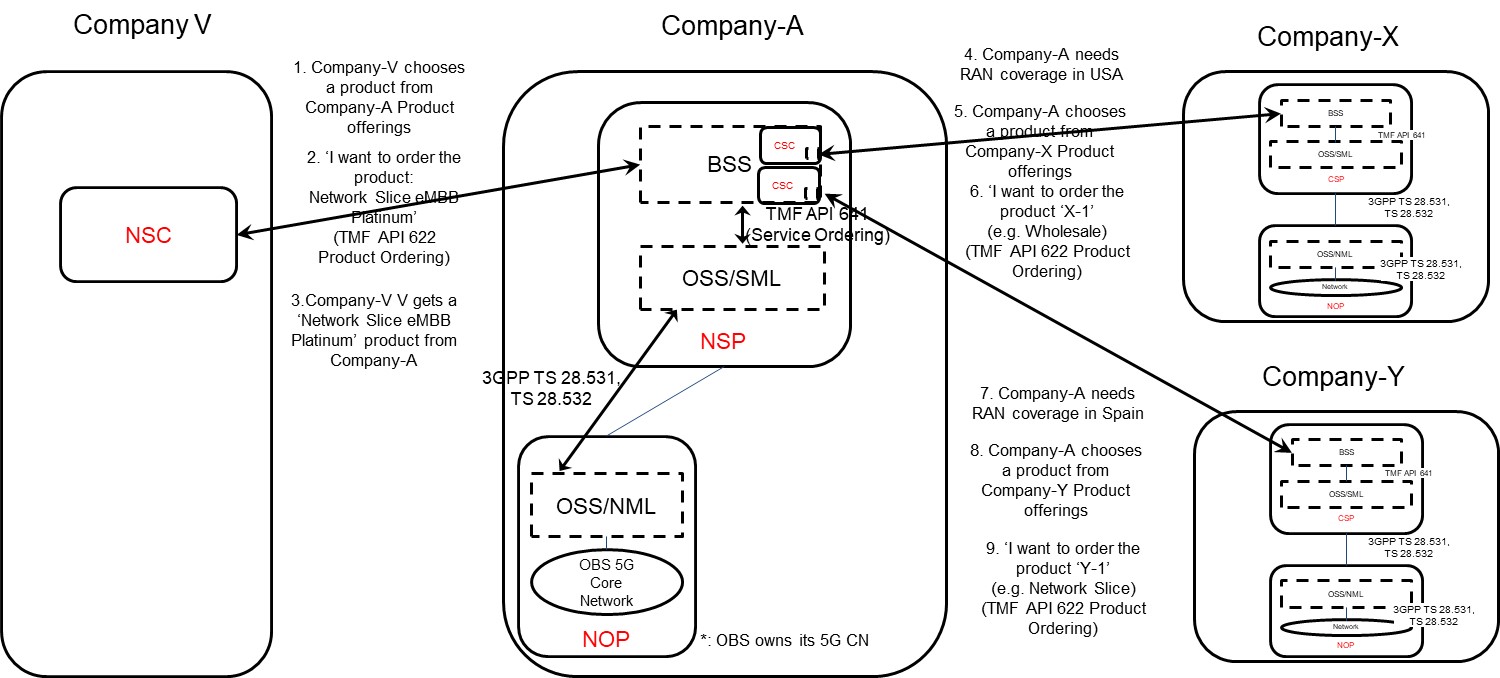


Figure 5.4.1.2-1: Sub-use case 2 - NOP role played simultaneously by different organizations

Company-A product catalogue proposes the following product offerings:

- Network Slice eMBB with different flavours: Silver, Gold, Platinum

- Network Slice URLLC with different flavours: Silver, Gold, Platinum

Network Slice MIoT with different flavours: Silver, Gold, Platinum.

In this sub-use case 2:

1. Company-V (as the NSC) chooses a product from Company-A product offerings

2. Company-V sends a request to Company-A (as the NSP) to order the product ‘Network Slice eMBB Platinum’. To achieve this, a candidate API is TMF API 622 (Product Ordering)

2.1 Company-A BSS determines which service supports the product being ordered by Company-V and issues a request to its OSS/SML to order this service. This service can be e.g. a network slice. To achieve this, a candidate API is TMF API 641 (Service Ordering)

2.2 Company-A OSS / SML determines which network resources support the service being ordered and:

2.2.1 based on its knowledge that required 5G core network resources are available internally, it issues a request to its own OSS / NML to allocate required 5G core network resources, e.g. network slice subnet(s) for its 5G core network, etc. To achieve this, candidate APIs are from TS 28.531 and TS 28.532

2.2.2 Company-A OSS / NML allocates 5G core network resources required to support the service and informs OSS / SML about the characteristics of the network resources being allocated

2.2.3 based on its knowledge that required RAN resources are not available internally, it informs Company-A BSS about missing RAN resources

2.3 Company-A BSS:

2.3.1 acting as a CSC, issues a request to Company-X to order product X-1 (e.g. from the Wholesale offerings) to get RAN coverage in the US. To achieve this, a candidate API is TMF AP 622 (Product ordering). Company-X, as the CSP, receives the product order. Company-X BSS determines which service supports the product being ordered by Company-A and issues a request to its OSS/SML to order this service. This service can be e.g. a network slice. To achieve this, a candidate API is TMF API 641 (Service Ordering). Company-X OSS / SML determines which network resources support the service being ordered, etc. Once completed, Company-X BSS informs Company-A BSS that the product which has been ordered is now available to Company-A

2.3.2 acting as a CSC, issues a request to Company-Y to order product Y-1 (e.g. from the inter-operator network slice offerings) to get RAN coverage in Spain. To achieve this, a candidate API is TMF AP 622 (Product ordering). Company-Y, as the CSP, receives the product order. Company-Y BSS determines which service supports the product being ordered by Company-A and issues a request to its OSS/SML to order this service. This service can be e.g. a network slice. To achieve this, a candidate API is TMF API 641 (Service Ordering). Company-Y OSS / SML determines which network resources support the service being ordered, etc. Once completed, Company-Y BSS informs Company-A BSS that the product which has been ordered is now available to Company-A

2.3.3 informs its own OSS/SML that required RAN resources are available

2.4 Company-A OSS / SML associates the network resources allocated either internally or externally (by Company-X or Company-Y) to the service and informs its BSS about the characteristics of the service supporting the product

3. Company-A (as the NSP) sends a reply to Company-V to inform that the product ordered is now available to Vertical-V.

NOTE: in this use case, aspects related to Transport Network(s) are not addressed as they are out of 3GPP scope.

### 5.4.2 Potential issues and gaps

#### 5.4.2.1 Issues

In both sub-use case 1 and sub-use case 2, the characteristics of the network slice ordered by the NSC to the NSP are exposed by the NSP to the NSC at product-level, i.e. as specified by the product specification in the NSP catalogue. The product specification provides the characteristics of the product being offered by the NSP at business level and is not subject to standardization. These characteristics are generally more abstract than attributes defined in the 3GPP 5G NRM (cf. TS 28.541) and performance measurements defined in TS 28.552.

#### 5.4.2.2 Gaps

In these two sub-use cases, there is no exposure of service or network resources directly to the NSC. From a BSS perspective no gaps in SA5 specifications have been identified

## 5.5 Exposure of network slice as a service

### 5.5.1 Description

This use case involves the following roles:

- NSP: Network Slice Provider

- NSC: Network Slice Customer

- NOP: Network Operator

- CSC: Communication Service Customer

- CSP: Communication Service Provider

, and the following systems:

- BSS: Business Support System

- OSS: Operations Support System, made up of the two following sub-systems:

- SML: Service Management Layer

- NML: Network Management Layer (for sake of simplicity, network management and network element / function management are both in the NML).

#### 5.5.1.1 Sub-use case 1: NSP and NOP play by the same organization

In this scenario, the following organizations play aforementioned roles as follows:

- Company-V, which has a contract with Company-A for the exposure directly via OSS, plays the role of NSC

- Company-A plays the role of NSP and NOP

- As NSP, it has:

- a BSS, e.g. to manage its customers, products, contracts, and

- a SML, to manage the services that support its products,

- As NOP, it has:

- its own 5G network (RAN + core). In this sub-use case, Company-A owns the whole set of network resources used by the service that can potentially support the service required by Company-V

- a NML, to manage the network resources used by services

NOTE 1: NSC may have connection with Company-A BSS for the product-level interaction. If not, the OSS/SML may have an embedded BSS functionalities for the product-level interaction.

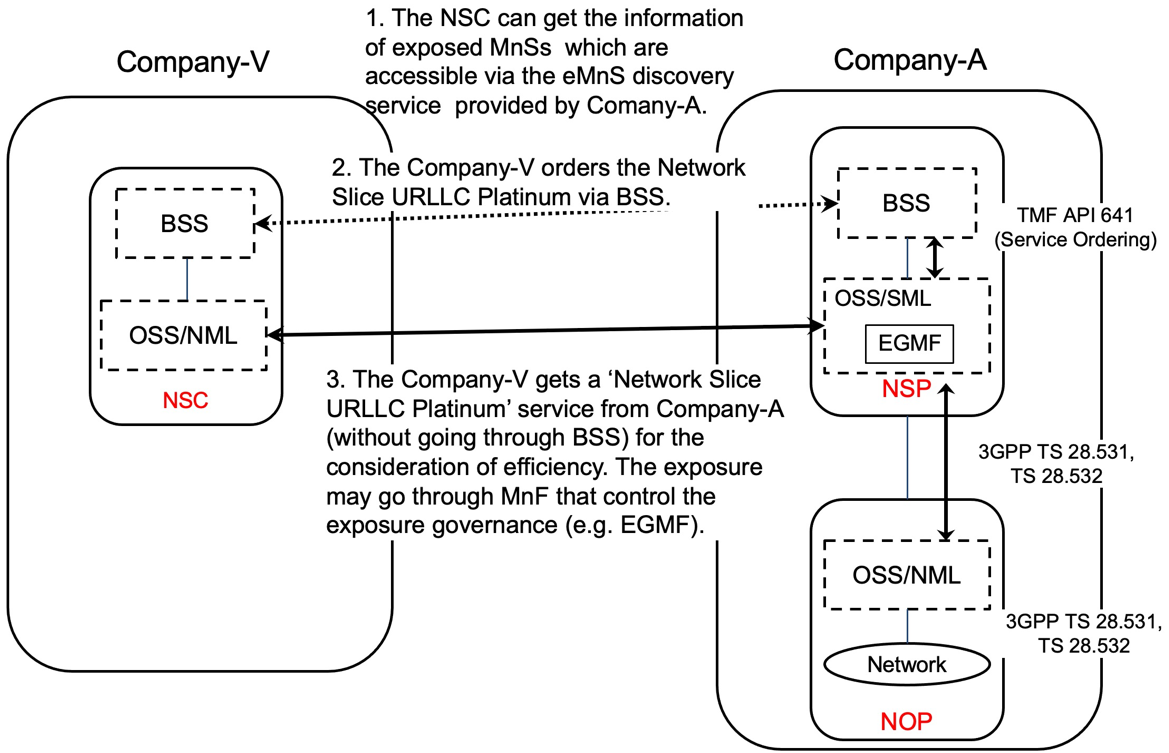


Figure 5.5.1.1-1 Sub-use case – NSP and NOP played by the same organization

Company-A proposes the following product offering together with the exposure capability:

- Network Slice eMBB with the exposure capability of related KPI monitoring and alarm notification, etc.

In this sub-use case 1:

1. Company-V (as the NSC) gets the information regarding exposed MnSs that are available via the exposed MnS discovery service from the Company-A.

2. Company-V sends a request to Company-A (as the NSP) for the access to exposed MnS set ‘Network Slice eMBB’, which contains the exposure capabilities such as related KPI monitoring and alarm notification, etc. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF).

2.1 Company-A SML determines which service supports the exposed MnS being requested by Company-V.

2.2 Company-A OSS / SML sends a response, including the authentication materials (e.g. key, token) for access to the chosen exposed MnS.

3. The company-V can direct consume the exposed MnS (e.g. KPI monitoring and alarm notification) from SML of the Company-A’s 3GPP management system.

#### 5.5.1.2 Sub-use case 2: NOP role played simultaneously by different organizations

In this scenario, the following organizations play aforementioned roles as follows:

- Company-V, which has a contract with Company-A for the exposure directly via OSS, plays the role of NSC

- Company-A plays the role of NSP and NOP

- As NSP, it has:

- a BSS, e.g. to manage its customers, products, contracts, and

- a SML, to manage the services that support its products,

- As NOP, it has:

- its own 5G core network. In this sub-use case, Company-A owns the whole set of 5G core network resources used by the service that can potentially support the service required by Company-V

- a NML, to manage the 5G core network resources used by services

As Company-A has no RAN in all requested areas, it relies on a different organization with a specific contract (e.g. exposure directly via OSS), namely Company-B Spain and Company-C USA, to provide RAN coverage in the Spain and in the USA respectively. Therefore:

- Company-A plays the role of Communication Service Customer (CSC) wrt. Company-B Spain and Company-C USA who both play the role of Communication Service Provider (CSP)

- Both Company-B Spain and Company-C USA have their own services to offer RAN coverage in their respective countries

- Both Company-B Spain and Company-C USA play the role of CSP (for their respective product offerings) and NOP (for their respective RAN).

