**3GPP TSG-SA3 Meeting #120 S3-250773**

**Athens, Greece, 17 - 21 February 2025**

**Source: Samsung**

**Title: Security procedures for nested API invocation**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122**

**Version: 18.4.0**

**Work Item: CAPIF\_Ph3\_sec**

**Comments**

This pCR proposes normative text for nested API invocation.

**Proposed Changes**

\* \* \* 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".

[2] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

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

[4] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[5] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[6] IETF RFC 7519: "JSON Web Token (JWT)".

[7] IETF RFC 7515: "JSON Web Signature (JWS)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] Void

[10] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[11] IETF RFC 7636: " Proof Key for Code Exchange by OAuth Public Clients".

[xx] IETF RFC 8693: "OAuth 2.0 Token Exchange".

\* \* \* Next Change \* \* \* \*

## 6.X Authorization procedure in a nested API invocation

The nested API invocation scenario is a scenario where an API invocation towards a first API exposing function (AEF-1) triggers that API exposing function to request an API invocation towards a second API exposing function (AEF-2), which is in the same API provider domain as the first API exposing function. The authorization of API invocation triggered towards second API exposing function shall use token exchange procedure as specified in IETF RFC 8693 [xx], where AEF-1 assumes the role of actor and the access token of the API invoker to be used towards AEF-1 is used as the subject token as per the IETF RFC 8693 [xx]. AEF-1 before triggering API invocation towards AEF-2, invokes the token exchange request towards the CCF by sending the subject token to receive a delegated security token. AEF-1 uses the received delegated security token towards AEF-2 for nested API invocation. This is depicted in figure 6.X-1.



Figure 6.27.2-1: Authorization for nested API invocation

1. CAPIF-1e authentication and secure session is established as specified in subclause 6.3.1 of the present document.
2. After successful establishment of TLS session over CAPIF-1e the API invoker shall request authorization information to invoke the service API exposed by API exposing function 1.
3. The CAPIF core function shall verify the Access Token Request message as per OAuth 2.0.
4. If the CAPIF core function successfully verifies the request message, the CAPIF core function shall generate an access token specific to the API invoker in an Access Token Response message.
5. The API invoker shall send a service API invocation request to API exposing function 1 with the authorization information received in step 4.
6. Based on the service API invocation request, API exposing function 1 verifies the access token and decides to invoke another service API exposed by API exposing function 2.
7. API exposing function 1, acting as an API invoker, obtains from the CCF the authorization information to access the service API exposed by API exposing function 2. The API exposing function 1 sends token exchange request message to CCF, to get the authorization information to invoke the service API in API exposing function 2. The request message includes information as shown in Table 6.10.2.2-1.

Table 6.27.2.2-1: Token exchange request message

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| Authorization information | M | The authorization information with resource owner consent obtained from API invoker in the service API request message. |
| Security information | M | Security information related to API exposing function 1 to validate the request from API exposing function 1. |
| Resource Owner (s) Information | M | Identifiers or other information related to the resource owners for which the authorization information with resource owner consent is needed. |
| Service API access | M | Information related to the service API, service API request parameters and the API exposing function 2, for which the delegated authorization is requested. |

The CCF validates the request from API exposing function 1. CCF validates whether the requesting API exposing function 1 is allowed for delegated authorization to access service API related to the resource owners on API exposing function 2. Also, the CCF validates the Authorization information in the request message that is provided by the API invoker to the API exposing function 1. After successful validation, the CCF responds to API exposing function 1 with token exchange response message that includes the delegated authorization information to allow API exposing function 1 to invoke the service API on API exposing function 2. The response message includes information as shown in Table 6.10.2.2-2.

Table 6.27.2.2-2: Token exchange response message

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| Delegated authorization information | M | The delegated authorization information with resource owner consent. |
| > Resource owner (s) information | M | Identifiers or other information related to the resource owners for which the authorization information is applicable |
| > Authorization information about primary subject | M | The authorization information with resource owner consent provided by API invoker in the request message. |
| > Delegated subject | M | Information related to entities for which the delegated authorization is applicable. In this case, the information related to API exposing function 1. |
| > Expiry time | M | Time for which the delegated authorization is valid. |
| > Allowed permissions | M | Information related to allowed service API access and the permissions or permitted service operations or permitted API resources on the service APIs. |
| > Allowed API Exposing Functions | M | The API exposing function (s) where the allowed permissions are applicable. In this case, the information related to API exposing function 2. |

1. API exposing function 1, shall send a service API invocation request to API exposing function 2 with the authorization information i.e., security token received in step 7.
2. The API exposing function 1 receives the service API invocation response resulting from the service API invocation once API exposing function 2 has checked whether the API invoker is authorized to invoke that service API based on the authorization information.
3. The API invoker receives the service API invocation response resulting from the service API invocation.

\* \* \* End of Change \* \* \* \*