**3GPP TSG-SA3 Meeting #122 S3-251959-r1**

**Merger of S3-251931, S3-251945, S3-251973, S3-252040,**

**S3-252076, S3-252218, S3-252233, S3-252252**

**Fukuoka, JP, 19 - 23 May 2025**

**Source: Chinatelecom**

**Title: Baseline pCR against Draft CR for KI#1.2 on revocation**

**Document for: Approval**

**Agenda item: 4.22**

**Spec: 3GPP TS 33.122**

**Version: v19.0.0**

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

# 1 Decision/action requested

***It is proposed to approve the pCR to address the EN and make a correction.***

# 2 References

[1] 3GPP TR 33.700-22: "Study on security aspects of CAPIF Phase3".

# 3 Rationale

The contribution proposes to address the left ENs and make a correction on approved living CR S3-251800.

1) Editor’s Note: Whether any additional the resource owner- related information is needed in resource owner authorization revocation information is ffs.

In Annex C.2.2 of TS 33.122, access token claims include parameter resOwnerId (i.e., Resource Owner ID) for RNAA. Because the Resource Owner ID in resource owner authorization revocation request message is enough to identify the RNAA-related revoked token, there is no need for additional resource owner-related information. Propose to remove the resource owner-related information.

2) Editor’s Note: Whether purpose of data processing is needed is FFS.

Based on current work of TS 33.122, purpose of data processing is not a parameter of RNAA-related token. Thus, purpose of data processing is no needed.

3) Editor’s Note: clarification on additional information used for AEF to identify the RNAA-related token is ffs.

The term ‘additional information’ is not clear, e.g., information of token, the token itself, the token id. Considering minimum impact on current procedure, propose to change ‘additional information’ to ‘detail information identified in step 2’.

4) Editor’s Note: Whether the name of the message sent by CCF to AEF is Revoke API authorization Request or Revoke resource authorization notify is ffs.

The EN will be addressed after correction work of SA6.

5) Editor’s Note: Whether and how to update the resource due to token revocation is not in the scope of the present document.

The EN will be converted to NOTE.

Besides, there is a correction on approved living CR S3-251800:

*4. The AEF, storing the* ***resource owner authorization revocation information*** *about the RNAA-related revoked token, checks whether the token presented by an API invoker is revoked or not, before responding to the API invoker’s invocation request.*

The resource owner authorization revocation information is transferred from ROF to CCF in step 1. There are no steps to describe how AEF stores this information. This information is too high-level for AEF to identify the RNAA-related revoked token. Thus, propose to change ‘resource owner authorization revocation information’ to ‘detail information’, which is sent from CCF to AEF in step 3.

# 4 Detailed proposal

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

#### 6.5.3.4 Revocation

The CCF can initiate the Authorization Revocation Request message as defined in clause 8.23.4 of TS 23.222 [3] with additional information to identify the RNAA-related revoked token.

NOTE: The CCF can receive a revocation request message from the resource owner via the UE, resource owner function, web page etc.

AEF, storing the information about the RNAA-related revoked token, shall check whether the token presented by an API invoker is revoked or not, before responding to the API invoker’s invocation request.

The CCF provided notification message to the API invoker shall include the information to identify the RNAA-related revoked token.

The procedure illustrated in Figure 6.5.3.4-1 and explained below can be used for revoking RNAA-related token in RNAA scenarios.

Pre-conditions:

1. The API invoker is authenticated and authorized to use the service API.

API invoker

Resource owner function

CAPIF Core function

AEF

0. TLS session establishment.

1. Resource owner authorization revocation request

2. Identify the RNAA-related revoked token.

3. Revoke API invoker authorization request

4. Invalidate the authorization of API invoker for service API and resource

5-7: Same steps as the steps 4-6 in clause 8.23.4 of TS 23.222

8. Resource owner authorization revocation response

Figure 6.5.3.4-1: Procedure for revoking resource owner authorization

1. CCF and ROF shall establish TLS session over CAPIF-8 reference point as specified in clause 6.11.
2. Triggered by the resource owner, the resource owner function sends a resource owner authorization revocation request to the CCF. The resource owner authorization revocation information in the request message shall include 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 [3]), information related to service API (e.g., service operation information, service information). The request may include Resource Owner ID (e.g., GPSI), and resource information (Lenovo)and application identifier. . The request may include other information specified in TS 23.222 [x]. (Nokia) The purpose for revocation may be added.
3. The CCF determines the detail information of the resource owner ID, API invoker ID and the service API in the scope of the token based on the received resource owner authorization revocation information to identify the RNAA-related token to be revoked.

(Ericsson) The CCF uses the information in the resource owner authorization revocation request to identify the RNAA-related token to be revoked.

1. The CCF sends the Revoke resource authorization request message to the AEF as defined in clause 8.35 of TS 23.222 [3] with information in RNAA-related token (e.g., token itself, token id) to identify the RNAA-related revoked token.
2. The AEF, storing the information about the RNAA-related revoked token, checks whether the token presented by an API invoker is revoked or not, before responding to the API invoker’s invocation request.

(Chinatelecom, Nokia)NOTE: Whether and how to update the resource due to token revocation is not in the scope of the present document.

(Ericsson)NOTE: The need of updating the resource due to the token revocation and how to do it if resource update is needed are not in the scope of the present document.

(Lenovo) NOTE: The AEF does not allow any service for an API invoker when the access token is not valid (e.g., token is already revoked or expired etc.), so the related resource is not further impacted due to any invalid token based requests.

5-7. Step 5-7 are the same as in steps 4-6 in clause 8.23.4 of TS 23.222 [3].

8. The CCF sends a resource owner authorization revocation response as an acknowledgement to the ROF that the resource owner authorization has been revoked.

Revocation in RNAA interconnection scenarios will be merged in clause 6.x.3.4

(Lenovo) Alternatively, there is an AEF initiated revocation procedure i.e., according to TS 23.222 Clause 8.23, an AEF sends Revoke API Invoker authorization request to the CCF, in such as case the CCF after authorization revocation sends Revoke API invoker authorization notify to the API Invoker.

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