NOTE 1: NSC may have connection with Company-A BSS for the product-level interaction. If not, the OSS/SML may have an embedded BSS functionalities for the product-level interaction.

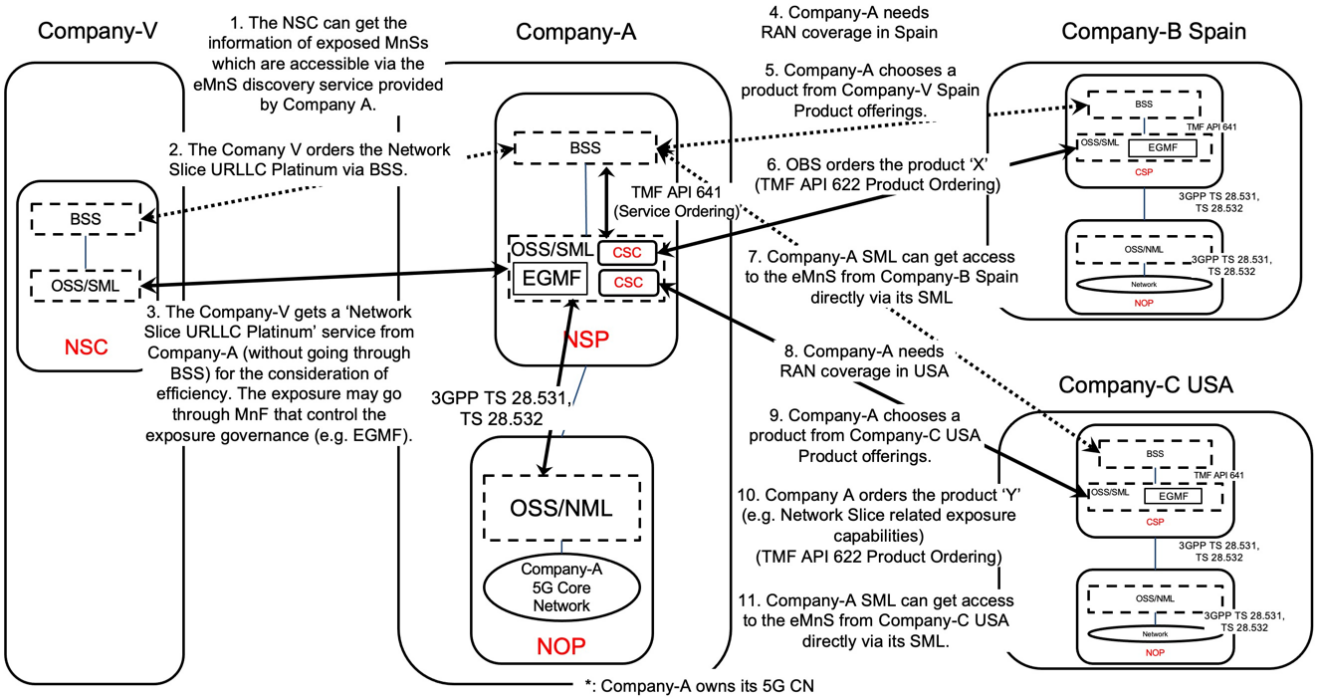


Figure 5.5.1.2-1 Sub-use case – NOP role played simultaneously by different organizations

Company-A proposes the following product offering together with the exposure capability:

- Network Slice eMBB with the exposure capability of related KPI monitoring and alarm notification, etc.

In this sub-use case 2:

1. Company-V (as the NSC) gets the information regarding exposed MnSs that are available via the exposed MnS discovery service from the Company-A.

2. Company-V sends a request to Company-A (as the NSP) for the access to exposed MnS set ‘Network Slice eMBB Platinum’, which contains the exposure capabilities such as related KPI monitoring and alarm notification, etc. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF).

2.1 Company-A SML determines which service supports the exposed MnS being requested by Company-V.

2.2 Company-A OSS / SML determines which network resources support the service being requested and:

2.2.1 based on its knowledge that required RAN resources are not available internally, the SML, acting as a CSC, issues a request to Company-C USA to request service to get RAN coverage in the US. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF) of Company-C USA. Company-C USA, as the CSP, receives the service request. Company-C USA SML determines which service supports the exposed MnS being requested by Company-A. This service can be e.g. a network slice. Company-C USA OSS / SML determines which network resources support the service being requested, etc. Once completed, Company-C USA SML informs Company-A SML that the exposed MnS which has been requested is now available to Company-A. The Company-A SML can consume the exposed MnS from Company-C USA directly via its SML.

2.2.3 acting as a CSC, issues a request to Company-B Spain to request service to get RAN coverage in Spain. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF) of Company-B Spain. Company-B Spain, as the CSP, receives the service request. Company-B Spain SML determines which service supports the exposed MnS being requested by Company-A. This service can be e.g. a network slice. Company-B Spain OSS / SML determines which network resources support the service being requested, etc. Once completed, Company-B Spain SML informs Company-A SML that the exposed MnS which has been requested is now available to Company-A. The Company-A SML can consume the exposed MnS from Company-B Spain directly via its SML.

3. Company-A (as the NSP) sends a reply to Company-V to inform that the exposed MnS requested is now available to Company-V. The reply may also include the authentication materials (e.g. key, token) for access to the chosen exposed MnS.

NOTE 3: NSP may not have network at all. In this case, if and how NSP can offer exposure services to NSC is FFS.

NOTE 4: in this use case, aspects related to Transport Network(s) are not addressed as they are out of 3GPP scope.

### 5.5.2 Potential issues and gaps

#### 5.5.2.1 Issues

Editor’s Note: the issues if any are FFS.

#### 5.5.2.2 Gaps

Editor’s Note: the gaps if any are FFS.

## 5.6 Exposure to application servers and application functions

### 5.6.1 Description

The operator has other non-management entities such as the middleware (example SEAL server) or application servers (AS) defined by 3GPP SA6 that could consume management services as shown in Figure 4.1.1.3.2-1. These could be internal or external to the operator. In such cases the BSS may or may not be directly involved. An example of an external application could be a V2X application server may use the management system to provision V2X slices in a certain geography (AS2 or AS3 in Figure). An example for an internal application could be the operators eMBB application server discovering a newly supported coverage area and provisioning the operator eMBB network slice instance in that area (AS1 in Figure). AS1 and AS2 access the 3GPP management system from an operator internal enabler server (see TR23.700-99), another enabler server could be located in the vertical premises and therefore external to the operator. In TR23.700-99 both such options are considered. In this scenario the operator MnSs are directly access by internal or external entities (subject to prior agreements) without going through the BSS. In addition to application servers and application enabler server, any internal of external authorized application function may also access exposed MnS.

In Figure 4.1.1.3.2-1 AS1 and AS2 may or may not be aware that they use exposed MnSs from the operator. The respective enabler servers could hide this internal implementation. Bother enabler servers may access exposed MnS subject to respective authorization. However, it is likely that the application enabler server A and AF1 have direct access to management services without a BSS, whereas the application enabler server B and AF2 would need some sort of involvement of the BSS.



Figure 5.6.1-1 Exposure to application server within and outside operator network

### 5.6.2 Issue and gaps

Issues:

To be able to consumer MnS the external entities need to be aware of the existence of the operator and the respective MnS it wants to consumer. This issue depends on the dynamism supported by the system. In a highly dynamic and changing system the issue is equivalent to Section 5.4 exposed MnS support to discovery systems

Furthermore, the external entities need to gain credentials to access the exposed MnS.

# 6 Potential requirements for network management capability exposure

## 6.1 Potential requirements related to exposed MnS discovery service

* **REQ-NSCE-01** The 3GPP management system may provide capabilities allowing to discover exposed MnS and related exposed MnS producers that are managing a specific managed entity.
* **REQ-NSCE-02** The 3GPP management system may have functionalities to register exposed MnS to an appropriate discovery service/system (e.g. exposed MnS discovery service producer).
* **REQ-NSCE-03** The 3GPP management system may provide capabilities to authenticate and authorize network slice consumers to discover exposed MnS and related MnS producers.

## 6.2 Potential requirements related to exposure interface via OSS

* **REQ-NSCE-04** The 3GPP management system may provide capabilities to authenticate and authorize network slice consumers to consume exposed MnS directly from 3GPP management system.

# 7 Possible solutions for network management capability exposure

## 7.1 Possible solution for “exposed MnS support to discovery systems” – Scenario 5.4

The steps of the solution are as follows:

1. A MnS consumer configures using the appropriate MnS (for example the generic provisioning service) the details of the external discovery service location and other supporting details (for e.g., authentication and authorization). Further, the detail on which parts of which MnS (component A) IOCs and which instances of the corresponding MOI (component B) and corresponding data (component C) can be registered with the discovery service/system. As an example, the operator may want to register her the ability to provision (Management object A) a particular slice type (NSSAI-ID) at a certain coverage area (coverageArea item 6.3.3 TS28.541) with some additional details (example: supported latency or maxNumberofUEs or delayTolerance) to an external discovery service or system.
2. In addition to the information of what is externally registered, information relating to the address of the exposed MnS needs to be provided. This could be default information based on the operator in the external discovery system or in case of a trusted discovery the address of the actual exposed management service.
3. The 3GPP Management System registers the exposed management component A, B and C as configured in step 1 to the appropriate external discovery service/system.
4. Eventually, if any of the exposure details change – for example the same slice type can now be supported in a new coverageArea – the registration to the external discovery system may now need to be updated.

Editor’s note: provide a picture explain the operator and JV relationship below.

The solution for the trust issue between the three MnS discovery system owner, MnS consumer and the MnS producer is scenario dependent. Let’s take for example a multi-operator network scenario. In this scenario let’s take operator A as an MnS producer, a joint venture of multiple operators as a MnS discovery system owner and operator B as an MnS consumer. Both Operator A and Operator B have business relations with the joint venture thereby creating a trust relationship between Operator A and the joint venture (JV) AND operator B and the joint venture. The JV provides the authorization and authentication details for each of the operator to use the discovery service. Operator A may then expose aspects of its MnS that it considers ok to expose with the JV. Operator B can then discover the MnS offered by operator A and contact operator A to access them. If operator B requires a higher level of access than operator A provides in the JV by default, then they need to form a new business relationship.

## 7.2 Possible solutions for exposed MnS discovery service

To enable communication between exposed MnS consumers and exposed MnS producers, exposed MnS consumers need a mechanism to discover exposed MnS producers that are available in the 3GPP management system, this is called exposed MnS discovery service.

When the operator decides to expose a management service (exposed MnS), the operator must decide which MnS(s) should be exposed, which internal MnS operations should be abstracted/filtered, and which internal MnS data should be abstracted/filtered. As part of this decision, the operator may use the MnS Discovery Service to collect information. The operator exposes the MnS and registers it with the exposed MnS discovery service, this may be done using an EGMF.

The exposed MnS discovery service consumer sends a request to appropriate discovery service (e.g. exposed MnS discovery service producer) to obtain the exposed MnS data.

## 7.3 Potential solution for MnS discovery service for exposure

The MnS data can be accessed by different kinds of discovery service consumers based on different use cases.

In some use cases, the exposure usually goes through BSS. The BSS can obtain MnS data from the MnS discovery service on behalf of the NSC.

There are different scenarios where the NSC could directly interact with the MnS producer exposure interface via OSS.

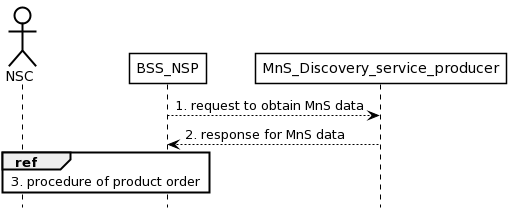


Figure 7.3.1 Procedure for MnS discovery service for exposure via BSS

1. The BSS requests for MnS data from the MnS discovery service for NSC on behalf of the NSC. The MnS data may contain the address of the exposed producer.
2. MnS discovery service producer for NSC provides discovery service to NSC. The MnS discovery service producer returns the MnS data to BSS. The BSS may provide discovery service to NSC based on MnS data.
3. The NSC completes the product order via the interaction with BSS\_NSP.

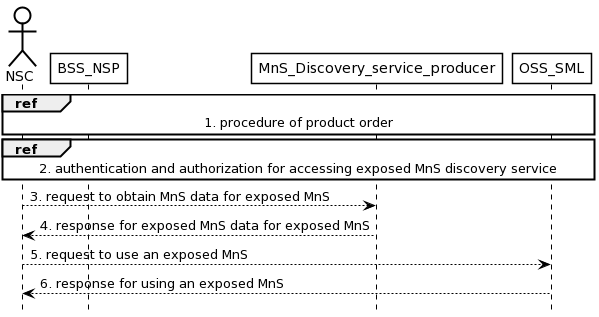


Figure 7.3.2 Procedure for MnS discovery service for exposure via OSS

1. The NSC completes a product order via the interaction with BSS\_NSP. As a result of the product ordering, the NSC obtains the address of the MnS discovery service producer for exposure.

