**3GPP TSG-SA3 Meeting #117 draft\_S3-242xxx-r3**

Maastricht, Netherlands 19 - 23 August 2024

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

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

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***It is proposed to add the following key issue to the TR 33.700-22.***

# 2 References

[1] 3GPP TR 23.700-22: "Study on CAPIF Phase 3".

[2] 3GPP TR 33.700-22: "Study on security aspects of CAPIF Phase3".

# 3 Rationale

CAPIF interconnection architecture is under study as captured with a key issue in TR 23.700-22 [1] and that study requires coordination with SA3 as stated in the following note in clause 5.4.2 of TR 23.700-22:

*NOTE: Coordination with SA3 is needed for security details.*

This document proposes a key issue to be included in TR 33.700-22 [2] for studying the security details of CAPIF interconnection.

# 4 Detailed proposal

It is proposed to approve the following change to TR 33.700-22 [2].

\* \* \* 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

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 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 TR 23.700-22 [Y].



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

Figure 5.X.1-Y describes the CAPIF interconnection framwork that connects CAPIF core functions (CCFs) in two different CAPIF provider domains. For CAPIF interconnection architecture defined in Figure 5.X.1-Y, the API provider domain function (AEF) of one domain only communicates with the CCF (CCF-2), where it is registered. It does not communicate with the interconnected CCF (CCF-1) in another domain, but still must be able to provide AEF service APIs to an API invoker onboarded at CCF-1 via CAPIF-2e. Therefore, one target of this key issue is to study how the API invoker onboarded to CCF-1 is autheticated and authorized to access API services of the AEF registered to CCF-2.



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

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

In absence of a security protection of CAPIF-6/6e and CAPIF-2e for interconnection scenario, potential Man-in-the-Middle (MiM) or compromised end point risk results into inadvertent disclosure of information, unauthorized changes, and denial of service.

### 5.X.3 Potential security requirements

The transport of messages over the CAPIF-6/6e reference point should be integrity protected.

The transport of messages over the CAPIF-6/6e reference point should be protected from replay attacks.

The transport of messages over the CAPIF-6/6e reference point should be confidentiality protected.

CAPIF should provide mechanisms for mutual authentication and authorization between CCFs over the CAPIF-6/6e reference point.

CAPIF should provide for mutual authentication and authorization between API invoker and AEF over the CAPIF-2e reference point for the interconnection scenario.

NOTE: Coordination with SA6 is needed.

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