**3GPP TSG-SA5 Meeting #140-eS5-216383**

**e-meeting, 15 - 24 November 2021**

**Source: Ericsson, Deutsche Telekom**

**Title: Clarifications on clause 4 overview**

**Document for: Approval**

**Agenda Item: 6.5.4**

# 1 Decision/action requested

***The group is asked to agree the text in detailed proposal.***

# 2 References

Not applicable

# 3 Rationale

This contribution proposes a number of changes to clause 4 overview to improve readability and understanding. The following changes are proposed:

- the study has progressed and the text in clause 4.1.1.3 on exposure scenarios has been replaced with more recent agreed text in clause 4.1.3. It is proposed to remove the sub-structure under 4.1.1.3 and remove clause 4.1.1.3.2 which is old text and old figures;

- the heading of clause 4.1.2 is currently Exposed MnS consumer, this is not the correct phrasing as this MnS consumer consumes exposed MnSs it is more appropriate to call it External MnS consumer. That is an MnS consumer outside the operator’s management domain;

- the figures describing Use case 1 and Use case 2 do not have a title. Titles are proposed to be added; and

- minor spelling corrections.

# 4 Detailed proposal

|  |
| --- |
| **First change** |

# 4 Overview

## 4.1 General

### 4.1.1 Concepts related to network management capability exposure

#### 4.1.1.1 Exposed Management Services

Exposed MnS (eMnS) represents the MnS that can be exposed by MnS producer to the external MnS consumer. eMnS 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.

Editor’s notes: Whether eMnS is exposed transparently to external MnS consumer via BSS or being processed through a dedicated exposure platform is FFS.

#### 4.1.1.2 Exposure of Management Services

Exposure of management services indicates the case that an external MnS consumer which is outside 3GPP management system can indirectly access management capability offered by MnS producer within 3GPP management system. In order to enable the exposure of eMnS, an external customer, which has external MnS consumer, has to sign a contract with the CSP or NOP, which contains the agreement and conditions for exposing an eMnS, by a CSP or NOP. The signing of the contract may need the interaction with BSS. The condition can be a certain constraint of eMnS access based on the contract, e.g. the access quota of certain eMnS, the access frequency of certain eMnS, etc.

#### 4.1.1.3 Exposure via BSS

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.

### 4.1.2 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 (eMnS). 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 accessing management capability offered by an Exposed MnS producer is called an Exposed MnS consumer. An eMnS consumer is equivalent to an MnS consumer with the difference that it is outside the trust domain of the CSP or NOP. An eMnS 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 accessed by an Exposed MnS consumer is called Exposed MnS producer. An eMnS 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, 3GPP 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 which is corresponding to a RAN sharing scenario.

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 network management capability exposure

#### 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 if 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

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



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

Editor’s Note: The details and the description of the steps in the sequence diagram as well as the actual names of requests and responses are FFS

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



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

Editor’s Note: The details and the description of the steps in the sequence diagram as well as the actual names of requests and responses are FFS

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



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

Editor’s Note: The details and the description of the steps in the sequence diagram as well as the actual names of requests and responses are FFS

## 4.2 Key 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, within the scope of SA6.
* Management layer capabilities, within the scope of SA5.
* Network layer capabilities, within the scope of SA2.

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, SA2), management layer capabilities (@MCEG, SA5), application layer capabilities (@SEAL, SA6), together with non-3GPP capabilities (e.g. cloud related capabilities). Otherwise, if every SA WG starts defining their own exposure fabric, (i) the likelihood of encountering incompatibilities/duplicities across these WG 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. Which 3GPP working group is responsible to provide the single exposure layer is FFS.

## 4.2.3 Issue #3: EGMF/MCEG

The Exposure Governance Management Function (EGMF) was originally defined in TS 28.533 [2] 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 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 SA5 really need to define this MnF? Doesn’t this approach mean moving away from producer centric model of SA5, i.e., focus on service producers rather than MnFs?
* If EGMF standardization is within the scope of SA5, then does SA5 need to provide details on EGMF internals? Does SA5 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 SA2/SA5/SA6 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. 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.

|  |
| --- |
| **Second of change** |

Annex A (informative):
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

actor NSC

participant BSS\_NSP

participant OSS\_SML

participant OSS\_NML

participant Network

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 : request(s) for management and orchestration\nof resources

OSS\_NML --> OSS\_NML : process request(s) for management and orchestration\nof resources

OSS\_NML --> Network : management and orchestration\nof resources

OSS\_NML <-- Network : management and orchestration\nof resources completed

OSS\_SML <-- OSS\_NML : request(s) for management and orchestration\nof resourcescompleted

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

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 --> 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 completed(s)

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

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.X 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: eMnS

@enduml

|  |
| --- |
| **End of changes** |