**3GPP TSG-SA5 Meeting #145-e *S5-225164rev1***

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

**Source: Huawei**

**Title: Possible solutions for EGMF implementing CAPIF functional entities**

**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

[2] 3GPP TS 28.533 Management and orchestration; Architecture framework

# 3 Rationale

In TR 28.824 [1] clause 7.9, three exposure scenarios which are compliant with CAPIF are introduced. The problem is that the CAPIF function entities (e.g. CAPIF Core Function, API provider domain functions) are placeholders representing a set of functionalities related to common northbound API exposure framework. Therefore, this contribution will further fill the gap between the common CAPIF function entities with EGMF to fulfil CAPIF function entities implementation on management domain.

For CAPIF alternative 2, API provider domain functions are within the scope of MnS producers, yet it doesn’t specify which MnS producer will implement the functions defined in API provider domain. Therefore, this contribution proposes that EGMF will play the role as the service API provider function and fulfil all functionalities defined for API provider domain functions.

For CAPIF alternative 3, CAPIF core function and API provider domain functions are within the scope of MnS producers, yet it doesn’t specify which MnS producer will implement the functions defined in CAPIF core function and API provider domain functions. Therefore, this contribution proposes that EGMF will play the role as the combination of CAPIF core function and service API provider function to fulfil all functionalities defined for CAPIF core function and API provider domain functions.

# 4 Detailed proposal

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

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

### 7.x Possible solutions for EGMF implementing CAPIF functional entities7.x.1 EGMF implements the API provider domain functions

This clause describes how the API provider domain functions are implemented by EGMF and the corresponding EGMF functionalities compliant with clause 7.9.2 Exposure via CAPIF alternative 2.



Figure 7.x.1: EGMF implements the API provider domain functions

Figure 7.x.1 conforms to Figure 7.9.2-1: Exposure via CAPIF alternative 2 in clause 7.9.2. EGMF, as a dedicated MnS producer providing the exposed management services, implements API Exposing Function, API Publishing Function, API Management Function as specified in TS 23.222 [14].

To implement API Exposing Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.4 [14]

* Authenticate the API invoker based on the identity and other information required for authentication of the API invoker provided by the CAPIF core function.
* Validate the authorization provided by the CAPIF core function.
* Log the service API invocations at the CAPIF core function.
* Invocation of Service APIs. The exposed MnS can be provided to API invoker as service APIs as is.

To implement API Publishing Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.5 [14]

* Publish the service API information of the API provider to the CAPIF core function.

To implement API Management Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.6 [14]

- Audit the service API invocation logs received from the CAPIF core function.

- Monitor the events reported by the CAPIF core function.

- Configure the API provider policies to the CAPIF core function.

- Monitor the status of the service APIs.

- Onboard the new API invokers and offboard API invokers.

- Register and maintain registration information of the API provider domain functions on the CAPIF core function.

### 7.x.2 EGMF implements the CAPIF Core Function and API provider domain functions

This clause describes how the CAPIF Core Function and API provider domain functions are implemented by EGMF and the corresponding EGMF functionalities compliant with clause 7.9.3 Exposure via CAPIF alternative 3.



Figure 7.x.2: EGMF implements the CAPIF Core Function and API provider domain functions

Figure 7.x.2 conforms to Figure 7.9.3-1: Exposure via CAPIF alternative 3 in clause 7.9.3. EGMF, as a dedicated MnS producer providing the exposed management services, implements CAPIF Core function, API Exposing Function, API Publishing Function, API Management Function as specified in TS 23.222 [14].

To implement API Exposing Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.4 [14]

* Authenticate the API invoker based on the identity and other information required for authentication of the API invoker provided by the CAPIF core function.
* Validate the authorization provided by the CAPIF core function.
* Log the service API invocations at the CAPIF core function.
* Invocation of Service APIs. The exposed MnS can be provided to API invoker as service APIs as is.

To implement API Publishing Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.5 [14]

* Publish the service API information of the API provider to the CAPIF core function.

To implement API Management Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.6 [14]

- Audit the service API invocation logs received from the CAPIF core function.

- Monitor the events reported by the CAPIF core function.

- Configure the API provider policies to the CAPIF core function.

- Monitor the status of the service APIs.

- Onboard the new API invokers and offboard API invokers.

- Register and maintain registration information of the API provider domain functions on the CAPIF core function.

To implement CAPIF Core Function, EGMF should implement the following functionalities, see further details in TS 23.222 clause 6.3.3 [14]

- Authenticate the API invoker based on the identity and other information required for authentication of the API invoker.

- Support mutual authentication with the API invoker.

- Provide authorization for the API invoker prior to accessing the service API.

- Publish, storing and supporting the discovery of service APIs information.

- Control the service API access based on PLMN operator configured policies.

- Store the logs for the service API invocations and providing the service API invocation logs to authorized entities.

- Monitor the service API invocations;

- Onboard a new API invoker and offboard an API invoker;

- Store policy configurations related to CAPIF and service APIs;

- Support accessing the logs for auditing (e.g. detecting abuse); and

- Support publishing, discovery of service APIs information with another CAPIF core function in CAPIF interconnection.

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