**3GPP TSG-SA5 Meeting #145-eS5-225217rev3**

**e-meeting, 15 - 24 August 2022**

**Source: Alibaba group**

**Title: pCR 28.824 Update of solution 7.9**

**Document for: Approval**

**Agenda Item: 6.9.6.3**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.8.0 Study on network slice management capability exposure

# 3 Rationale

This contribution is to resolve the Editor’s note in solution 7.9.

Solution 7.9 was captured in TR 28.824 with the following Editor’s Note:

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

According the discussion paper S5-225215, the CAMARA covers the scope of abstraction. The abstraction covers 1) hide telco complexity making API easy to consume for customer with no telco expertise, 2) fulfil data privacy and regulatory requirement, 3) to facilitate application to network. The abstraction is mainly implemented by transformation function which resides between the external customer and the exposure gateway which take charge of the exposure goverance aspects. The network slice management capability exposure will not be affected by the transformation function because the transformed service will be treated by the exposure governance equally as the normal management service.

Therefore, it is suggested to declare that the transformation function is covered by CAMARA and does not affect the network slice management capability exposure.

Editor’s note: Whether it is necessary to extend CAPIF-5 for alternative 2 is FFS.

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

Editor’s note: API invoker ID is defined in CAPIF architecture. However, the format of API invoker ID is not studied yet. Since API invoker ID can be mapped into the MnS consumer ID in the context of exposure, the format of MnS consumer ID has to be studied.

CAPIF core function can authorize MnS consumer with certain permission (e.g. access token) using CAPIF-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 recoginize 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: Whether NSC can directly interact with MnS producer using service API for alternative 2 is FFS.

The group tends to agree that MnS can be directly accessed by NSC if strong exposure governance can be enforced. Therefore, it is suggested to remove the Editor’s note. This issue may be revisited if any pontential issue is identified for direct access of MnS.

# 4 Detailed proposal

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

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

## 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 network slice management capability exposure and authorization/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 7.9.2-1 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 to discover the MnS producer for NSC 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 for NSC 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 differentate each MnS consumer during the auditing is not specified. |

After the completion of authentication and authorization with the NSC, the CAPIF core function needs to help the NSC to discover the address of the MnS producer so that the NSC can request for MnS consumption. In order to provide the discovery service to the NSC, the MnS data that contains the address of the MnS producer needs to be pulished to the CAPIF core function. This request for the 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 NSC.

The mnsAddress of MnsInfo within CAPIF-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-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 recoginize 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-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 represents 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 NSC 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.

For CAPIF-2e, when checking the granular consumer’s authorizations, the MnS producer may be able to provide original MnS following exposure goverance 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. The exposure governance can be implemented by a dedicated MnS producer/MnF (e.g. EGMF) for exposure governance.

