**3GPP TSG-SA5 Meeting #148e *S5-233387rev1***

Electronic meeting, Online, 17 -25 April 2023

**Source: Huawei**

**Title: Add conclusion and recommendation for** **network slice management capability exposure via CAPIF**

**Document for: Approval**

**Agenda Item: 6.9.5.1**

# 1 Decision/action requested

***Approval***

# 2 References

[1] 3GPP TR 28.824: "Study on network slice management capability exposure"

[2] 3GPP TS 23.682: "Architecture enhancements to facilitate communications
with packet data networks and applications".

[3] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[4] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[5] S5-232893 SA5 way forward on capability exposure topic

# 3 Rationale

This contribution is proposed to make conclusion and recommendation for TR 28.824 [1] based on the endorsed document S5-232893 [5] clause 3.3 Acticity#1.

According to 3GPP TS 23.682 [2], when the CAPIF is supported, the SCEF supports the API provider domain functions. According to 3GPP TS 23.501 [3], when the CAPIF is supported,the NEF supports the API provider domain functions. Clause B.3.2 Deployment model of TS 23.222 [4] illustrates the integrated deployment of the 3GPP network exposure systems (SCEF and NEF) with the CAPIF.

***----------------- extract BEGIN from TS 23.222-h50 -----------------***

# B.3 Integrated deployment of 3GPP network exposure systems with the CAPIF

## B.3.1 General

According to 3GPP TS 23.682 [2], when the CAPIF is supported, the SCEF supports the API provider domain functions. According to 3GPP TS 23.501 [3], when the CAPIF is supported,the NEF supports the API provider domain functions.

## B.3.2 Deployment model

### B.3.2.1 General

The SCEF and the NEF may be integrated with a single CAPIF core function to offer their respective service APIs to the API invokers. The following deployment model is possible for integrated deployment of the SCEF and the NEF with the CAPIF core function.

### B.3.2.2 Integrated deployment of the SCEF and the NEF with the CAPIF

Figure B.3.2.2-1 illustrates integrated deployment of the SCEF and the NEF with the CAPIF.



Figure B.3.2.2-1: Integrated deployment of the SCEF and the NEF with the CAPIF

The CAPIF core function, the SCEF and the NEF are deployed in the PLMN trust domain, where the CAPIF core function takes the role of a unified gateway and provides services to different API invokers. The API invokers obtains the T8 and N33 service API information and the corresponding entry point details from the CAPIF core function via CAPIF-1 or CAPIF-1e reference points.

The API invokers can interact independently with the SCEF, the NEF and the 3rd party API exposing functions via CAPIF-2 or CAPIF-2e reference points. In this case, T8 and N33 can be reused to implement the service specific aspects of CAPIF-2 or CAPIF-2e reference points for the corresponding service API interactions of the SCEF and the NEF respectively.

The SCEF and the NEF applies any service API access policy control to the interactions between the API invokers and the T8 and N33 service APIs respectively by communicating with the same CAPIF core function via the CAPIF-3 reference point.

***----------------- extract END from TS 23.222-h50 -----------------***

To make CSPs have a single gateway to expose whatever capability (SCEF, NEF and MnS producer) they want, it is recommended that SA5 follow same deployment approach as SA2 SCEF and NEF with the CAPIF, i.e., the CAPIF core function, the SCEF, the NEF and the MnS producer are deployed in the PLMN trust domain, where the CAPIF core function takes the role of a unified gateway and provides services to different API invokers. The API invokers obtains the T8, N33 and MnS service API information and the corresponding entry point details from the CAPIF core function via CAPIF-1 or CAPIF-1e reference points. SA5 alternative 2 fits this deployment approach well.

# 4 Detailed proposal

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

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

## 8.X Network slice management capability exposure via CAPIF

### 8.X.1 Conclusion

Three alternatives for potential solutions (see clause 7.9.1, 7.9.2 and 7.9.3) for network slice management capability exposure via CAPIF have been evaluated in clause 7.9.4, which can help to draw the conclusion and recommendation for the solutions. Based on the evaluation, all analysed gaps can be resolved by alternative 2 and alternative 3 since all the related interfaces are within the scope of alternative 2 and alternative 3.

Meanwhile, alternative 2 and alternative 3 are also supported in solution for network slice management capability exposure depicted in clause 7.9.10.

Clause B.3.2 Deployment model of TS 23.222 [14] illustrates the integrated deployment of the 3GPP network exposure systems (SCEF and NEF) with the CAPIF. The SCEF and the NEF may be integrated with a single CAPIF core function, where the CAPIF core function takes the role of a unified gateway, to offer their respective service APIs to the API invokers.

To make CSPs have a single gateway to expose whatever capability they want, it is recommended that SA5 follow same deployment approach as SA2 SCEF and NEF with the CAPIF, i.e., the CAPIF core function, the SCEF, the NEF and the logical MnF providing management capability exposure governance (e.g. EGMF) are deployed in the PLMN trust domain, where the CAPIF core function takes the role of a unified gateway and provides services to different API invokers. The API invokers obtains the T8, N33 and MnS service API information and the corresponding entry point details from the CAPIF core function via CAPIF-1 or CAPIF-1e reference points. SA5 alternative 2 fits this deployment approach well.

Therefore, it is suggested to recommend alternative 2 as baseline for the normative work.

### 8.X.2 Recommendation

It is recommended that the alternative 2 depicted in clause 7.9.2 as baseline for the normative work, which includes:

- Specify normative requirements on management capability exposure;

- Define procedures enabling different external consumers to access management services via CAPIF.

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