NOTE: MnS discovery service producer providing discovery service for the exposed MnS to external.

1. The NSC executes authentication and authorization for accessing MnS discovery service.
2. The NSC requests for MnS data for exposed MnS from the MnS discovery service. The exposed MnS data for exposed MnS may contain the information of the exposed MnS instance and the address of the exposed MnS producer. The MnS data for exposed MnS is the data for authorized NSC to identify proper MnS producer which produces the exposed MnS.
3. The MnS discovery service returns the MnS data for exposed MnS to the NSC.
4. The NSC requests the services from the target exposed MnS producer.
5. The target exposed MnS producer returns the responses.

## 7.4 Potential solution for exposed MnS consumption via OSS interface

This clause introduces the solution for the use case described in clause 5.6, where the NSC can directly interact with OSS for the consumption of exposed MnS.

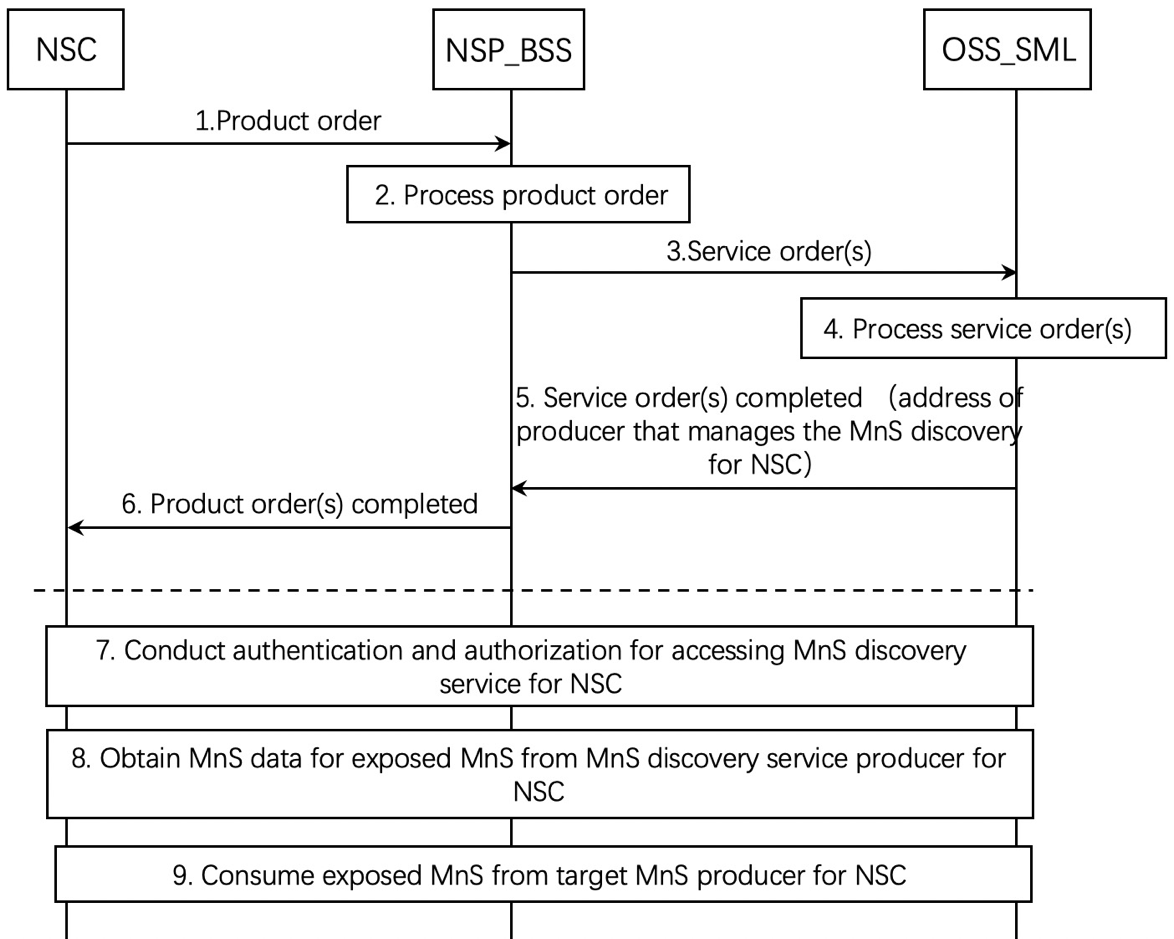


Figure 7.4.1 Exposed MnS consumption via OSS interface

1. The NSP receives a product order from the NSC through BSS. The interface used towards the BSS is specified by TM Forum specifications [2].

2. The BSS processes the product order and when applicable converts it to appropriate service order(s) for the OSS Service Management Layer. This is internal to BSS and there are no interface requirements.

3. The OSS Service Management Layer receives a service order from the BSS. The interface used is specified by TM Forum specifications [3].

4. The MnS producer for NSC (e.g. NSMF) on the OSS Service Management Layer processes the service order and when applicable converts it to appropriate request(s) for the OSS Network Management Layer as requests for management and orchestration of resources. In addition, MnS producer on the OSS Service Management Layer can decides to expose MnS directly from OSS\_SML and prepares the address of MnS discovery service producer for NSC that can be accessed by the NSC and related authorization information (e.g. token) for accessing the MnS discovery service for NSC. The service order may trigger a procedure of resource order with OSS\_NML.

5. The MnS producer for NSC on OSS Service Management Layer notifies the BSS that the service order has been completed. In addition, the notification may contain the address of producer that manages the MnS discovery service for NSC to access and also identities of the related MOIs which is related to the exposed MnSs that the NSC requests. The interface used is specified by TM Forum specifications [3].

NOTE 1: The MnS discovery service producer for NSC can be within the OSS or outside the OSS.

6. The BSS notifies the NSC that the product order has been completed. In addition, the address of MnS discovery producer for NSC and the related authorization information (e.g. token) for accessing the MnS discovery service for NSC are sent to the NSC by the product order completed message. The interface used the interface towards the BSS is specified by TM Forum specifications [2].

7. If the notification in step 6 contains the address of MnS discovery service producer for NSC, the NSC conducts authentication and authorization for accessing exposed MnS discovery service.

8. After the authentication and authorization, the NSC obtains the MnS data for exposed MnS, which contains the information of the exposed MnS instance and the address of target MnS producer for NSC. The MnS data for exposed MnS is the data for authorized NSC to identify proper MnS producer which produces the exposed MnS.

9. After obtaining the information of the MnS data for exposed MnS, the NSC identifies the target MnS producer for NSC and consumes the exposed MnS. To consider the security, the MnS producer may leverage a dedicated MnF which controls the exposure governance as a proxy for exposing MnS.

The NSC has to consume several MnSs e.g., for authentication, authorization, and MnS discovery. When the NSC consumes an MnS, the MnS may rely on other MnSs to be able to produce the service.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Description in step** | **Interface** | **Reference** | **Description in reference** |
| 1 | product order | External | TM Forum TMF622 [2] | Product Order |
| 2 |  | None | - | - |
| 3 | service order | Internal | TM Forum TMF641 [3] | Service Order |
| 4 |  | None | - | - |
| 5 | service order completed | Internal | TM Forum TMF641 [3] | Service Order State Change Event with the address of MnS producer |
| 6 | product order completed | External | TM Forum TMF622 [2] | Product Order State Change Event with the address of MnS producer |
| 7 | Authentication and Authorization | External | - | Authentication and authorization of the NSC’s MnS consumers. Dedicated operation for Authentication and Authorization is missing in current specification. |
| 8 | MnS discovery | External | TS 28.532 [15], TS 28.622 [17] | MnS discovery of MnS producers may require enhancement of TS 28.532 and TS 28.622 for registry. |
| 9 | MnS consumption | External | TS 28.532 [15], TS 28.531 [5] | Consumption of MnS may need enhancement to TS 28.532 and TS 28.531, for authorization. |

**Table 7.4.1 Exposed MnS consumption via OSS interface**

## 7.5 Solution for internal service order after receiving product order

This clause describes a solution for the procedure described in clause 4.1.4.2. For each step in the procedure Table 7.5.1 identifies the following:

- if an interface is Internal to an operator, i.e. internal to a CSP or internal to an NSP, or External between a CSP and an NSP, or None in case the step is an internal process and there is no interface requirement,

- which operation or notification is used by that step, and

- which specification describes the interface (stage 2 and stage 3).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Description in step** | **Interface** | **Reference** | **Description in reference** |
| 1 | product order | External | TM Forum TMF622 [2] | Product Order |
| 2 |  | None | - | - |
| 3 | service order | External | TM Forum TMF641 [3] | Service Order |
| 4 |  | None | - | - |
| 5 | resource order | Internal | TM Forum TMF652 [4] | Resource Order |
| 6 |  | Internal | TS 28.531 [5], clause 6.5.1- | AllocateNsi |
| 7 | resource order completed | Internal | TM Forum TMF652 [4] | Service Order State Change Event |
| 8 | service order completed | External | TM Forum TMF641 [3] | Product Order State Change Event |
| 9 | product order completed | External | TM Forum TMF622 [2] | Product Order State Change Event |

Table 7.5.1 Solution for internal service order after receiving product order

## 7.6 Solution for external product order after receiving product order

This clause describes a solution for the procedure described in clause 4.1.4.3. For each step in the procedure Table 7.6.1 identifies the following:

- if an interface is Internal to an operator, i.e. internal to a CSP or internal to an NSP, or External between a CSP and an NSP, or None in case the step is an internal process and there is no interface requirement,

- which operation or notification is used by that step, and

- which specification describes the interface (stage 2 and stage 3).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Description in step** | **Interface** | **Reference** | **Description in reference** |
| 1 | product order | External | TM Forum TMF622 [2] | Product Order |
| 2 |  | None | - | - |
| 3 | product order | External | TM Forum TMF622 [2] | Product Order |
| 4 |  | None | - | - |
| 5 | service order | Internal | TM Forum TMF641 [3] | Service Order |
| 6 |  | None | - | - |
| 7 | service order completed | Internal | TM Forum TMF641 [3] | Service Order State Change Event |
| 8 | product order completed | External | TM Forum TMF622 [2] | Product Order State Change Event |
| 9 | product order completed | External | TM Forum TMF622 [2] | Product Order State Change Event |

Table 7.6.1 Solution for external product order after receiving product order

## 7.7 Solution for external service order after receiving product order

This clause describes a solution for the procedure described in clause 4.1.4.4. For each step in the procedure Table 7.7.1 identifies the following:

- if an interface is Internal to an operator, i.e. internal to a CSP or internal to an NSP, or External between a CSP and an NSP, or None in case the step is an internal process and there is no interface requirement,

- which operation or notification is used by that step, and

- which specification describes the interface (stage 2 and stage 3).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Description in step** | **Interface** | **Reference** | **Description in reference** |
| 1 | product order | External | TM Forum TMF622 [2] | Product Order |
| 2 |  | None | - | - |
| 3 | service order | Internal | TM Forum TMF641 [3] | Service Order |
| 4 |  | None | - | - |
| 5 | service order | External | TM Forum TMF641 [3] | Service Order |
| 6 |  | None | - | - |
| 7 | notify service order completed | Internal | TS 28.202 [6] | Service Order Completed Notification |
| 8 | service order completed | External | TM Forum TMF641 [3] | Service Order State Change Event |
| 9 | service order completed | External | TM Forum TMF641 [3] | Service Order State Change Event |

Table 7.7.1 Solution for external product order after receiving product order

## 7.8 Potential solution for product onboarding

This clause describes a solution for the procedure described in clause 4.1.4.5. For each step in the procedure Table 7.8.1 identifies the following:

- if an interface is Internal to an operator, i.e. internal to the NSP or External between a NSC and NSP, or None in case the step is an internal process and there is no interface requirement,

- which operation or notification is used by that step, and

- which specification describes the interface (stage 2 and stage 3).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Description in step** | **Interface** | **Reference** | **Description in reference** |
| 1 | service discovery | Internal | TS 28.537[10], clause 5- | Editor’s Note: further details are FFS |
| 2 |  | None | - | - |
| 3 | request list of available services | Internal | TM Forum TMF633[12] | Service Catalogue |
| 4 | provide list of available services | Internal | TM Forum TMF633[12] | Service Catalogue |
| 5 |  | None | - | - |
| 6 | product catalogue request | External | TM Forum TMF620[13] | Product Catalogue |
| 7 | product catalogue | External | TM Forum TMF620[13] | Product Catalogue |

Table 7.8.1 Solution for product onboarding

## 7.9 Potential solutions for network slice management capability exposure via CAPIF

### 7.9.1 Exposure via CAPIF alternative 1

This clause describes a potential solution where network slice management capability is exposed via the Common API Framework for 3GPP Northbound APIs, see TS 23.222 [14].