### 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.

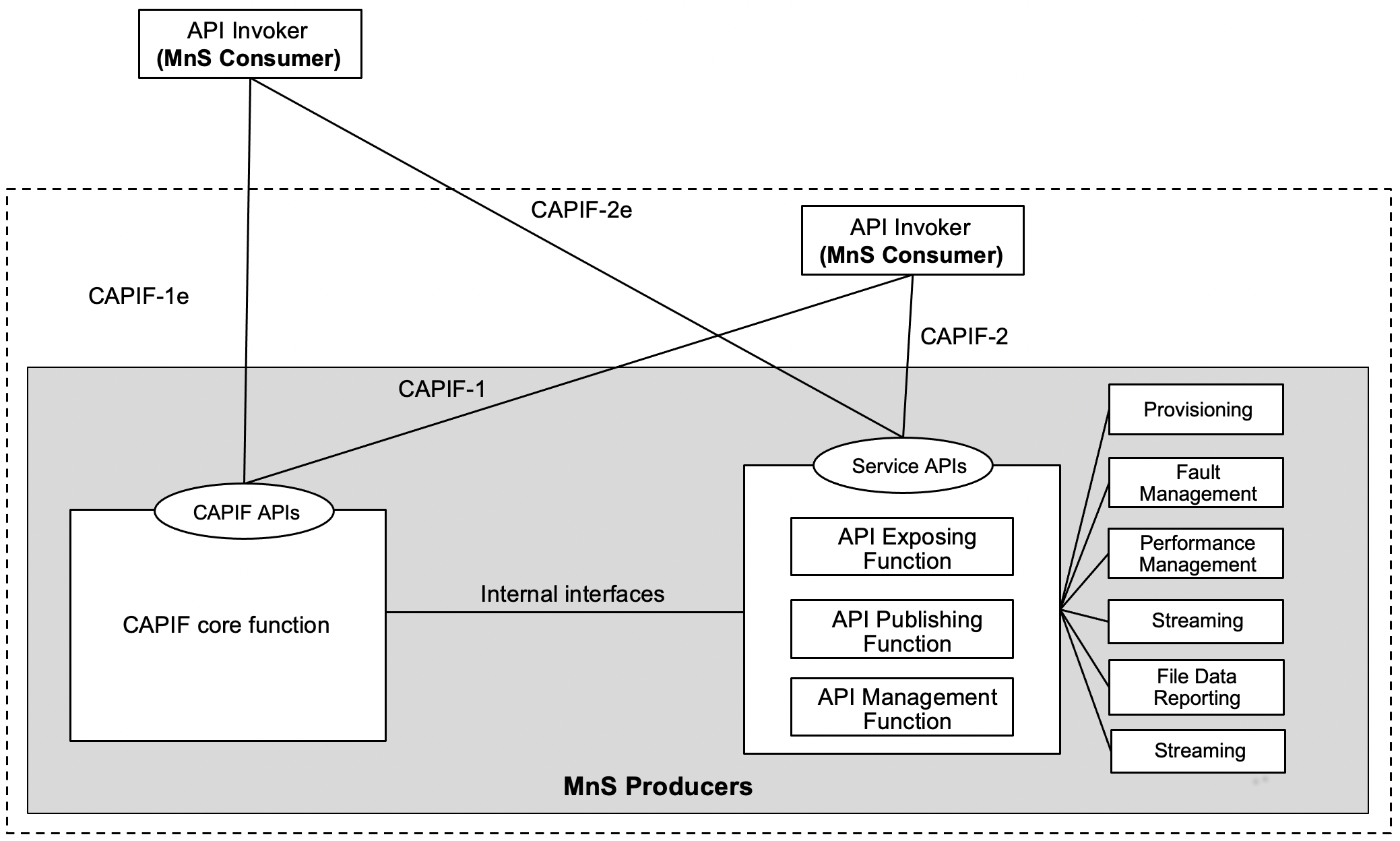


Figure 7.9.3-1: Exposure via CAPIF alternative 3

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.

Table7.9.3-1 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. Note that in CAPF alternative 3, 4, 5 in alternative 3 are internal interface. However, since external interface may bring impacts on the internal interface. The gap analysis for these interfaces is needed.

**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 to discover the MnS producer for NSC 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 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 for NSC using CAPIF 4 is not specified.  - The ServiceAPIDescription for CAPIF\_Publish\_Service\_API in CAPIF-4 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 |  |

After the completion of authentication and authorization with the NSC, the CAPIF core function needs to help the NSC to discover the address of the MnS producer so that the NSC can request for MnS consumption via the MnS producer. In order to provide the discovery service to the NSC, the MnS data that contains the address of the MnS producer needs to be pulished to the CAPIF core function. This request for the 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 NSC.

The mnsAddress of MnsInfo within CAPIF-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 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-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 recoginize 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-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 NSC 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.

For CAPIF-2e, when checking the granular consumer’s authorizations, the MnS producer may be able to provide original MnS following exposure goverance 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. The exposure governance can be implemented by a dedicated MnS producer/MnF (e.g. EGMF) for exposure governance.

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