**3GPP TSG-SA WG3 Meeting #117 draft\_S3-24xxx-r2**

**Maastricht, Netherlands, 19th – 23th Aug 2024**

**Source: China Telecom, Xiaomi, Nokia**

**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#1 about CAPIF interconnection in TR 33.700-22.

**2. Reason for Change**

This contribution provides the key issue needed to be considered in SA3.

**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 TS 23.222: " Common API Framework for 3GPP Northbound APIs".

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

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

## 5.X Key issue X: CAPIF interconnection

### 5.X.1 Key issue details

This key issue addresses the security aspects of 29.700-22 KI #4.

TS 23.222 [x] defines an architectural model for the CAPIF interconnection which allows API invokers of a CAPIF provider to utilize the service APIs from the 3rd party CAPIF provider and other CAPIF core function within the same CAPIF provider.

TS 23.222 [x] specifies some information, like service API information, shareable information, which is transferred between 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 CAPIF Phase 3 in TR 23.700-22 [Y].

Up to Rel-18, as shown in Figure 5.X.1-Z, CAPIF interconnection framework only describes CAPIF core functions (CCFs) interconnected in the same CAPIF provider domain.



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

As studied in CAPIF Phase 3, Figure 5.X.1-Y describes the CAPIF interconnection framwork that connects CAPIF core functions (CCFs) in two different CAPIF provider trust domains. The API provider domain function (AEF) of one domain only sees the CCF, where it is registered. It does not see the interconnected CCF in another domain, but still must be able to provide AEF service APIs to the API invoker onboarded at a CCF of another domain via CAPIF-2e.



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

This key issue is about AEF service API and API invoker being in two different CAPIF domains. An API invoker onboarded with CCF-1 needs to be authenticated and authorized to access AEF registered in CCF-2. The key issue addresses how the AEF of one domain authenticates and authorizes the API access from the API invoker of the other domain.

### 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 the attackers.

Without confidentiality protection for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be sniffed by the 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, AEF can only authenticate the API invoker in its own domain. A malicious API invoker accessing APIs across domains can impersonate another victim API invoker.

Even if the API invoker is authorized by the CCF in its own domain, if the API invoker is not authorized in CAPIF interconnection scenarios, this API invoker can still misbehave to request AEF's service APIs of another domain and get sensitive information (e.g., user's location information) without permission.

Without the API invoker authorization revocation mechanism in CAPIF interconnection scenarios, CCF can only revoke authorization information in its own domain, CAPIF system cannot withdraw the authorization for API invoker accessing APIs across domains.

### 5.X.3 Potential security requirements

Authenticating and authorizing service API access for the AEF service API(s) exposed via CAPIF-6/6e shall be supported.

The 5G system shall be able to revoke authorization related to the API invoker in CAPIF interconnection scenarios.

The API invoker in one domain shall be able to retrieve the security method needed for accessing AEF in another domain.

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

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

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

Mutual authentication between the CAPIF core functions shall be supported.

The CAPIF core function shall be able to authorize the other CAPIF core functions to publish and manage the service API information via CAPIF-6/6e.

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