**3GPP TSG-SA3 Meeting #122 S3-251972-r1**

**Fukuoka, Japan, 19 – 23 May 2025 merging of 1888, 1933, 1972, 2216, 2077, 2250**

**Source: Huawei, HiSilicon, Nokia**

**Title: Pseudo-CR on updating RO authorization to address EN**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122/ Living CR S3-251722**

**Version: 19.0.0**

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

**Comments**

This pCR is to address the following EN in the living CR:

Editor Notes – whether authorization request is transfered via CAPIF-8 and what additional information carried via CAPIF-8 are ffs.

Based on the RFC 6749 (clause 4.1), authorization request in the authorization code grant flow is initiated by the client (API invoker) and sent to the authorization server (CCF) via the user agent (ROF). This is to obtain code grant before the API invoker can send to the CCF for access tokens. The authorization request contains client\_id and may contain scope and other parameters as specified in clause 4.1.1. In response after authorization and authorization procedure, the CCF issues Authorization Code in the authorization response message to the client through the ROF.

The CAPIF-8 is the interface between the ROF and CCF and should be the interface to carry above messages.

This is clarified and convert the EN to a NOTE.

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

### 6.5.3 Authentication and authorization for RNAA

#### 6.5.3.1 General

The authorization function shall obtain the necessary permission from the resource owner for allowing the API invoker to access a northbound API.

RNAA shall use token-based authorization using OAuth 2.0 framework with the following roles:

- The API invoker has the role of the OAuth 2.0 client.

- The CCF has the role of the OAuth 2.0 authorization server, i.e., providing the access token used for RNAA.

- The AEF has the role of the resource server.

The access tokens used for RNAA shall contain the resource owner ID.

The resource owner may be the user of the UE or the owner of the subscription depending on the use case and regulations. The resource owner ID is specified as the GPSI of the corresponding UE if the resource is related to a UE.

NOTE: The present document does not specify the resource owner.

The access token shall include the resource owner ID and the API invoker ID. The resource owner ID is the GPSI. The API invoker ID binds the token to the API invoker. To avoid privacy issues, GPSI should be different from MSISDN, SUPI etc.

Authorization information/authorization revocation information is transferred between the ROF and the CCF via the secure CAPIF-8 reference point.

The resource owner is authenticated before being allowed to manage the resource owner authorization information.

NOTE: How to authenticate the resource owner is left to implementation.

The authorization information contains the API invoker information (where the API invoker may be either an application on a server or an application on a UE as specified in TS 23.222), and service information. The request may also include other information as specified in TS 23.222.

~~NOTE: authorization request and authorization response messages are transferred via CAPIF-8.~~

The AEF shall check if the token includes *resOwnerId* claim, which includes resource owner ID, to identify that it is a token used in RNAA.

AEF shall do the authorization check of the API invocation request for accessing the resources of the resource owner. AEF checks the request against the token, including:

1) checking the token integrity and

2) checking whether the GPSI (if present) in the API invocation request is compliant with the resource owner ID in the access token. As the token includes resource owner ID, there is no need for additional UE authentication in API invocation. Moreover, the token should be able to restrict the API invoker to a specific resource (e.g., location, QoS, PDN connectivity status) of the resource owner.

For OAuth 2.0 flows involving redirection, authentication between CCF/AUF and UE should be performed after API Invoker redirects the UE to CCF/AUF.

In case of an external AF (i.e., not the application on the UE) being the API invoker, for mutual authentication of API invoker AF and API exposing function, the authentication methods of clause 6.4 and clause 6.5.2 are reused.

For authorization, the following OAuth 2.0 flows may be used:

- Client credential flow (according to RFC 6749 [4]),

- Authorization code flow (according to RFC 6749 [4]), or

- Authorization code flow with PKCE (according to RFC 7636 [11]).

CCF shall indicate the selected flows to the API invoker.

CCF shall give service authorization which subscribers or users can use RNAA.

For selecting the authorization method, the procedure as specified in clause 6.3.1.2 is used with the following RNAA specific additions. The API invoker shall include in the Security Method Request the supported RNAA authorization flows. The CCF shall determine the RNAA authorization flow based on the RNAA capabilities of the CCF, AEF, and API invoker. The API invoker shall use the determined RNAA authorization flow in the subsequent communication with the CCF and AEF.

NOTE: In the present document, only a UE accessing its own resources is considered if the API invoker is on a UE.

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

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Resource owner authorization:** The permission provided by the resource owner to allow the API invoker to access the resource owner’s resource via the northbound API.

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

#### 6.5.3.B Resource owner authorization management

Editor’s Note: This clause will be updated to capture the security procedures for resource owner authorization management

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