**3GPP TSG-SA WG3 Meeting #117**  **draft\_S3-243638-r8**

**Maastricht, Netherlands, 19th – 23th Aug 2024 was merger of S3-243154, S3-243134, S3-243384**

**Source: China Telecom, Xiaomi, Nokia, Ericsson (?)**

**Title: New key issue about CAPIF interconnection**

**Spec:** **3GPP TR 33.700-22**

**Agenda item: 5.19**

**Document for: Approval**

**1. Introduction**

This contribution adds new key issue about CAPIF interconnection in TR 33.700-22.

**2. Reason for Change**

CAPIF interconnection architecture is under study as captured with a key issue in TR 23.700-22 [X] and that study requires coordination with SA3 as stated in the following note in clause 5.4.2 of TR 23.700-22 [X]:

NOTE: Coordination with SA3 is needed for security details.

This document proposes a key issue to be included in TR 33.700-22 [Z] for studying the security details of CAPIF interconnection.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TR 33.700-22.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[X] 3GPP TR 23.700-22: "Study on CAPIF Phase 3".

[Y] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[Z] 3GPP TR 33.700-22: "Study on security aspects of CAPIF Phase3".

\* \* \* Second Change \* \* \* \*

## 5.X Key issue #X: CAPIF interconnection security

### 5.X.1 Key issue details

TS 23.222 [Y] defines an architectural model for the CAPIF interconnection which allows API invokers of a CAPIF provider to utilize the service API(s) from the 3rd party CAPIF provider and other CAPIF core function within the same CAPIF provider. TS 23.222[Y] specifies some information, like service API information, shareable information, which is transferred between CAPIF core functions (CCFs) via CAPIF-6/6e. Besides, CCFs coordinate to authenticate and authorize service API access for the AEF service API(s) exposed via CAPIF-6/6e, which is studied in TR 23.700-22 [X]. Figure 5.X.1-1 and 5.X.1-2 shows the architectural models defined in TS 23.222 [Y] clause 6.2.2.



Figure 5.X.1-1: High level functional architecture for CAPIF interconnection with multiple CAPIF provider domains

Figure 5.X.1-1 describes the CAPIF interconnection framework that connects CCFs in two different CAPIF provider domains. For CAPIF interconnection architecture defined in Figure 5.X.1-1, the API provider domain function (AEF) of one domain only communicates with the CCF in CAPIF provider domain A (CCF-A), where it is registered. It does not communicate with the interconnected CCF in CAPIF provider domain (CCF-B), but still must be able to provide AEF service APIs to an API invoker onboarded at CCF-A. Therefore, one target of this key issue is to study how the API invoker onboarded to CCF-A is autheticated and authorized to access API services of the AEF registered to CCF-B.



Figure 5.X.1-2: High level functional architecture for CAPIF interconnection within a CAPIF provider domain

Figure 5.X.1-2 describes the CAPIF interconnection framework that connects CCFs in the same CAPIF provider domains. Another target of this key issue is study how one API invoker onboarded with CAPIF core function 1 (CCF-1) is authenticated and authorized to access AEF registered in CAPIF core function 2 (CCF-2).

### 5.X.2 Security threats

Without integrity protection for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be modified by attackers.

Without confidentiality protection for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be sniffed by attackers.

Without the anti-replay attacks mechanism for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be replayed by the attackers.

Without the API invoker authentication mechanism in CAPIF interconnection scenarios, a malicious API invoker can impersonate another victim API invoker to access service API(s) registered in the other CCFs.

Even if the API invoker is authorized by the CCF which it’s onboarded with, if there is no sufficient API service authorization and verification in CAPIF interconnection scenarios, this API invoker can still invoke AEF's service APIs registered in the other CCFs and get sensitive information (e.g., user's location information) without authorization.

Without the API invoker authorization revocation mechanism in CAPIF interconnection scenarios, the CAPIF system cannot revoke the authorization for API invoker accessing service API(s) registered in the other CCFs.

### 5.X.3 Potential security requirements

Potential security requirements for CAPIF interconnection are as followed:

1. The CAPIF shall support mutual authentication between API invoker and AEF when AEF service APIs are published via CAPIF-6/6e reference point in CAPIF interconnection scenarios.

2. The API invoker shall support retrieval of the security method needed for accessing service APIs when these AEF service APIs are published via CAPIF-6/6e reference point in CAPIF interconnection scenarios.

3. The CAPIF shall support authorization and revocation of the API invoker in CAPIF interconnection scenarios.

4. The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be integrity protected.

5. The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be protected from replay attacks.

6. The transport of messages over the CAPIF-6 and CAPIF-6e reference points shall be confidentiality protected.

7. The CAPIF shall support mechanisms for mutual authentication between CCFs over the CAPIF-6/6e reference point.

NOTE: Coordination with SA6 is needed.

\* \* \* End of Changes \* \* \* \*