**3GPP TSG-SA5 Meeting #141-eS5-221216**

**e-meeting, 17 - 26 January 2022**

**Source: Huawei**

**Title: pCR 28.824 Clarification on access to exposed MnS**

**Document for: Approval**

**Agenda Item: 6.5.2**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.4.0 Study on network slice management capability exposure

# 3 Rationale

TR 28.824 [1] contains multiple ambiguous cases where the term “access” is used. In cases where access control is not the intended meaning, other terms are proposed instead.

# 4 Detailed proposal

This contribution proposes to make the following changes in [1].

|  |
| --- |
| **1st change** |

#### 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 indrectly consume management capability offered by MnS producer within 3GPP management system. Even though the eMnS complies with the same Technical Specification as a MnS, the actual operational behavior and managed data may be constrained by the network slice provider.

|  |
| --- |
| **2nd change** |

##### 4.1.1.3.2 Exposure scenarios

Scenario 1: Consumption of exposed MnS by applications

Editor’s note: This scenario doesn’t fit in the level of details of this section. Where to incorporate this section is FFS.

The operator has other non-management entities such as the middleware or application servers (AS) defined by 3GPP SA6 that could consume management services as shown in Figure 4.1.1.3.2-1. In such a case 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 consumed 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 4.1.1.3.2-1 Exposure to application server within and outside operator network

|  |
| --- |
| **3rd change** |

#### 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 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 consumed 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.

|  |
| --- |
| **4th change** |

### 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 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 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.

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.

|  |
| --- |
| **5th change** |

#### 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.

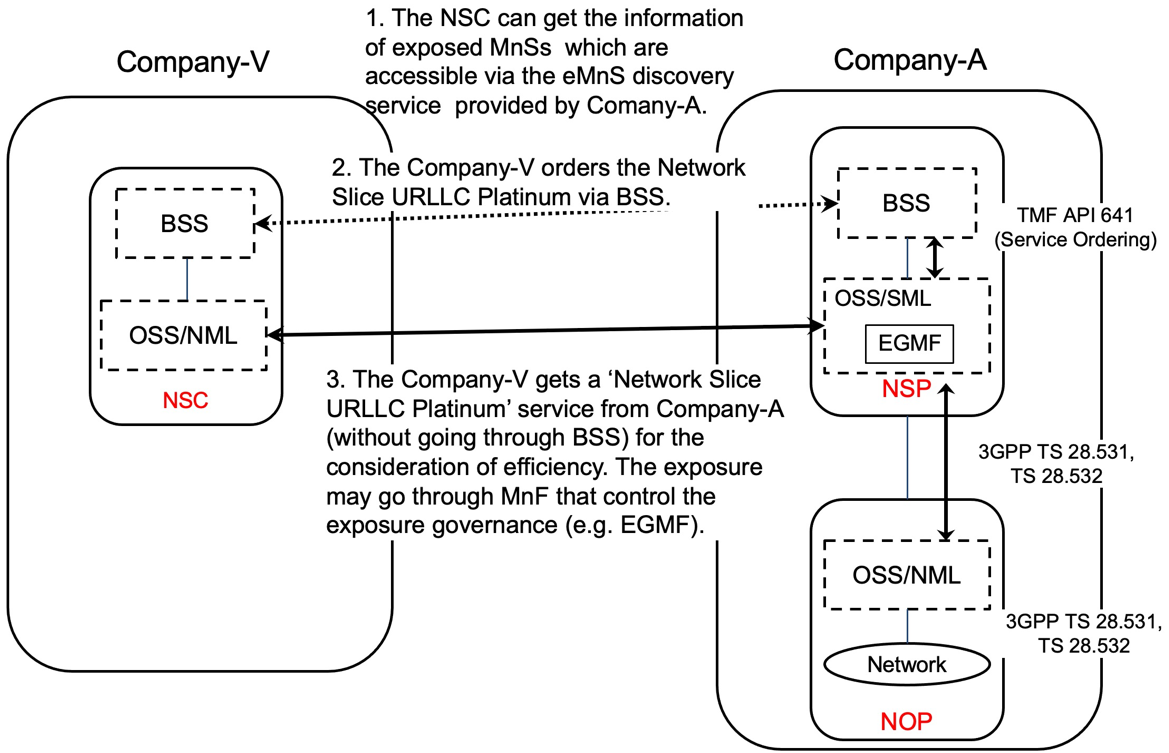


Figure 5.6.1.1-1 Sub-use case – NSP and NOP played by the same organization

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 eMnSs that are available via the eMnS 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.