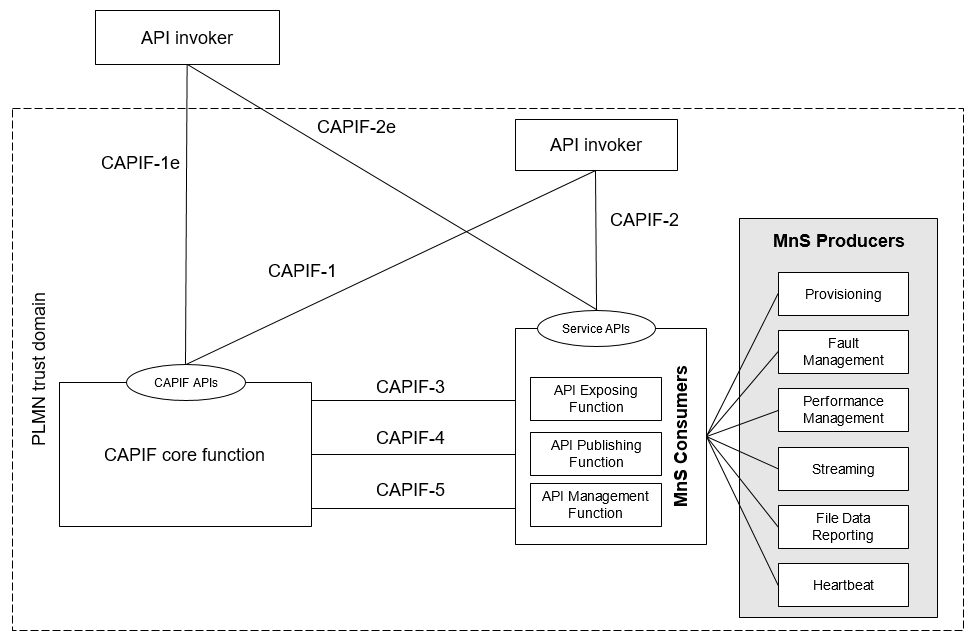
4

Figure 7.9.1-1: Exposure via CAPIF alternative 1

In this alternative, network slice management capability exposure provides faultMnS, fileDataReportingMnS, heartbeatNtf, perfMnS, provMnS, and streamingDataMnS as specified in in TS 28.532 [15].

Editor’s note: Whether network slice management capability exposure is affected by transforming the management service API to another service API is FFS.

### 7.9.2 Exposure via CAPIF alternative 2

This clause describes a potential solution where network slice management capability exposure is used in conjunction with a CAPIF core function (see TS 23.222 [14]) to expose management services to MnS consumers.

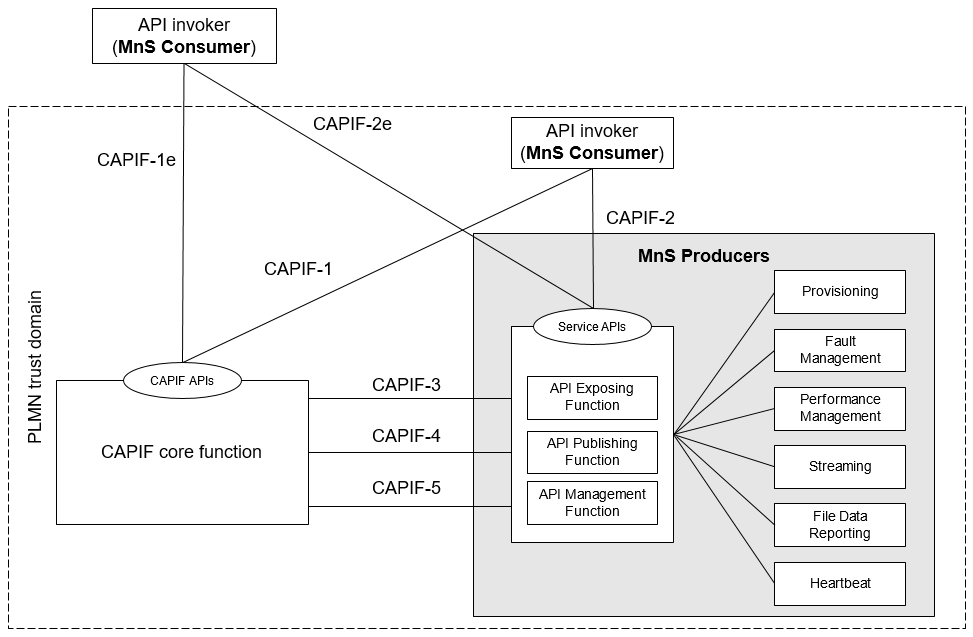


Figure 7.9.2-1: Exposure via CAPIF alternative 2

In this alternative, network slice management capability exposure consumes the interfaces at reference points CAPIF-3, CAPIF-4, and CAPIF-5 as defined in TS 23.222 [14]. It may be necessary to extend CAPIF-3/4/5 as defined in TS 23.222 [14] to support exposure of network slice management services.

In this alternative, network slice management capability exposure provides the interfaces at reference point CAPIF-2/2e. It may be necessary to extend CAPIF-2/2e as defined in TS 23.222 [14] to support network slice management capability exposure and authentication of MnS consumers.

In this alternative, MnS consumers utilize the interfaces at reference point CAPIF-1/1e. It may be necessary to extend CAPIF-1/1e as defined in TS 23.222 [14] to support authorization/authentication of MnS consumers and discovery of MnS producers.

Editor’s note: Whether network slice management capability exposure is affected by transforming the management service API to another service API is FFS.

Table 7.9.2-1 shows the CAPIF interface and the potential MnS that can be implemented within the interface for alternative 2. In addition, extension of CAPIF interface may be needed to achieve certain functionalities in the context of network slice management capability exposure.

**Table 7.9.2-1 Interface description**

|  |  |  |
| --- | --- | --- |
| **Interface** | **Related MnS** | **Gap analysis** |
| CAPIF 1/1e | - Discovery of MnS(s) from MnS registry using ProvMnS Specified in TS 28.622 [17], TS 28.623 [16], and TS 28.532 [15] | - How the MnS consumer can discover the MnS producer using CAPIF 1/1e is not specified.  - The ServiceAPIDescription for CAPIF\_Discover\_Service\_API needs to be extended in the context of network slice management capability exposure. The MnS address within the MnS data can indicate a MnS producer for exposing MnS after authentication and authorization.  - Management of MnS consumers includes the management of MnS consumer type and identity. The management of MnS consumer type and identity is for differentiating different access permission for different MnS consumer. |
| CAPIF 2/2e | - Authentication and authorization of MnS consumers is specified in TS 28.533 [11] clause 4.9.  - Service APIs (MnS): faultMnS, fileDataReportingMnS, heartbeatNtf, perfMnS, provMnS, and streamingDataMnS Specified in in TS 28.532 [15] | - How to use MnS as extension for CAPIF 2/2e is not specified.  - The Service API for CAPIF 2/2e need to be extended to support MnS. |
| CAPIF 3 | - Nchf\_ConvergedCharging Specified in TS 28.201 [18] and TS 28.202 [6]  - Access control capability specified in TS 28.533 [11] |  |
| CAPIF 4 | - MnS Registry Specified in TS 28.622 [17] and TS 28.623 [16]. | - How to publish the MnS data for MnS discovery by the MnS consumer using CAPIF 4 is not specified.  - The ServiceAPIDescription for CAPIF\_Publish\_Service\_API needs to be extended in the context of network slice management capability exposure. The MnS address within the MnS data can indicate a MnS producer for exposing MnS after authentication and authorization. |
| CAPIF 5 | - Auditing of the MnS producer is not specified | - How to allow MnS producer to recognize and differentiate each MnS consumer during the auditing is not specified.  - MnS consumer ID is needed for auditing service API invocation. |

After the MnS consumer completes authentication and authorization, the CAPIF core function needs to help the MnS consumer to discover the address of the MnS producer so that the MnS consumer can request MnS consumption. In order to provide the discovery service to the MnS consumer, the MnS data that contains the address of the MnS producer needs to be published to the CAPIF core function. This may require an extension of CAPIF-4 interface to make sure that the ServiceAPIDescription for CAPIF\_Publish\_Service\_API can carry the MnS data in order to support the discovery service for the MnS consumer.

The mnsAddress of MnsInfo within CAPIF-1/1e and 4 can be extended as below:

**Table 7.9.2-3 mnsaddress information within MnsInfo**

|  |  |  |  |
| --- | --- | --- | --- |
| Attributes | Support | Cardinality | Description |
| mnsAddress | M | 1 | The MnS address for external MnS consumer indicates a MnS producer for exposing MnS after authentication and authorization. |

For CAPIF-5 interface, According to TS 23.222, API management function can access the service API invocation logs via CAPIF-5. The procedure for auditing needs the query service API log request from API management function to the CAPIF core function. Since API management function is within the 3GPP management system, in order to differentiate each MnS consumer, MnS consumer ID is needed in order to allow MnS producer to recognize each MnS consumer during the auditing. Therefore, API Invoker’s ID need to be extended as MnS customer ID.

The MnS consumer management information is needed for differentiating the MnS consumer in term of consumer type and different access permission. The MnS consumer type is for differentiate the MnS consumer inside and outside the PLMN trust domain.

CAPIF core function can authorize MnS consumer with certain permission (e.g. access token) using CAPIF-1/1e interface. The permission can allow the MnS consumer to get access to the authorized information of MnS from respective MnS producer. In order to allow the corresponding MnS producer to recognize the MnS consumer and the corresponding authorized MnS, MnS consumer ID is needed. Therefore, API Invoker’s ID need to be extended as MnS customer ID.

Editor’s note: The format of MnS consumer ID is FFS.

The MnS consumer management information within CAPIF-1/1e can be extended as below:

**Table 7.9.2-4 MnS consumer management information**

|  |  |  |  |
| --- | --- | --- | --- |
| Attributes | Support | Cardinality | Description |
| MnSConsumerType | O | 1…N | It indicates the type of MnS consumer that requests for the exposure of the MnSs provided by MnS producer. The type of MnS consumer is external if the MnS consumer is outside the PLMN trust domain. The type of MnS consumer is internal if the MnS consumer is inside the PLMN trust domain.  allowedValue: EXTERNAL,  INTERNAL |
| MnSConsumerID | O | 1…N | It indicates the Identifier of the MnS consumer that requests MnSs from the MnS producer.  The identifier of the MnS consumer can be associated to its access token. The access token can represent a set of MnSs that are allowed to be exposed to MnS consumer.  The format of the MnS consumer ID can use FQDN (See TS 21.003 clause 19.4.2.1). |

The MnS consumer can directly get access to MnS producer after the authentication and validation with MnS producer if the expsoure governance is implemented in respective MnS producer. The MnS producer may be able to provide original MnS following exposure governance which includes filtering. As a result, MnS consumer may be able to access only a subset of original MnS via the response from the MnS producer.

### 7.9.3 Exposure via CAPIF alternative 3

This clause describes a potential solution where network slice management capability exposure implements a Common API Framework for 3GPP Northbound APIs (see TS 23.222 [14]) to expose management services to MnS consumers.

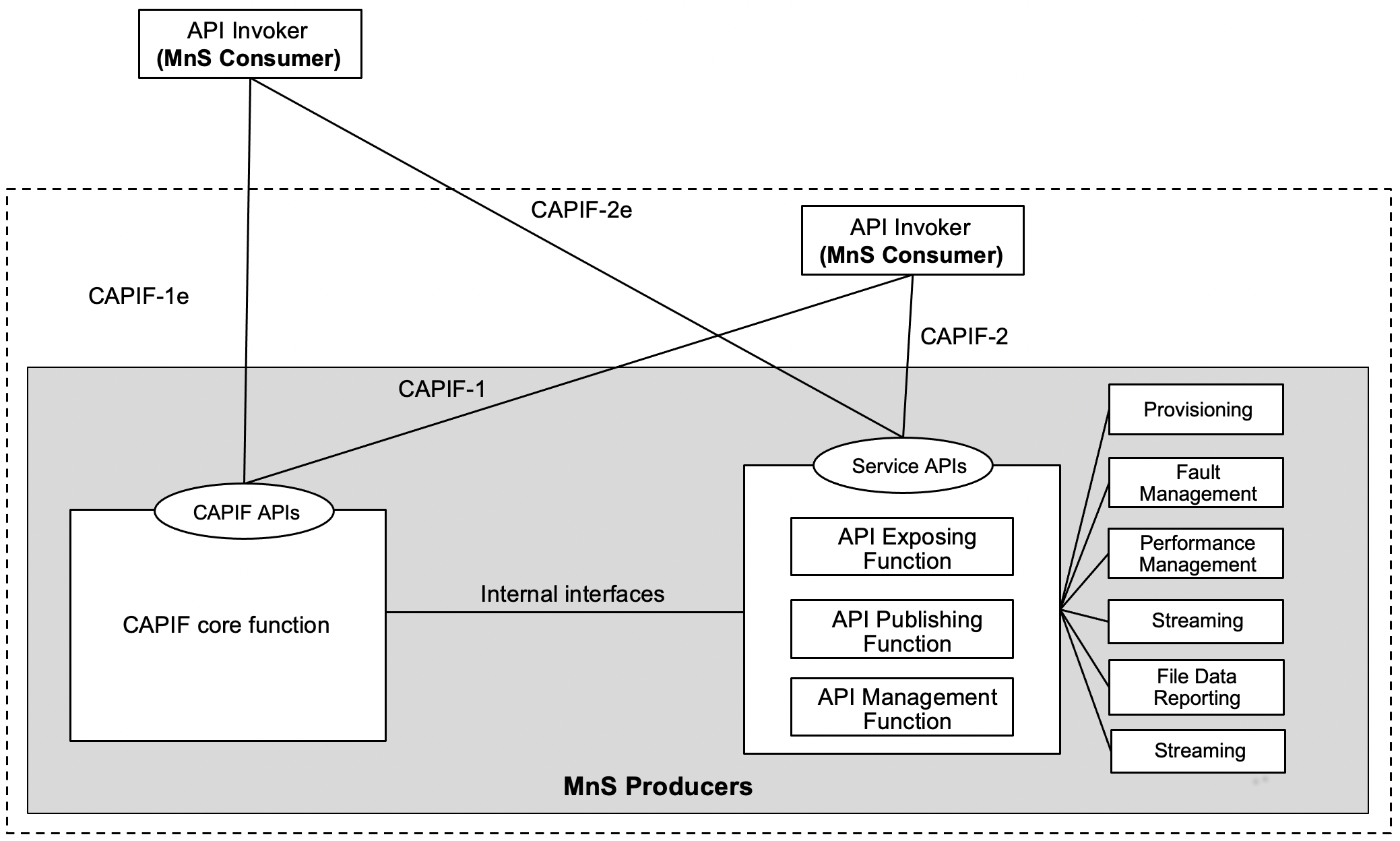


Figure 7.9.3-1: Exposure via CAPIF alternative 3

In this alternative, network slice management capability exposure may internally implement the internal interfaces using reference points CAPIF-3, CAPIF-4, and CAPIF-5 as defined in TS 23.222 [14] or may use non-standardized interfaces.

