**3GPP TSG-SA5 Meeting #140-eS5-216384**

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

**Source: Ericsson, Deutsche Telekom**

**Title: Clarifications on clause 5 use cases**

**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 changes to clause 5 use cases to improve readability and understanding. The following changes are proposed:

- It is proposed to change the following in clause 5.1.1, second bullet: “to enable the exposure of” to “to access the”

. It is proposed to clarify that the point made is in relation to the “current SA5 work”

- Minor spelling corrections.

- Throughout eMNS has been replaced by eMnS as that is the correct nomenclature.

- It is proposed to change the following in clause 5.2.1, second bullet: “contract” to “offer” as to align with the generally known concept of product catalogue. Same for the third bullet, also it is clarified that the management function should be replaced with exposure governance management service as should be done in a service based management description.

- The first two bullets in clause 5.3.1 describe mostly the eMnS discovery service it is proposed to update second bullet and remove the third bullet as that makes the description unclear.

- The issues and gaps in 5.3.2 have been updated to improve readability and understanding

- The description in 5.4.1 has been updated to improve readability and understanding, an Editor’s note has been added for additional clarification.

- The description in 5.4.2 has been updated to improve readability and understanding, an Editor’s note has been added for additional clarification.

# 4 Detailed proposal

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

# 5 Use cases for network management capability exposure

## 5.1 Network slice management capability exposure

### 5.1.1 Description

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

1. MNO A selects the MnS that can be exposed to Externals (e.g. verticals) and publishes the related MnS data in certain MnS producer that the BSS can access.

2. In order to access the network slice related eMnS, a vertical A firstly makes a contract with the MNO A. The vertical A negotiates its specific requirements for the network slice management capability exposure with the MNO A. The negotiation can be done via the following ways:

a) For vertical A which is small enterprise, it can directly have a view on the network slice related management capability through the BSS (e.g. by using Product Catalog). Based on that, the vertical A can select the network slice related eMnSs which will be covered by the contract.

b) For vertical A which is large enterprise (i.e. Internet giants that have their own service customer), it can select the network slice related eMnSs that are available to be exposed offline (e.g. through a F2F meeting). The MNO A can proceed with the service ordering through BSS based on the contract.

3. The BSS may interact with the OSS in order to complete certain configuration (i.e. permission regarding what eMnS, optionally under what condition, can be exposed) regarding the exposure of eMnS based on the customized requirement from the eMnS consumer (e.g. vertical A).

4. The vertical A can get access to the network slice related management capability offered by eMnS producer within 3GPP management system. The access may need the interaction with BSS (e.g. through Service Catalog).

### 5.1.2 Issue and gaps

Gap:

An External needs to apply for the access of network slice management capability through BSS. However, there is no discussion and agreement (in current SA5 work) on whether an eMnS is exposed transparently through the BSS or being processed through a dedicated exposure platform before exposing to the external.

The definition and the format of permission for the exposure of network slice related eMnS and its potential impact on internal interface with BSS is not discussed in current SA5 work.

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

## 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 eMnS 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 to be accessed from both the local hosting network and PLMN. Service provider A and the provider of PLMN (i.e. associate to eMnS 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 accessing certain management MnS related to QoS. According to the contract, the service provider A can have the permission to use the MnS for accessing 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.

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 to get access to the local hosting network for improving the QoS of the high-resolution video application.

### 5.2.2 Issue and gaps

Gap:

The definition and the format of the permission rule 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 externals to a suitable MnS service producer for the exposure of performance MnS regarding NR and 5GC is not specified in existing 3GPP management system.

## 5.3 eMnS discovery service

### 5.3.1 Description

A use case of eMnS discovery service is described as follows:

1. MNO A provides eMnSs from 3GPP management system for external customers and these eMnSs go through the BSS for exposure.

2. In order to provide such discovery service to external customer, MNO A wishes to use an eMnS discovery service producer that takes responsibility for making eMnS data available for it to be discovered by the BSS.

3..

### 5.3.2 Issue and gaps

#### Gap:

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

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

## 5.4 eMnS support to discovery systems

### 5.4.1 Description

An eMnS should be allowed to register to 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 eMnS is only exposed to a discovery system where a pre-existing contract allows for such an exposure.

1. An operator would like to register its eMnS to a trusted discovery system. The operator configures the eMnS with the discovery system’s address and the appropriate level of exposure for the registration. The eMnS is registered at the discovery system with the appropriate level of exposure.

2. The operator performs changes in its management system that impacts the information exposed by the eMnS. The changed information is automatically updated in the discovery system.

3. In case the relationship between the operator and a discovery system ends, which implies the system is no longer trusted, then the eMnS automatically deletes its registration in the discovery system.

Editor’s Note: How the “is no longer trusted” would be handled by the authentication and authorization and system is FFS, since it is not clear how a non-trust party can be trusted to delete a registration entry.

### 5.4.2 Issue and gaps

There are several issues that need to be resolved.

Issues:

There is a difference if the discovery system is external or internal to the operator. A discovery system for internal use may still exist outside the scope of management.

There is an issue with managing which consumers have access to the discovery system and could theoretically consume the management service.

Editor’s Note: There is an issue with the trust (i.e., authentication and authorization) between the three parties (MnS producer/operator, MnS consumer/customer and discovery system owner) in this use case

Gap:

To limit issues the exposure from a discovery system of the operator may only provide “read” permissions (w.r.t the eMnS) without authentication and authorization. To execute the discovered eMnS 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.

## 5.5 Exposure of network slice as a product

### 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 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 5.5.1.1-1: 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 3GPP 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.

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

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

- Company-V 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 5.5.1.2-1: 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 3GPP 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.

#### 5.5.1.3 Exposure of the network slice as a product

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.

In these two sub-use cases, there is no exposure of service or network resources directly to the NSC.

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