**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250086-r1**

**Online, Electronic meeting, 13 -16 January 2025**

**Source: Samsung**

**Title: Update to solution#27**

**Document for: Approval**

**Agenda item: 5.18**

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

**Version: 0.3.0**

**Work Item: FS\_CAPIF\_Ph3-sec**

**Comments**

Solution#27 in TR 33.700-22 is updated to include other authentication method(s) specified in TS 33.122 for API invoker-2 and AEF-2 to mutually authenticate. Currently, solution#27 only considers access token based authentication and authorization whereas it is not necessary that AEF-2 supports same method. Hence, it is required for the API invoker-2 and AEF-2 to negotiate the security method(s) and derive or get the required security materials accordingly to facilitate the authentication procedure.

Further, EN for usage of actor token is deleted. It is proposed that the standard token claims additionally includes the nested actor claims to express that delegation has occurred and to identify the acting party to whom authority has been delegated. In this case AEF-1 (API invoker-2) is the acting party.

Furthermore, evaluation is updated.

**Proposed Changes**

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

## 6.27 Solution #27: Authorization for nested API invocation

### 6.27.1 Introduction

This solution addresses the security requirements of key issue#4. For nested API invocation, if the negotiated authentication method with AEF-2 is access token based, then it is proposed to re-use the OAuth 2.0 protocol with the extension that enables the API invoker(s) (AEF-1) to request and obtain security tokens from authorization server and use it as delegated access token when the AEF-1 decides to invoke the service API provided by the AEF-2. This solution proposes the API invoker – 2 (AEF – 1) requesting the CCF a delegated security token to invoke service APIs provided by the AEF – 2. Further, if the negotiated authentication method is TLS-PKI or certificate based then security procedure as specified in TS 33.122 [4] for generating or retrieving security materials.

### 6.27.2 Solution details

The nested API invocation scenario is a scenario where an API invocation towards a first API exposing function triggers that API exposing function to request an API invocation towards a second API exposing function.



Figure 6.27.2-1: Authorization for nested API invocation

1. CAPIF-1e authentication and secure session establishment is performed.
2. After successful establishment of TLS session over CAPIF-1e the API invoker requests authorization information to invoke the service API exposed by API exposing function 1.
3. The CAPIF core function 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 generates an access token and security token specific to the API invoker in an Access Token Response message.
5. The API invoker sends 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. |

NOTE: Table 6.27.2.2-1 and Table 6.27.2.2-2 needs SA6 co-ordination.

1. API exposing function 1, sends 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.

10. The API invoker receives the service API invocation response resulting from the service API invocation.

#### 6.27.2.3 Access token claims

The standard claims would include client\_id of the API invoker – 2 (AEF – 1) acting as the actor. Further, the CAPIF OAuth 2.0 security token conveys the following actor claims for nested API invocation as specified in IETF RFC 8693 [5] additional to the token claims as specified in Annex C.2, TS 33.122 [4].

Table 6.27.2.3-1: Nested actor (act) claims

|  |  |
| --- | --- |
| Parameter | Description |
| client\_id | OPTIONAL. The identifier of the API Invoker-2 (AEF-1) making the API request. |
| iss | OPTIONAL. The issuer of the security token (in this case it is the CCF in the same or different trust domain) |

### 6.27.3 Evaluation

This solution addresses security requirements of key issue#4. If API invoker 2 and AEF-2 selects access token based method for authorization the below entities are impacted. Otherwise, it follows existing security procedure with no additional impacts implying that there will be no optimization case in nested API.

Impacts to entities:

- CCFs to provide delegated security token

- AEF-1 as an API invoker to contact CCF for delegated security token

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