In this alternative, network slice management capability exposure provides the interfaces at reference point CAPIF-1/1e. It may be necessary to extend CAPIF-1/1e as defined in TS 23.222 [14] to support authorization/authentication of MnS consumers and discovery of MnS producers.

In this alternative, network slice management capability exposure provides the interfaces at reference point CAPIF-2/2e. It may be necessary to extend CAPIF-2/2e as defined in TS 23.222 [14] to support network slice management capability exposure and authentication of MnS consumers.

Editor’s note: Whether network slice management capability exposure is affected by transforming the management service API to another service API is FFS.

Table 7.9.3-1 shows the CAPIF interface and the potential MnS that can be implemented within the interface for alternative 3. In addition, extension of CAPIF interface may be needed to achieve certain functionalities in the context of network slice management capability exposure.

**Table 7.9.3-1 Interface description**

|  |  |  |
| --- | --- | --- |
| **Interface** | **Related MnS** | **Gap analysis** |
| CAPIF 1/1e | - Discovery of MnS(s) from MnS registry using ProvMnS Specified in TS 28.622 [17], TS 28.623 [16], and TS 28.532 [15] | - How the MnS consumer can discover the MnS producer using CAPIF 1/1e is not specified.  - The ServiceAPIDescription for CAPIF\_Discover\_Service\_API needs to be extended in the context of network slice management capability exposure. The MnS address within the MnS data can indicate a MnS producer for exposing MnS after authentication and authorization.  - Management of MnS consumers includes the management of MnS consumer type and identity. The management of MnS consumer type and identity is for differentiating different access permission for different MnS consumer. |
| CAPIF 2/2e | - Authentication and authorization of MnS consumers is specified in TS 28.533 [11] clause 4.9  - Service APIs (MnS): faultMnS, fileDataReportingMnS, heartbeatNtf, perfMnS, provMnS, and streamingDataMnS Specified in in TS 28.532 [15] | - How to use MnS as extension for CAPIF 2/2e is not specified.  - The Service API for CAPIF 2/2e need to be extended to support MnS. |

After the MnS consumer completes authentication and authorization, the CAPIF core function needs to help the MnS consumer to discover the address of the MnS producer so that the MnS consumer can request MnS consumption via the MnS producer. In order to provide the discovery service to the MnS consumer, the MnS data that contains the address of the MnS producer needs to be published to the CAPIF core function.

The mnsAddress of MnsInfo within CAPIF-1/1e can be extended as below:

**Table 7.9.2-3 mnsaddress information within MnsInfo**

|  |  |  |  |
| --- | --- | --- | --- |
| Attributes | Support | Cardinality | Description |
| mnsAddress | M | 1 | The MnS address for external MnS consumer indicates MnS producer for exposing MnS after authentication and authorization. |

For CAPIF-5 interface, According to TS 23.222, API management function can access the service API invocation logs via CAPIF-5. The procedure for auditing needs the query service API log request from API management function to the CAPIF core function. Since API management function is within the 3GPP management system, in order to differentiate each MnS consumer, MnS consumer ID is needed in order to allow MnS producer to recognize each MnS consumer during the auditing. Therefore, API Invoker’s ID need to be extended as MnS customer ID.

The MnS consumer management information is needed for differentiating the MnS consumer in term of consumer type and different access permission. The MnS consumer type is for differentiate the MnS consumer inside and outside the PLMN trust domain.

CAPIF core function can authorize MnS consumer with certain permission (e.g. access token) using CAPIF-1/1e interface. The permission can allow the MnS consumer to get access to the authorized information of MnS from respective MnS producer. In order to allow the corresponding MnS producer to recognize the MnS consumer and the corresponding authorized MnS, MnS consumer ID is needed. Therefore, API Invoker’s ID need to be extended as MnS customer ID.

The MnS consumer management information within CAPIF-1/1e can be extended as below:

**Table 7.9.2-4 MnS consumer management information**

|  |  |  |  |
| --- | --- | --- | --- |
| Attributes | Support | Cardinality | Description |
| MnSConsumerType | O | 1…N | It indicates the type of MnS consumer that requests for the exposure of the MnSs provided by MnS producer. The type of MnS consumer is external if the MnS consumer is outside the PLMN trust domain. The type of MnS consumer is internal if the MnS consumer is inside the PLMN trust domain.  allowedValue: EXTERNAL,  INTERNAL |

The MnS consumer can directly get access to MnS producer after the authentication and validation with MnS producer if the expsoure governance is implemented in respective MnS producer. The MnS producer may be able to provide original MnS following exposure governance which includes filtering. As a result, MnS consumer may be able to access only a subset of original MnS via the response from the MnS producer.

### 7.9.4 Evaluation

An evaluation of these 3 alternatives is given, which can help to draw the conclusion and recommendation for this solution.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Summary | pros | Cons |
| Alternative 1 | API provider domain acts as MnS consumer which interacts with the MnS producer within SA5. SA5 jurisdiction ends at MnS Consumer. What MnS consumers does to expose the MnS further to API Invoker (external entity) is out–of-scope of SA5.How the external MnS consumer conduct authentication, authentication, discover the MnS and consume the MnS is not specified in this alternative. | No standardization work needed for SA5. | The requirements in clause 6 are not addressed in a standardized manner. |
| Alternative 2 | MnS producer embeds API provider domain functions capabilities and has direct interaction with CAPIF core function. External MnS consumer can conduct authentication and authorization with CCF. After that, the external MnS consumer can consume the MnS via the service API provided by API provider domain. | With certain extension for CAPIF interface, solution on how external MnS consumer discover and consume MnS can be specified. | Extension of CAPIF interfaces (e.g. CAPIF-1e, CAPIF-2e, CAPIF-3, CAPIF-4, CAPIF-5) is needed. |
| Alternative 3 | MnS producer embeds both CAPIF Core Function and API provider domain functions capabilities. CCF and API provider domain interact with each other via internal interfaces. | With certain extension for CAPIF interface, solution on how external MnS consumer discover and consume MnS can be specified. | Extension of CAPIF interface (e.g. CAPIF CAPIF-1e, CAPIF-2e) is needed. |

So far, there are several gaps regarding, MnS publishing, discovery, which are captured in TR 28.824:

- Whether and how to publish a MnS that can be discovered by external customer is not specified in existing 3GPP management system.

- If there is a need to publish MnS, then the exposure of MnS (e.g. performance MnS regarding NR and 5GC) is not specified in 3GPP management system.

- To limit issues the exposure from a discovery system of the operator may only provide “read” permissions (w.r.t the exposed MnS) without authentication and authorization. To execute the discovered exposed MnS the consumer still needs to be authenticated and authorized by the management system. Therefore, there is a gap in the difference in exposure for consumption, and exposure for discovery which needs to be solved.

All these gap can be resolved by alternative 2 and 3 since all the related interfaces are within the scope of alternative 2 and 3. Alternative 1 cannot solve the gaps mentioned above.

Based on the aforementioned evaluation, It is suggested to recommend alternative 2 and 3 as baseline for the normative work.

## 7.10 Possible solution for network slice management capability exposure

This solutions supports exposure via CAPIF alternative 2and exposure via CAPIF alternative 3 as defined in 7.9.2 and 7.9.3.

This solution proposes to use CAPIF framework [14] to expose network slice management capabilities to external entities. The solution requires extending the existing CAPIF mechanism to support MnS exposure and authorization. This includes extending the ServiceAPIDescription (see clause 8.2.4.2.2 of [19]) to support the description of the 3GPP management services required for exposure. This also includes defining mechanism to build exposure governance rules for allowing granular access to MnS from external entities.

In addition to external entities, the same solution can be used to provide access to entities inside PLMN trust domain (see clause 3.1 of [14]). Three types of consumer are considered here;

- NOP-External: the consumer is external to PLMN trust domain,

- OAM-External: the consumers is external to 3GPP management domain e.g (5GC NFs, trusted AF and application layer entities e.g SEAL)

- OAM-Internal: consumer is internal to 3GPP management domain.



1. MnS Producer (acting as API Provider Domain Function) registers with CCF using Register\_API\_Provider operation as defined in 5.11.2.2.2 of [19].
2. MnS consumer (acting as API Invoker) registers with CCF. The registration request will include related MnS Consumer details as part of APIInvokerEnrolmentDetails (8.4.4.2.2 of [19]).

Editor’s Note 1: Whether the APIInvokerEnrolmentDetails (clause 8.4.4.2.2 of [19]) need to be extended with provided consumer details in FFS.

1. MnS producer publishing the available management services with CCF. MnS Producer can optionally perform transformation of MnS into service API(s) before publishing. In absence of this transformation MnS are considered to be service APIs being exposed to MnS Consumer.

Note: Whether this optional transformation is needed or not, and its implementation details, is out-of-scope of SA5.

Editor’s Note: Initiatives such as CAMARA are working on this kind of transformation.

1. MnS consumer gets authenticated with CCF as per the procedures defined in clause 8.10 of [14].
2. MnS consumer discovers the available service APIs using the CAPIF discovery mechanisms. CCF authenticates the MnS Consumer and reports the available management service described by the ServiceAPIDescription.
3. MnS consumer gets authorization to access available service APIs as per the procedures defined in clause 8.11 of [14].
4. MnS consumer gets authenticated with AEF as per the procedures defined in clause 8.14 of [14].
5. MnS consumer tries to access the service API.
6. MnS Producer checks the validity of the token including checking the granular consumer’s authorizations. MnS Producer will then decide whether to allow the access or not.
7. MnS Producer may interact with CAPIF Core for authentication, authorization and charging.
8. MnS Producer provides appropriate response.

NOTE: When this solution applies to alternative 3, the CAPIF core function becomes part of MnS Producer.

This solution requires MnS to be described as a Service API. To accomplish this, the management service discovery data must be mapped to CAPIF data structures.

As defined in 28.622[17], a Management Service is described by IOC MnsInfo (clause 4.3.42).

As defined in 29.222[19], the service API is described in a ServiceAPIDescription datatype (clause 8.2.4.2.2) which contains one or multiple aefProfiles (clause 8.2.4.2.4). Each aefProfile contains one or multiple API versions (clause 8.2.4.2.5). Each API version may expose one or multiple resources (clause 8.2.4.2.6).

One possible solution to represent an exposed MnS as a Service API is as follows:

MnsInfo attribute mnsLabel is mapped to ServiceAPIDescription/apiName.

MnsInfo attribute mnsVersion is mapped to ServiceAPIDescription/AefProfile/Version/apiVersion.

MnsInfo attribute mnsType is mapped to ServiceAPIDescription/AefProfile/Version/Resource/resourceName.

MnsInfo attribute mnsAddress is mapped to ServiceAPIDescription/AefProfile/Version/Resource/uri.

MnsInfo attribute mnsScope is mapped to ServiceAPIDescription/AefProfile/Version/Resource/description.

Editor Notes 3: Whether the authorization mechanism as defined in [14] need to be extended is FFS.

## 7.11 Potential solution for consumption of exposed MnS after service order completed

This clause describes a solution for the procedure for consumption of exposed MnS after service order completed described which is described in clause 4.1.4.6. For each step in the procedure Table 7.11.1 identifies the following:

- if an interface is:

- Internal to the NSP,

- External between a NSC and NSP,

- None, for internal processes within a function.

