**3GPP TSG-SA3 Meeting #122 S3-251974**

**Fukuoka, Japan, 19 – 23 May 2025**

**Source: Huawei, HiSilicon, Nokia (1974) (+Nokia 2248), Ericsson (2213), Lenovo (2232)**

**Title: Pseudo-CR on updating text for finer level authorization**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122/ Living CR S3-251721**

**Version: 19.0.0**

**Work Item: CAPIF\_Ph3\_Sec**

**Comments**

This pCR is to provide revisions to the finer level authorization procedures.

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

## 6.Y Authorization for finer level service API access

[Additions by Huawei, Nokia and Lenovo]

The authorization function shall support finer level authorization as specified in TS 23.222 [3]. In both RNAA and non-RNAA scenarios, finer level service API access authorization can be used to limit access to specific API services resources and service API operations.

To enable finer level service API access, the authorization request or access token request includes the requested service resources and service operations at the respective granularity. In case of authorization request from API invoker to the CCF, it includes optionally application identifier as in TS 23.222 [3]. For RNAA, the request may also include the resource owner ID.

If the request includes desired Network Slice Info of the service API, the authorization request or access token request shall include related details.

If the API invoker is authorized, the CCF responds to the API invoker with an access token including finer level authorization information, or an authorization code.

[Alternative? Ericsson proposal]

The token request and token profiles are specified in Annex C for finer level service API access.

[Alternative? Huawei, Nokia proposal]

The following procedures are adapted to support finer level authorization:

Clause 6.5.3.2on Authorization using oauth client credential flow:

- The access token request message may also include details on finer level authorization.

Clause 6.5.3.3 on Authorization using authorization code (optional PKCE) flow:

- The authorization token and/or authorization request may also include finer level authorization information.

- The CCF shall also check the finer level authorization if included in the request.

Clause 6.5.3.4 on Revocation:

The additional information in the Authorization Revocation Request message may also include information for finer level authorization.

Clause C.2.2 on Token claims:

The "Values" of the parameter "scope" in the Table C.2.2-1 is changed to

OPTIONAL. A string containing a space-delimited list of AEF ID(s), service API name(s), service operation(s), API resource(s).

Clause C.3.2 on Access token request

The "Values" of the parameter "scope" in the Table C.3.2-1 is changed to

OPTIONAL. A string containing a space-delimited list of AEF ID(s), service API name(s), service operation(s), API resource(s).

[additional Ericsson proposals]\*\*\* 2nd Change \*\*\*

#### 6.5.3.2 Authorization using oauth client credential flow

If client credential flow is used for authorization of the API invoker by the AEF, the procedures in RFC 6749 [4] shall be followed with the following profile:

- The access token request message may include the resource owner ID.

- The access token request message may include purpose of the data processing.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

NOTE 2: The mapping of API Invoker ID and GPSI is left for stage 3.

- The CCF shall check whether the API invoker is entitled to consume the API and allowed to access the resources of the resource owner, by using authorization information available in the CCF.

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. If the API invoker is an AF not on a UE, the check is omitted.

NOTE 2: How to get the authorization from the resource owner and store it in the CCF is out of scope of the present document.

\*\*\* 3rd Change \*\*\*

#### 6.5.3.3 Authorization using authorization code (optional PKCE) flow

If authorization code flow, optionally with PKCE, is used by the AEF for authorization of the API invoker, the procedures in RFC 6749 [4] and optionally RFC 7636 [11] shall be followed, with the following profile:

- The authorization token and/or authorization request may include the resource owner ID.

- The authorization request may include purpose of the data processing.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

NOTE 2: The mapping of API Invoker ID and GPSI is left for stage 3.

- The resource owner dynamically authorizes the API invoker to access the resource owner's resources as described in RFC 6749 [4] and optionally RFC 7636 [11].

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. The access token shall contain the resource owner ID (i.e. GPSI) and the API invoker ID. If the API invoker is an AF not on a UE, the check is omitted.

\*\*\* 4th Change \*\*\*

## C.2.2 Token claims

The CAPIF ‘Method–3 - TLS with OAuth token’ access token or an access token used in RNAA shall convey the following claims as defined in IETF RFC 7519 [6] and IETF RFC 6749 [4].

Table C.2.2-1: Access token standard claims

|  |  |
| --- | --- |
| Parameter | Description |
| exp | REQUIRED. The expiration time of the access token. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew (not to exceed 30 seconds). |
| client\_id | REQUIRED. The identifier of the API Invoker making the API request as previously established with the CAPIF Core Function through onboarding. |
| scope | REQUIRED. A string containing a space-delimited list of AEF ID(s), service API name(s), service operation(s), API resource(s). |

NOTE: Feature level access is left to stage 3 to decide.

The CAPIF OAuth 2.0 access token shall additionally convey the following claim for RNAA.

Table C.2.2-1: Access token customized claims

|  |  |
| --- | --- |
| Parameter | Description |
| resOwnerId  | OPTIONAL. Resource owner ID. |

The ‘exp’and ‘scope’ parameters of the access token shall be determined by the CAPIF core function based upon the client\_id of the API Invoker provided in the Access Token Request message.

The scope parameter ‘List of Services per AEF’ shall contain a full or partial list of services which the API Invoker is permitted to access at each AEF.

\*\*\* 5th Change \*\*\*

## C.3.2 Access token request

To obtain an access token, the API Invoker makes a request to the CAPIF Core Function by sending an Access Token Request message with the following parameters using the "application/x-www-form-urlencoded" format, with a character encoding of UTF-8 in the HTTP request entity-body. The access token request parameters are shown in table C.3.2-1.

Table C.3.2-1: Access token request message parameters

|  |  |
| --- | --- |
| Parameter | Values |
| grant\_type | REQUIRED. The value shall be set to "client\_credentials or “authorization\_code”". |
| client\_id | REQUIRED. The identifier of the API Invoker making the request. It shall match the value that was assigned to the API Invoker during the onboarding process. |
| client\_cred | OPTIONAL. The client credential that was provided to the API Invoker during the onboarding process. |
| Redirect\_uri | OPTIONAL. The value shall be identical with the value in authorization request once authorization code grant or PKCE is used. |
| code | OPTIONAL. The authorization code received from the CCF for RNAA once authorization code grant or PKCE is used. |
| code\_verifier | OPTIONAL. If the authorization code grant with PKCE flow is selected, the code verifier is used by the CCF to check the code\_challenge according to IETF RFC 7636 [11] once PKCE is used. |
| scope | OPTIONAL. A string containing a space-delimited list of AEF ID(s), service API name(s), service operation(s), API resource(s). |

NOTE: Feature level access is left to stage 3 to decide.

If the token is used for RNAA (see clause 6.5.3), the parameter resOwnerID is used for the resource owner ID.

|  |  |
| --- | --- |
| resOwnerID | OPTIONAL. Resource owner ID |

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