**3GPP TSG-SA5 Meeting #143-eS5-223230**

**e-meeting, 09 - 17 May 2022**

**Source: Ericsson**

**Title: Make descriptions in issues and gaps more uniform**

**Document for: Approval**

**Agenda Item: 6.5.22.1**

# 1 Decision/action requested

***The group is asked to agree the detailed propsal.***

# 2 References

[1] 3GPP [TS 28.](https://www.3gpp.org/DynaReport/28533.htm)824 Study on network slice capability exposure

[2]

# 3 Rationale

The use case analysis in clause 5 follows the pattern of a the clause having a “Use case title” and contains a subclause for “Description” and a subclause for “Issues and gaps“. However the text described in issues and gaps is not consistent. Some examples of this inconsistency are: a gap has been identified without an issue or the subclause content is not consistent with the subclause title. Furthermore the issues and gaps are not definitive (it is a study) which the title may suggest, it is proposed to use potential issues and gaps instead.

Therefore this contribution propose to update all use cases clauses to follow the template:

5.x <use case title>

5.x.1 Description

5.x.2 Potential issues and gaps

5.x.2.1 Issues

5.x.2.2 Gaps

In some cases the text is rephrased to clearly identify the issue(s) and/or gap(s).

# 4 Detailed proposal

***1st 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. NSP selects the MnS that can be exposed externally.

2. NSP decides on any constraints 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.

3. NSP implements and deploys a Management Function which consumes the MnS, applies any constraints, and exposes the resulting functionality as an exposed MnS.

4. NSP may publish the exposed MnS in a service catalog or service directory.

### 5.1.2 Potential issues and gaps

#### 5.1.2.1 Issues

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

If exposed through BSS, the BSS decides which MnS it needs to expose BSS type of services. If BSS exposes a service to an external party that requires for example information from an MnS (fault supervision or performance assurance information) the BSS consumes these from OSS before exposing to the external customer. The external customer may see information that is derived from Mns and contextualized to service provided from BSS to external customer

#### 5.1.2.2 Gaps:

The BSS is in the same trust domain as OSS and the BSS does not expose MnS(s). No gap has been identified.

exposed MnSexposed MnS

## 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 platfrom 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

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 for exposure.

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

### 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 or by a dedicated exposed MnS discovery service producer (e.g. EGMF).

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

#### 5.3.2.2 Gaps

The BSS is in the operator’s trusted domain, the discovery of external parties (outside the trusted domain) is within the scope of BSS. No gaps in SA5 specifications have been identified.

## exposed MnSexposed MnSexposed MnS5.4 Exposed MnS support to discovery systems

### 5.4.1 Description

An exposed MnS 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 exposed MnS 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 exposed MnS to a trusted discovery system. The operator configures the exposed MnS with the discovery system’s address and the appropriate level of exposure for the registration. The exposed MnS 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 exposed MnS. 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 exposed MnS automatically requests deletion of 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 Potential issues and gaps

#### 5.4.2.1 Issues

There is a difference 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 in this use case.

#### 5.4.2.2 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

## 5.5 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.

#### 5.5.2 Potential issues and gaps5.5.2.1 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.

#### 5.5.2.2 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

## 5.6 Exposure of network slice as a service

### 5.6.1 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).

#### 5.6.1.1 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: 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 5.6.1.1-1 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 sents 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.

#### 5.6.1.2 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.

NOTE 2: If the external customer can get access to the OSS directly, it must maintain a copy of a part of the operator’s MIB. If the customer wants to e.g. receive alarms or performance measurements or KPIs related to the network slice the customer has ordered to the NSP, these alarms / perf. meas / KPIs need to relate to some MOIs known at customer side. All these MOIs shall be part of a containment tree in the copy of the Operators’ MIB maintained by the customer.



Figure 5.6.1.2-1 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.

### 5.6.2 Potential issues and gaps

#### 5.6.2.1 Issues

Editor’s Note: the issues if any are FFS

#### 5.6.2.2 Gaps

Editor’s Note: the gaps if any are FFS

## 5.7 Network slice management capability consumption

### 5.7.1 Description

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

1. In order to enable the consumption of network slice related exposed MnS, a 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. The negotiation can be done via the following ways:

a) For NSC 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 NSC can select the network slice related exposed MnSs which will be covered by the contract.

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

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. NSP authorizes NSC to consume the exposed MnS as defined in the contract, and provides the relevant authentication keys to NSC.

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

### 5.7.2 Potential issues and gaps

#### 5.7.2.1 Issues

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.

#### 5.7.2.2 Gaps

exposed MnSThe discussion of service exposed by BSS is outside scope of SA5. The discussion referred to could be held in other fora e.g. TM Forum. No gaps in SA5 specifications have been identified

exposed MnS

***End of Changes***