- which operation or notification is used by that step, and

- which specification describes the interface (stage 2 and stage 3).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | Description in step | Interface | Reference | Description in reference |
| 1 | Authentication and authorization request | Internal | TS 23.222[14], clause 6.4.2 | CAPIF-1 |
| 2 |  | None | - | - |
| 3 | Authentication and authorization response | Internal | TS 23.222[14], clause 6.4.2 | CAPIF 1 |
| 4 | Discovery request | Internal | TS 23.222[14], clause 6.4.2 | CAPIF-1 |
| 5 |  | None | - | - |
| 6 | Discovery response | Internal | TS 23.222[14], clause 6.4.2 | CAPIF-1 |
| 7 | Authentication and authorization request | Internal | TS 23.222[14], clause 6.4.4 | CAPIF-2 |
| 8 |  | None |  |  |
| 9 | Authentication and authorization response | Internal | TS 23.222[14], clause 6.4.4 | CAPIF-2 |
| 10 | API invocation request | Internal | TS 23.222[14], clause 6.4.4 | CAPIF-2 |
| 11 |  | None |  |  |
| 12 | MnS request | Internal | TS 28.532 | MnS |
| 13 | MnS response | Internal | TS 28.532 | MnS |
| 14 |  | None |  |  |
| 15 | API invocation response | Internal | TS 23.222[14], clause 6.4.4 | CAPIF 2 |

Table 7.11.1 Solution for consumption of exposed MnS within the operator trusted domain (NSC\_Application is inside operator trusted domain)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Step | Description in step | Interface | Reference | Description in reference |
| 1 | Authentication and authgorizationrequest | External | TS 23.222[4], clause 6.4.3 | CAPIF-1e |
| 2 |  | None | - | - |
| 3 | Authentication and authorization response | External | TS 23.222[4], clause 6.4.3 | CAPIF 1e |
| 4 | Discovery request | External | TS 23.222[4], clause 6.4.3 | CAPIF-1e |
| 5 |  | None | - | - |
| 6 | Discovery response | External | TS 23.222[4], clause 6.4.3 | CAPIF-1e |
| 7 | Authentication and authorization request | External | TS 23.222[14], clause 6.4.5 | CAPIF-2e |
| 8 |  | None |  |  |
| 9 | Authentication and authorization response | External | TS 23.222[14], clause 6.4.5 | CAPIF-2e |
| 10 | API invocation request | External | TS 23.222[4], clause 6.4.5 | CAPIF-2e |
| 11 |  | None |  |  |
| 12 | MnS request | Internal | TS 28.532 | MnS/ |
| 13 | MnS response | Internal | TS 28.532 | MnS/ |
| 14 |  | None |  |  |
| 15 | API invocation response | External | TS 23.222[4], clause 6.4.5 | CAPIF 2e |

**Table 7.**11**.2 Solution for consumption of exposed MnS outside operator trusted domain (NSC\_Application is outside operator trusted domain)**

## 7.12 Possible solution for “Exposure to application servers and application functions” – Section 5.8

For consumer entities internal to the operator the access details to MnS are directly configured by the operator.

For consumer entities (AS or AF) external to the operator, the assumption is that the appropriate business relation exists between the entity owner and the operator. Given such an assumption, the following steps recommend how the consumer entities can access the exposed MnS. The steps assume that the entity is aware of the MnS:

1) The entity approaches an access controlling entity requesting access to the MnS. Which MnS and how this access is provided is implementation and business agreement dependent and is completely controllable by the operator.

2) If authorized, and in accordance with the business agreement the access controlling entity provides access tokens (which may be limited in some way) to the consumer entity.

3) These access tokens are then used by the consumer entity to access the exposed MnS.

## 7.13 Possible solution for end-to-end handling of NSC requirements for network slice management capabilities exposure

In this possible solution:

1. Network Slice Customer (NSC) orders a network slice to its Network Slice Provider (NSP). In the product order request, NSC expresses its requirements wrt. bandwidth, latency, coverage, etc. In addition, NSC may express its requirements for network slice management capabilities exposure;

NOTE 1: In order to enable NSC to express its network slice management capabilities exposure expectations, whether a new attribute is needed in NG.116 GST is FFS.

2. NSP BSS receives and analyzes NSC product order request;

3. NSP BSS sends a service order request to NSP OSS SML. The service order request includes NSC requirements including those related to network slice management capabilities exposure;

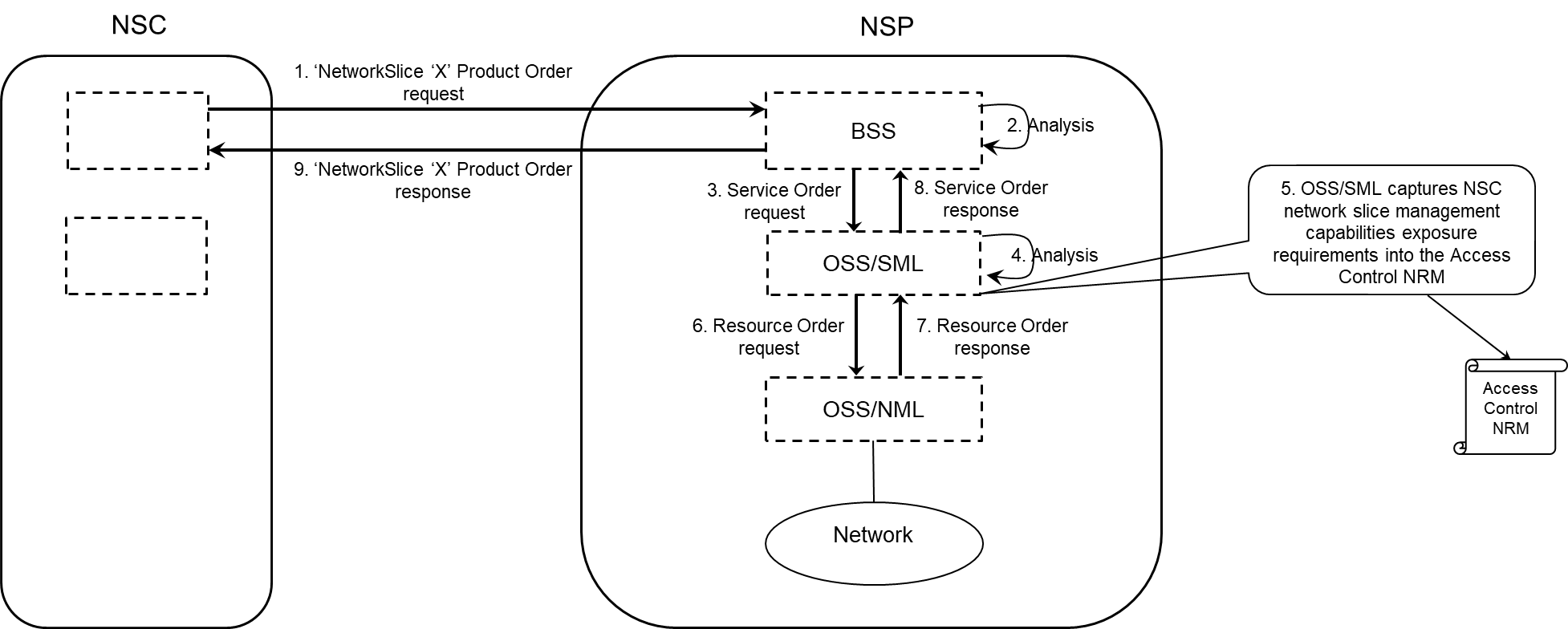
4. NSP OSS SML receives these requirements, analyzes them

5. NSP OSS SML captures them in the form of NSC-specific access control data

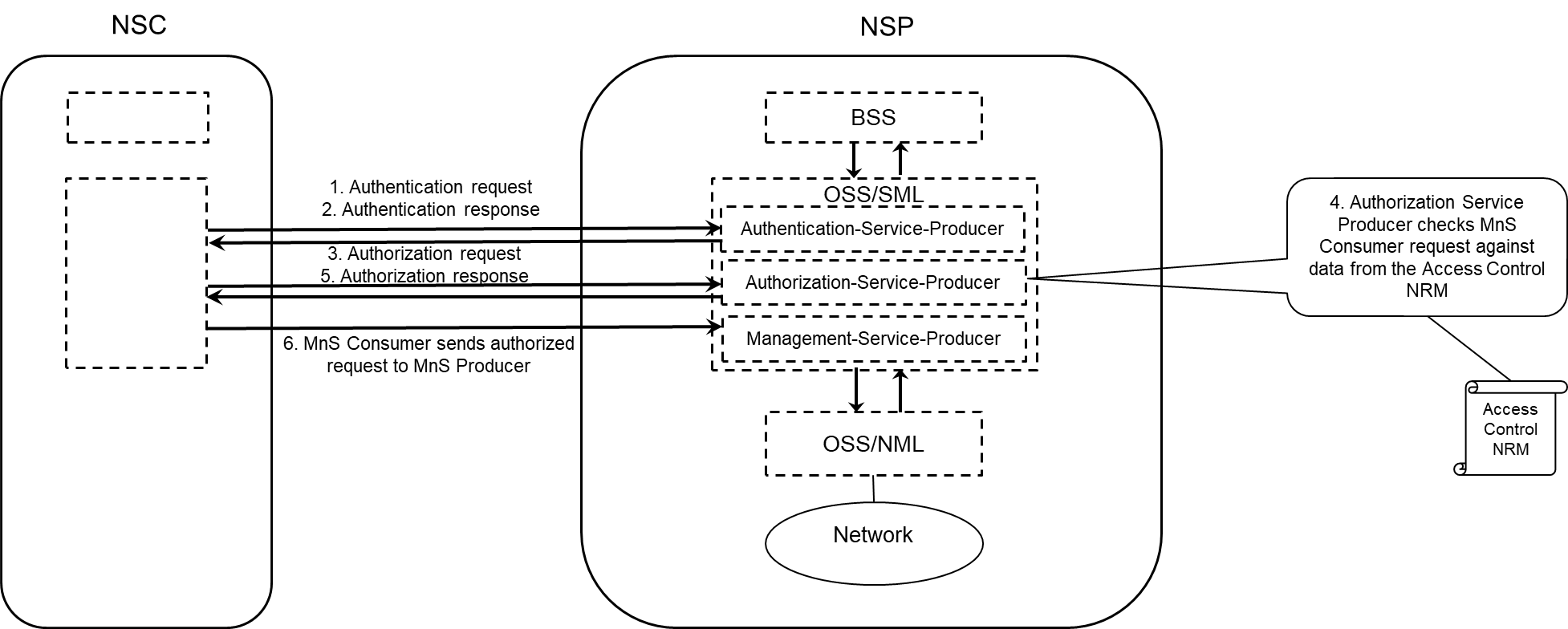
NOTE: an Access Control NRM fragment is required to capture per NSC (a.k.a. tenant) access rights.

6. NSP OSS/SML sends the service order response to BSS;

7. NSP BSS sends the product order response order to NSC.



Then, during the network slice operation phase, if NSC requests access to network slice management capabilities, NSP may, during the authorization phase, check NSC request against the data available in its Access Control NRM.



NSP OSS SML may accept or reject NSC request to access to network slice management capabilities.

# 8 Conclusion and Recommendation

## 8.1 Reference Architecture for network slice ordering, provisioning and assurance

### 8.1.1 Conclusion

From the use case specific architectures depicted in:

# Clause 4.1.1.4.2 (Exposure scenarios)

# Clause 4.1.3.2 (Use case No.1: simple case)

# Clause 4.1.3.3 (Use case No.2: partners involved)

# Clause 5.5 (Exposure of network slice as a product)

- 5.5.1.1 (Sub-use case 1: NSP and NOP played by the same organization)

- 5.5.1.2 (Sub-use case 2: NOP role played simultaneously by different organizations)

# Clause 5.6 (Exposure of network slice as a service)

- 5.6.1.1 (Sub-use case 1: NSP and NOP play by the same organization)

- 5.6.1.2 (Sub-use case 2: NOP role played simultaneously by different organizations)

, it is possible to derive a reference architecture valid for all use cases, by merging the use case specific architectures.