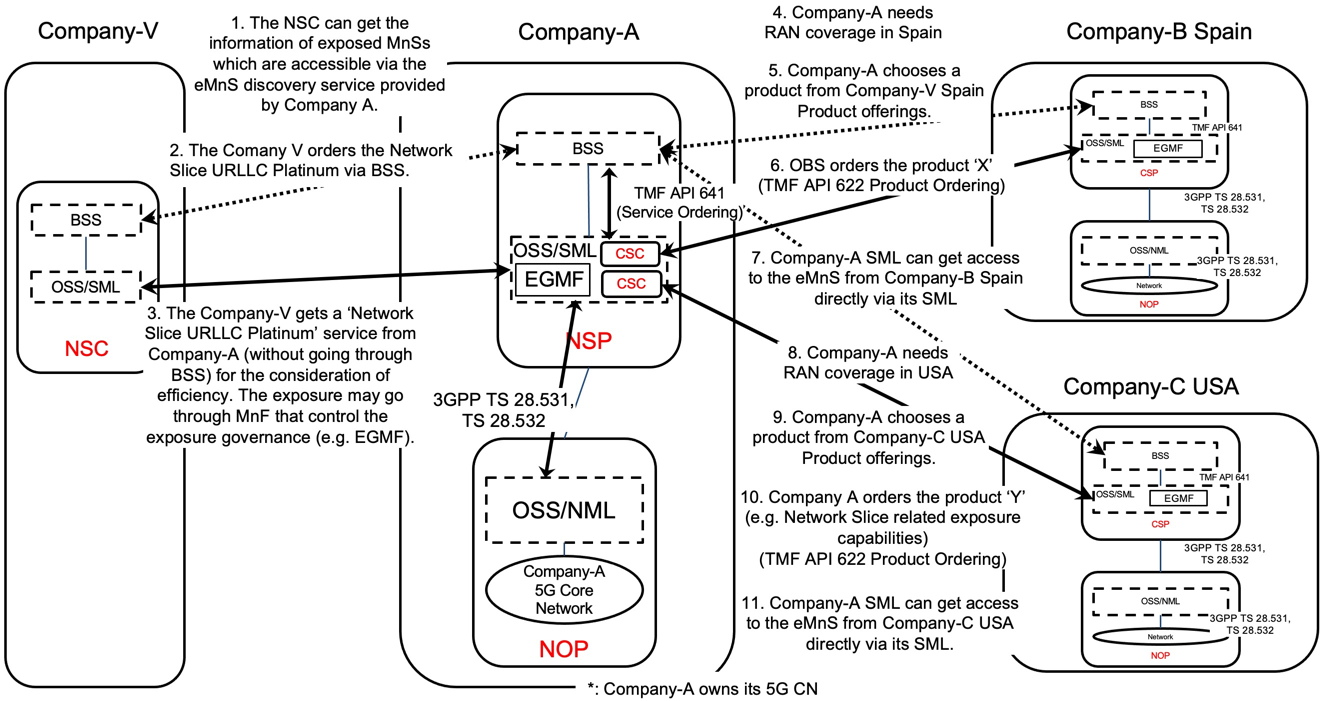


Figure 5.6.1.2-1 Sub-use case – NOP role played simultaneously by different organizations

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 eMnSs that are available via the eMnS 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 eMnS 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 eMnS 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.

## 5.7 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 eMnS, a NSC firstly makes a contract with the NSP, which contains the agreement and conditions for consuming an eMnS. The condition can be a certain constraint of eMnS consumption based on the contract, e.g. the usage quota of certain eMnS, the usage frequency of certain eMnS, 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 eMnSs 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 eMnSs 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 eMnS, optionally under what condition, can be consumed) regarding the consumption of eMnS based on the customized requirement from the NSC.

3. NSP authorizes NSC to consume the eMnS 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 eMnS producer within 3GPP management system. The access may need the interaction with BSS (e.g. through Service Catalog).

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