**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250022**

Online, Electronic meeting, 13 -16 January 2025

**Source: Huawei, HiSilicon**

**Title: removing EN in clause 6.4**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***Approve pCR proposal for TR 33.700-22***

# 2 References

[1] 3GPP TR 33.700-22

# 3 Rationale

There have been sufficient content in the evaluation clause, it is proposed to remove the following open ended EN for the Sol#4 [1].

Editor’s Note: further evaluation to be done is ffs.

# 4 Detailed proposal

pCR

\*\*\* START OF CHANGES \*\*\*

## 6.4 Solution #4: resource owner authorized revocation

### 6.4.1 Introduction

This solution addresses the "Key Issue #1.2: Resource owner authorization management ". The resource owner (RO) authorization is based on the RNAA procedure specified in TS 33.122 [4]. For the RO revocation, this solution extends the procedure in the

TS 33.122 [4], where it is stated

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

Specifically, in this solution, the revocation request message is described to complete the revocation procedure, given the CAPIF-8 reference point and relevant procedure is specified in the present document.

### 6.4.2 Solution details

#### 6.4.2.1 Authorization procedure

The procedure for authorization of resource owner follows the RNAA procedure as specified in clause 6.5.3 of TS 33.122 [2]. Specifically, the API invoker sends an access token request message to the CCF and the CCF issues the token with GPSI after checking specific to the authorization flow used. For example, the CCF may request RO authorization based on RFC 6794 if the authorization code flow is used.

#### 6.4.2.2 Revocation procedure

The procedure for revoking API invoker authorization initiated by the resource owner through the resource owner function (ROF) is given below extended from the procedure specified in clause 6.5.3.4 of TS 33.122 [4]:

1. The resource owner may trigger token revocation through the ROF. The ROF sends an authorization revocation request message to the CCF. The message shall include the service API ID, the GPSI, and other information related to the revoked token (e.g., the scope info).

NOTE: the GPSI is the identifier of the resource owner. It is stored at the ROF through configuration or the authorization procedure.

2. With reference to step 2 in clause 8.23.4 of TS 23.222 [3], the request message includes in addition the GPSI of the UE, on which the ROF resides.

3. With reference to step 3 in clause 8.23.4 of TS 23.222 [3], the AEF may additionally determine whether to update the resource due to revocation, e.g., the API invoker is using the resource (i.e., QoS) that should be revoked after token revocation for the QoS service API, the AEF may inform PCF/SMF to modify the QoS level of corresponding PDU sessions after revocation.

4. The same as the step 4 in clause 8.23.4 of TS 23.222 [3].

5. Similar to the step 5 in clause 8.23.4 of TS 23.222 [3], the difference is invalidated authorization here is API invoker authorization for the resource owner/UE corresponding to the GPSI.

6. Similar to the step 6 in clause 8.23.4 of TS 23.222 [3], the difference is that the message is sent to the ROF.



Figure 6.4.2-1: Revocation procedure for initiated through ROF

### 6.4.3 Evaluation

This solution addresses addresses the requirements of Key Issue #1.2.

This solution has two separate procedures for authorization and revocation.

This solution reuses the authorization procedure specified in clause 6.5.3 in the TS 33.122 [4] and extends the revocation procedure in clause 6.5.3.4 in TS 33.122 [4] to include steps related to CAPIF-8 interface. Therefore, no impact is introduced by the authorization procedure. As to the revocation procedure, the ROF will send a revocation request message to the CCF and receives the corresponding revocation response message. In addition, AEF may determine whether to update the resource due to revocation, if yes, the AEF may send a message to the PCF/SMF to modify the QoS level. The impact to the AEF in this aspect is that the AEF needs to store information of original resources in order to update related operations.

The revocation procedure is to prevent token being misused by an attacker. Although a short-lived token can potentially mitigate the issue, it has restrictions for its applicability or use cases. For example, setting token lifetime may be challenging in many scenarios. On the one hand, a large number of tokens or frequent token refreshing may be needed if the token lifetime is short, which constrains the system with complexity and overhead. On the other hand, if the token lifetime is short, the token may be misused or compromised.

A short-lived token can be an alternative solution. As comparison with the alternative solution, this solution can provide revocation immediately and avoid frequent refreshing of token.

\*\*\* END OF CHANGES \*\*\*