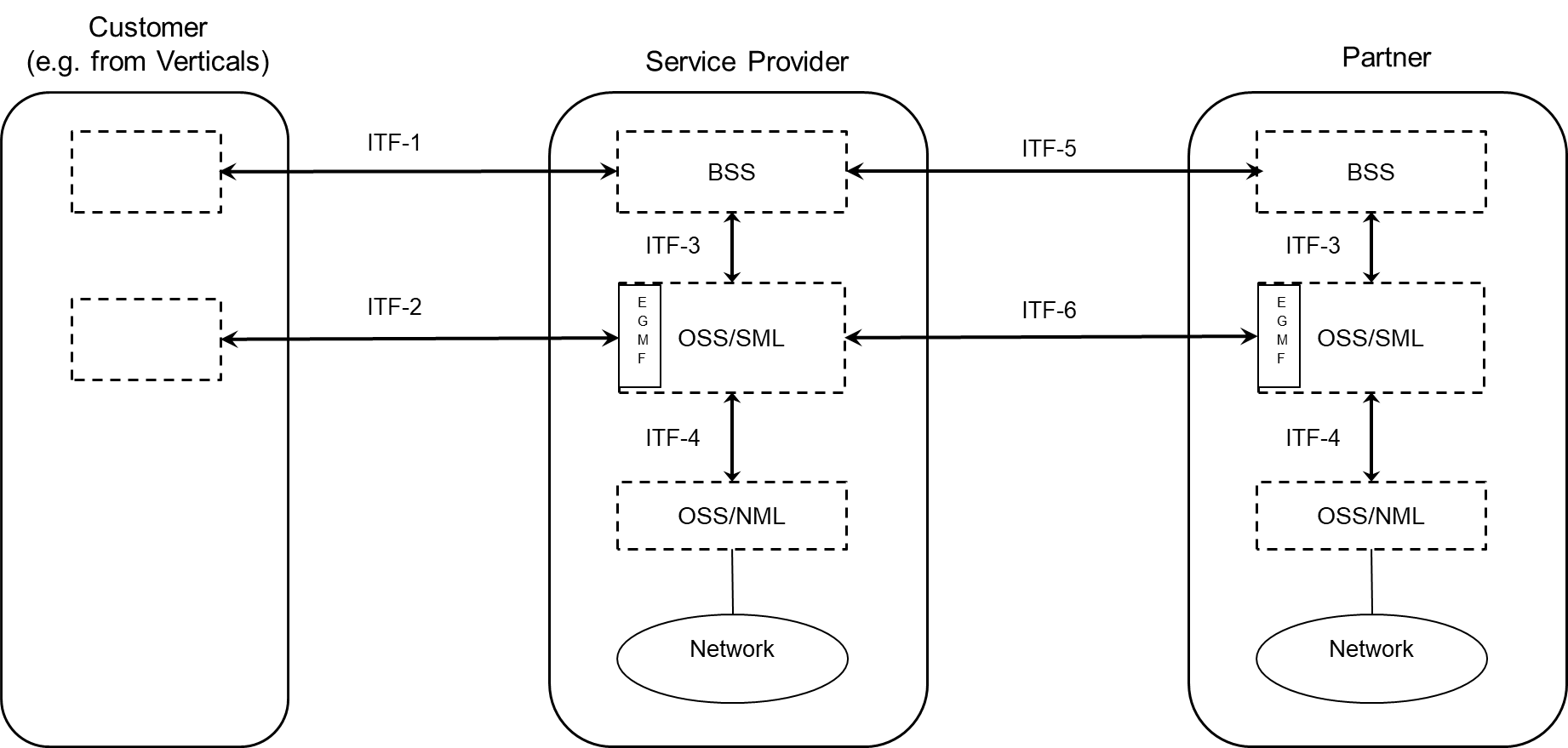


Figure 8.1.1-1: Reference architecture for network slice ordering, provisioning and assurance.

The interfaces present in this reference architecture are:

- Inter-organization interfaces (represented East-West):

- Between the Customer and the Service Provider:

- Interface ITF-1 to:

- create a product (e.g. network slice) order,

- retrieve information concerning a product (e.g. network slice) order,

- update a product (e.g. network slice) order,

- delete a product (e.g. network slice) order;

Candidate APIs for Interface ITF-1 include, but are not limited to, TMF API 622 (Product ordering), in which case entities managed via this interface include ProductOrder, ProductOrderItem, etc. defined in TMF 622 [2].- Interface ITF-2 to:

- enable the Service Provider to expose, from its Service Management Layer, network slice management capabilities to the Customer;

Candidate APIs for Interface ITF-2 include TS 28.531, TS 28.532, TS 28.545, TS 28.550.

Entities managed via the Interface ITF-2 include NetworkSlice (cf. TS 28.541 [9]).

At the Service Provider’s side of Interface ITF-2, the Exposure Governance Management Function (EGMF) governs the network slice management capabilities exposure.

- Between the Service Provider and its Partner(s):

- Interface ITF-5 to:

- create a product order,

- retrieve information concerning a product order,

- update a product order,

- delete a product order;

Candidate APIs for Interface ITF-5 include, but are not limited to, TMF API 622 (Product ordering), in which case entities managed via this interface include ProductOrder, ProductOrderItem, etc. defined in TMF 622 [2].

- Interface ITF-6 to:

- enable the Partner to expose, from its Service Management Layer, network slice management capabilities to the Service Provider;

Candidate APIs for Interface ITF-6 include TS 28.531, TS 28.532, TS 28.545, TS 28.550.

Entities managed via the Interface ITF-6 include NetworkSlice (cf. TS 28.541 [9]).

At the Service Provider’s side of Interface ITF-6, the Exposure Governance Management Function (EGMF) governs the network slice management capabilities exposure.

- Intra-organization interfaces (represented North-South), internal to the Service Provider:

- Between its BSS and its OSS/SML

- Interface ITF-3 to:

- create a service order,

- retrieve information concerning a service order,

- update a service order,

- delete a service order;

Candidate APIs for Interface ITF-3 include, but are not limited to, TMF API 641 (Service ordering), in which case entities managed via this interface include ServiceOrder, ServiceOrderItem, etc. defined in TMF 641 [3].

- Between its OSS/SML and its OSS/NML

- Interface ITF-4 to:

- create a network slice / network slice subnet,

- retrieve information concerning a network slice / network slice subnet,

- update a network slice / network slice subnet,

- delete a network slice / network slice subnet,

- collect PM and FM data concerning a network slice / network slice subnet;

Candidate APIs for Interface ITF-4 include, TS 28.531, TS 28.532, TS 28.545, TS 28.550.

Entities managed via the Interface ITF-4 include NetworkSlice, NetworkSliceSubnet, etc. (cf. TS 28.541 [9]).

NOTE: in order not to create confusion, especially for external readers, it has been proposed in Figure 8.1.1-1 to rename interfaces, since interfaces Type-A and Type-B, used elsewhere in this TR, could be mixed up with MnS Component Type-A, Type B, Type C, defined in TS 28.533; similarly, interfaces Type-1 and Type-2, used elsewhere in this TR, could be mixed up with interfaces type 1, 2, etc. defined in TS 32.101.

### 8.1.2 Recommendation

It is recommended that the architecture depicted in clause 8.1.1 be included in a normative TS, as the Rel-18 reference architecture for network slice ordering, provisioning and assurance. The above list of candidate interfaces / APIs is not exhaustive. Other organizations / open source projects / etc. may use this reference architecture with different interfaces / APIs.

## 8.2 Network slice management capability exposure via CAPIF

### 8.2.1 Conclusion

Three alternatives for potential solutions (see clause 7.9.1, 7.9.2 and 7.9.3) for network slice management capability exposure via CAPIF have been evaluated in clause 7.9.4, which can help to draw the conclusion and recommendation for the solutions. Based on the evaluation, all analysed gaps can be resolved by alternative 2 and alternative 3 since all the related interfaces are within the scope of alternative 2 and alternative 3.

Meanwhile, alternative 2 and alternative 3 are also supported in solution for network slice management capability exposure depicted in clause 7.9.10.

Clause B.3.2 Deployment model of TS 23.222 [14] illustrates the integrated deployment of the 3GPP network exposure systems (SCEF and NEF) with the CAPIF. The SCEF and the NEF may be integrated with a single CAPIF core function, where the CAPIF core function takes the role of a unified gateway, to offer their respective service APIs to the API invokers.

To make CSPs have a single gateway to expose whatever capability they want, SA5 is advised to follow the same deployment approach as SA2 regarding SCEF/NEF integration into CAPIF framework. This approach would mean the following :

* The CAPIF core function, the SCEF, the NEF and the logical MnF providing management capability exposure governance are all deployed in the PLMN trust domain
* The CAPIF core function, providing API registration and discovery capabilities, takes the role of a unified gateway and provides the entry point of exposure services provided by multiple 3GPP capabilities to different API invokers.
* The API invokers obtains the T8, N33 and MnS service API information and the corresponding entry point details from the CAPIF core function via CAPIF-1 or CAPIF-1e reference points.

SA5 alternative 2 fits this deployment approach well. Therefore, it is suggested to recommend alternative 2 as baseline for the normative work.

### 8.2.2 Recommendation

It is recommended that the alternative 2 depicted in clause 7.9.2 as baseline for the normative work. This work includes:

* Specify normative requirements on management capability exposure;
* Gap analysis, by comparing specified requirements against the features provided by the alternative 2. In case there are gaps, SA5 will conduct the following activity plan:
  + Document identified gaps, and recommended actions to bridge them.
  + Communicating the above (i.e., gaps + recommendations) to SA6, so that SA6 can take action on TS 23.222 accordingly, enhancing CAPIF as needed.
* Define procedures enabling different external consumers to access management services via CAPIF.

## 8.3 Filtering

### 8.3.1 Conclusion

As introduced in clause 4.1.1.3.1, the filtering is the exposure access control on certain information elements (i.e. granular access) of MnS component type A, type B and/or type C. Filtering plays an important role on exposure governance. It provides the ability to provision segregated yet tailored permissions to authorised MnS consumers in resource sharing environments, ensuring these permissions do not conflict our used by unauthorised MnS consumers. The solutions to implement the filtering functionality can leverage MSAC outcomes, and may translate into enhancements/extensions to NRM.

### 8.3.2 Recommendation

It is recommended to use granular access control mechanisms defined in MSAC work item as baseline solution for the filtering functionality.

## 8.4 Capability exposure ecosystem

### 8.4.1 Conclusion

The capability exposure ecosystem has been presented in clause 4.2.7, reporting on participating organizations and their scope of work. The touchpoints of their activities have been also clarified, noting the relevance of GSMA Open Gateway and TM Forum with regards to the exposure of management capabilities to 3rd parties.

### 8.4.2 Recommendation

In normative work, it is recommended for SA5 to:

* Aligning with the view drafted in GSMA Open Gateway initiative, to avoid industry misalignment and capability exposure ending up with a fragmented ecosystem.
* Consider the outcomes produced and periodically reported (via public documents and/or Liaisons Statements) by GSMA Open Gateway and TM Forum when developing solutions for management capability exposure in normative work.

Provide inputs to (and assist) GSMA Open Gateway and TM Forum for those capabilities whose invocation trigger FCAPS management operations on 5G managed resources (e.g., RAN NFs, 5GC NFs, sub-networks, network slices). These inputs may be provided through Liaison Statements with these two organizations, and/or the organizations of joint workshops.

Annex A:  
Appendix with UML code of the sequence diagrams

# A.1 UML code for Figure 4.1.4.2.1

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

autonumber

actor NSC

participant BSS\_NSP

participant OSS\_SML

participant OSS\_NML

NSC --> BSS\_NSP : product order

BSS\_NSP --> BSS\_NSP : process product order

BSS\_NSP --> OSS\_SML : service order(s)

OSS\_SML --> OSS\_SML : process service order(s)

OSS\_SML --> OSS\_NML : resource order(s)

OSS\_NML --> OSS\_NML : process resource order(s)

OSS\_SML <-- OSS\_NML : resource order(s) completed

BSS\_NSP <-- OSS\_SML : service order(s) completed

NSC <-- BSS\_NSP : product order completed

@enduml

# A.2 UML code for Figure 4.1.4.3.1

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

autonumber

actor NSC

participant BSS\_NSP

participant BSS\_CSP #lightgrey

participant OSS\_CSP #lightgrey

NSC --> BSS\_NSP : product order

BSS\_NSP --> BSS\_NSP : process product order

BSS\_NSP --> BSS\_CSP : product order(s)

BSS\_CSP --> BSS\_CSP : process product order(s)

BSS\_CSP --> OSS\_CSP : service order(s)

OSS\_CSP --> OSS\_CSP : process service order(s)

BSS\_CSP <-- OSS\_CSP : service order(s) completed

BSS\_NSP <-- BSS\_CSP : product order(s) completed

NSC <-- BSS\_NSP : product order completed

note right of OSS\_CSP

BSS\_NSP belongs to the company

fulfilling the NSP role.

BSS\_CSP (grey) and OSS\_CSP (grey) belong

to the company fulfilling the CSP role.

end note

@enduml

# A.3 UML code for Figure 4.1.4.4.1

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

autonumber

actor NSC

participant BSS\_NSP

participant OSS\_NSP

participant BSS\_CSP #lightgrey

participant OSS\_CSP #lightgrey

NSC --> BSS\_NSP : product order

BSS\_NSP --> BSS\_NSP : process product order

BSS\_NSP --> OSS\_NSP : service order(s)

OSS\_NSP --> OSS\_NSP : process service order(s)

OSS\_NSP --> OSS\_CSP : service order(s)

OSS\_CSP --> OSS\_CSP : process service order(s)

OSS\_CSP --> BSS\_CSP : notify service order(s) completed

OSS\_NSP <-- OSS\_CSP : service order(s) completed

BSS\_NSP <-- OSS\_NSP : service order(s) completed

NSC <-- BSS\_NSP : product order completed

note right of OSS\_CSP

BSS\_NSP and OSS\_NSP belong

to the company fulfilling the NSP role.

BSS\_CSP (grey) and OSS\_CSP (grey) belong

To the company fulfilling the CSP role.

end note

@enduml

# A.4 UML code for Figure 4.1.2.1.1

@startuml

skinparam backgroundColor white

skinparam classBackgroundColor white

skinparam classBorderColor black

skinparam rectangleBackgroundColor white

skinparam rectangleBorderColor black

skinparam Shadowing false

skinparam noteBackgroundColor white

skinparam noteBorderColor black

skinparam arrowColor black

hide circle

hide members

left to right direction

rectangle Exposed\_MnS\_Consumer

rectangle Exposed\_MnS\_Producer

Exposed\_MnS\_Consumer -(0- Exposed\_MnS\_Producer: exposed MnS

@enduml

# A.5 UML code for Figure 4.1.4.5

@startuml

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

actor NSC

participant BSS\_NSP

participant OSS\_SML

participant OSS\_NML

OSS\_SML--> OSS\_NML: 1. service discovery

OSS\_SML---> OSS\_SML: 2. configure the available MnS service

opt

BSS\_NSP -->OSS\_SML: 3. request list of available services

end

OSS\_SML---> BSS\_NSP: 4. provide list of available services

BSS\_NSP --> BSS\_NSP: 5. configure the MnS service for exposure

NSC --> BSS\_NSP: 6. product catalogue request

BSS\_NSP --> NSC: 7. product catalogue

@enduml

# A.6 UML code for 7.3.1

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

actor NSC

participant BSS\_NSP

participant MnS\_Discovery\_service\_producer

BSS\_NSP --> MnS\_Discovery\_service\_producer: 1. request to obtain MnS data

MnS\_Discovery\_service\_producer --> BSS\_NSP: 2. response for MnS data

Ref over NSC, BSS\_NSP : 3. procedure of product order

@enduml

# A.7 UML code for 7.3.2

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

BackGroundColor <<BSS\_Prov>> Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor Black

skinparam shadowing false

hide footbox

actor NSC

participant BSS\_NSP

participant MnS\_Discovery\_service\_producer

participant OSS\_SML

Ref over NSC, OSS\_SML: 1. procedure of product order

Ref over NSC, OSS\_SML: 2. authentication and authorization for accessing exposed MnS discovery service

NSC --> MnS\_Discovery\_service\_producer: 3. request to obtain MnS data for exposed MnS

MnS\_Discovery\_service\_producer --> NSC: 4. response for exposed MnS data for exposed MnS

NSC ---> OSS\_SML: 5. request to use an exposed MnS

OSS\_SML---> NSC: 6. response for using an exposed MnS

@enduml

# A.8 UML code for Figure 4.1.4.6.1

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor White

skinparam NoteColor White

skinparam shadowing false

hide footbox

autonumber

participant NSC\_Application

box "CAPIF core and API provider domain functions" #white

participant "CAPIF\_Core\_\nfunction" as CAPIF\_Core

participant "API\_Provider\_\ndomain\_function" as API\_Provider

end box

participant MnS\_Producers

NSC\_Application --> CAPIF\_Core : Authentication and authorization request

CAPIF\_Core -> CAPIF\_Core: process request

NSC\_Application <-- CAPIF\_Core : Authentication and authorization response

NSC\_Application --> CAPIF\_Core : Discovery request

CAPIF\_Core -> CAPIF\_Core: process request

NSC\_Application <-- CAPIF\_Core : Discovery response

NSC\_Application --> API\_Provider : Authentication and authorization request

API\_Provider -> API\_Provider: process request

NSC\_Application <-- API\_Provider : Authentication and authorization response

NSC\_Application --> API\_Provider : API Invocation request

API\_Provider -> API\_Provider: process request

API\_Provider --> MnS\_Producers: MnS request

API\_Provider <-- MnS\_Producers: MnS response

API\_Provider -> API\_Provider: process response

NSC\_Application <-- API\_Provider : API Invocation response

@enduml

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| *2021-05* | *SA5#137e* | *S5-213046* | *-* | *-* | *-* | *28.824 skeleton-0.0.0* | *0.0.0* |
| *2021-05* | *SA5#137e* | *S5-213565* | *-* | *-* | *-* | *pCR 28.824 External exposure via BSS* | *0.1.0* |
| *2021-05* | *SA5#137e* | *S5-213566* | *-* | *-* | *-* | *pCR 28.824 Add Description of Concept and Roles to TR 28.824* | *0.1.0* |
| *2021-05* | *SA5#137e* | *S5-213658* | *-* | *-* | *-* | *pCR 28.824 Use case – network slice management capability exposure* | *0.1.0* |
| *2021-05* | *SA5#137e* | *S5-213564* | *-* | *-* | *-* | *pCR 28.824 Use case – Exposure of MnS for monitoring QoS of video application* | *0.1.0* |
| *2021-08* | *SA5#138e* | *S5-214645* | *-* | *-* | *-* | *pCR 28.824 Use case – eMnS discovery service* | *0.2.0* |
| *2021-08* | *SA5#138e* | *S5-214646* | *-* | *-* | *-* | *pCR 28.824 eMNs discovery by other systems* | *0.2.0* |
| *2021-08* | *SA5#138e* | *S5-214128* | *-* | *-* | *-* | *pCR 28.824 Improve description of roles* | *0.2.0* |
| *2021-10* | *SA5#139e* | *S5-215523* | *-* | *-* | *-* | *pCR 28.824 Add use case for the exposure of network slice as a product* | *0.3.0* |
| *2021-10* | *SA5#139e* | *S5-215524* | *-* | *-* | *-* | *pCR 28.824 Types of interfaces for the exposure of network slice* | *0.3.0* |
| *2021-10* | *SA5#139e* | *S5-215525* | *-* | *-* | *-* | *pCR 28.824 Service management scenarios between CSC, CSP and NSP* | *0.3.0* |
| *2021-10* | *SA5#139e* | *S5-215526* | *-* | *-* | *-* | *pCR 28.824 Key issues relative to network slice management capabilities exposure* | *0.3.0* |
| *2021-10* | *SA5#139e* | *S5-215578* | *-* | *-* | *-* | *Possible solution to support eMnS discovery service* | *0.3.0* |
| *2021-10* | *SA5#139e* | *S5-215579* | *-* | *-* | *-* | *Solution for external discovery* | *0.3.0* |
| *2021-11* | *SA5#140e* | *S5-216583* | *-* | *-* | *-* | *Clarification on clause 4 overview* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216616* | *-* | *-* | *-* | *Add Use Case for exposure without going through BSS* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216617* | *-* | *-* | *-* | *Exposure of network slice as a service* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216624* | *-* | *-* | *-* | *Consolidate potential requirements of use cases for eMnS discovery service* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216585* | *-* | *-* | *-* | *Add procedures related to product onboarding* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216586* | *-* | *-* | *-* | *Clarification on clause 5 use cases* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216385* | *-* | *-* | *-* | *Clarification on clause 7 solution* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216582* | *-* | *-* | *-* | *Concept definition for Exposed Management Service* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216623* | *-* | *-* | *-* | *Exposure to SA6 applications or middleware* | *0.4.0* |
| *2021-11* | *SA5#140e* | *S5-216625* | *-* | *-* | *-* | *Add text to procedures related to management capability exposure* | *0.4.0* |
| *2022-02* | *SA5#141e* | *S5-221570* | *-* | *-* | *-* | *Add new solution for MnS discovery service for exposure* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221713* | *-* | *-* | *-* | *Skeleton restructuring proposal* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221714* | *-* | *-* | *-* | *Key issue and solution on exposure interface via OSS* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221719* | *-* | *-* | *-* | *pCR 28.824 Clarification on access to exposed MnS* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221742* | *-* | *-* | *-* | *Add solution for product and service order procedures to clause 7* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221743* | *-* | *-* | *-* | *Update procedure for product on-boarding* | *0.5.0* |
| *2022-02* | *SA5#141e* | *S5-221744* | *-* | *-* | *-* | *Resolve EN in 5.4* | *0.5.0* |
| *2022-04* | *SA5#142e* | *S5-222756* | *-* | *-* | *-* | *Describe possible solution for EGMF* | *0.6.0* |
| *2022-04* | *SA5#142e* | *S5-222680* | *-* | *-* | *-* | *Update use case 5.2* | *0.6.0* |
| *2022-04* | *SA5#142e* | *S5-222725* | *-* | *-* | *-* | *Solution on exposure architecture and related API* | *0.6.0* |
| *2022-05* | *SA5#143e* | *S5-223620* | *-* | *-* | *-* | *Make descriptions in issues and gaps more uniform* | *0.7.0* |
| *2022-05* | *SA5#143e* | *S5-223621* | *-* | *-* | *-* | *Update position and add solution for direct MnS exposure* | *0.7.0* |
| *2022-05* | *SA5#143e* | *S5-223622* | *-* | *-* | *-* | *Update to solution regarding CAPIF based management capability exposure* | *0.7.0* |
| *2022-05* | *SA5#143e* | *S5-223623* | *-* | *-* | *-* | *Add note on possible charging impact* | *0.7.0* |
| *2022-05* | *SA5#143e* | *S5-223624* | *-* | *-* | *-* | *Solution for Network slice management capability exposure* | *0.7.0* |
| *2022-05* | *SA5#143e* | *S5-223625* | *-* | *-* | *-* | *Add procedure for consumption of exposed MnS after service order completed* | *0.7.0* |
| *2022-07* | *SA5#144e* | *S5-224121* | *-* | *-* | *-* | *Add solution based on CAPIF ServiceAPIDescription* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224436* | *-* | *-* | *-* | *Updating use case for Network slice management capability exposure* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224443* | *-* | *-* | *-* | *Update of solution 7.9* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224442* | *-* | *-* | *-* | *evaluation of solution 7.9* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224437* | *-* | *-* | *-* | *Requirements related to authorized external consumers* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224120* | *-* | *-* | *-* | *Editorial improvements* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224288* | *-* | *-* | *-* | *Rephrase or replace eMnS with exposed MnS* | *0.8.0* |
| *2022-07* | *SA5#144e* | *S5-224289* | *-* | *-* | *-* | *Update introduction to procedures 4.1.4.1* | *0.8.0* |
| *2022-08* | *SA5#145e* | *S5-225249* | *-* | *-* | *-* | *Removal of unused interfaces in alternative 3* | *0.9.0* |
| *2022-08* | *SA5#145e* | *S5-225248* | *-* | *-* | *-* | *Cleanup of exposure without going through BSS* | *0.9.0* |
| *2022-08* | *SA5#145e* | *S5-225870* | *-* | *-* | *-* | *Rephrase or replace eMnS with exposed MnS* | *0.9.0* |
| *2022-08* | *SA5#145e* | *S5-225871* | *-* | *-* | *-* | *Update of solution 7.9* | *0.9.0* |
| *2022-11* | *SA5#146e* | *S5-227025* | *-* | *-* | *-* | *Concepts of filtering and combination in exposure governance* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227030* | *-* | *-* | *-* | *Concepts of filtering in exposure governance* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227033* | *-* | *-* | *-* | *Merge the use cases related to exposed MnS discovery* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227034* | *-* | *-* | *-* | *Merge the use cases related to network slice management capability exposure* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227035* | *-* | *-* | *-* | *Update the description of exposure scenarios in clause 4.1.1* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227036* | *-* | *-* | *-* | *Update Solution for network slice management capability exposure via CAPIF* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-227037* | *-* | *-* | *-* | *Handling of customer's requirement for network slice management capabilities exposure* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-226321* | *-* | *-* | *-* | *Add cons for alternative 1* | *0.10.0* |
| *2022-11* | *SA5#146e* | *S5-226325* | *-* | *-* | *-* | *Add Reference Architecture* | *0.10.0* |
| *2023-03* | *SA5#147* | *S5-232890* | *-* | *-* | *-* | *Clarify usage of CAPIF-1 and CAPIF-1e* | *0.11.0* |
| *2023-04* | *SA5#148e* | *S5-233354* | *-* | *-* | *-* | *Improve discovery solution* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233355* | *-* | *-* | *-* | *Improve description of exposure governance* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233626* | *-* | *-* | *-* | *clean-up* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233627* | *-* | *-* | *-* | *Add conclusion and recommendation for network slice management capability exposure via CAPIF* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233628* | *-* | *-* | *-* | *Add conclusion and recommendation for filtering* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233629* | *-* | *-* | *-* | *Correction of terminologies* | *0.12.0* |
| *2023-04* | *SA5#148e* | *S5-233630* | *-* | *-* | *-* | *Remove the EN about exposed management services* | *0.12.0* |
| *2023-05* | *SA5#149* | *S5-234080* | *-* | *-* | *-* | *Remove EN in clause 4.1.4.5* | *0.13.0* |
| *2023-05* | *SA5#149* | *S5-234081* | *-* | *-* | *-* | *Remove obsolete ENs* | *0.13.0* |
| *2023-05* | *SA5#149* | *S5-234082* | *-* | *-* | *-* | *Update exposed MnS discovery service* | *0.13.0* |
| *2023-05* | *SA5#149* | *S5-234564* | *-* | *-* | *-* | *Update scope clause* | *0.13.0* |
| *2023-05* | *SA5#149* | *S5-234565* | *-* | *-* | *-* | *Modify conclusions and recommendations for management capability exposure in normative work* | *0.13.0* |
| *2023-05* | *SA5#149* | *S5-234566* | *-* | *-* | *-* | *Add conclusions and recommendations for NaaS ecosystem* | *0.13.0* |
| *2023-06* | *SA#100* | *SP-230735* |  |  |  | *Presented for information and approval* | *1.0.0* |
| 2023-06 | SA#100 |  |  |  |  | Upgrade to change control version | 18.0.0 |