**3GPP TSG-SA3 Meeting #120 *draft S3-******xxxx-r2***

***Baseline 250510-r4***

**Athens, Greece 17 – 21 February 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **2** | **CR** | ***draft*** | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Resource owner authorization management for CAPIF\_Ph3\_Sec |
|  |  |
| ***Source to WG:*** | China Telecom, Huawei, Nokia, Lenovo, Xiaomi |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3\_Sec |  | ***Date:*** | 2025-2-10 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-19 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | This draft CR propose to define the Resource owner authorization management in TS 33.122 based on the conclusion of KI #1.2 in TR 33.700-22. |
|  |  |
| ***Summary of change:*** | Capture the security procedures for resource owner authorization management. |
|  |  |
| ***Consequences if not approved:*** | New CAPIF phase 3 features resource owner authorization will be unworkable.  |
|  |  |
| ***Clauses affected:*** | 6.5.3.4, 6.5.3.B (new clause) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

Start of Change

#### 6.5.3.4 Revocation

From CTC 0510

From Nokia 0479

From Huawei 0410

Figure 6.5.3.4-1 illustrates the procedure for revoking API invoker authorization initiated by resource owner in RNAA scenarios.

Pre-conditions:

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

2. The AEF in the CAPIF is configured with the access policy to be applied to the service API invocation corresponding to the API invoker and the service API.



Figure 6.5.3.4-1: Procedure for revoking API invoker authorization initiated by resource owner

1. Mutual authentication between the authorization server and the resource owner is completed.
2. The resource owner sends resource owner authorization revocation request to the CCF via the UE, resource owner function (e.g., web page etc). The resource owner authorization revocation information in request message includes the Resource Owner ID, the GPSI, service API information (e.g., service API ID) and API invoker ID / API invoker information.

NOTE: The GPSI is the identifier of the resource owner.

1. The CCF determine the details of the API invoker and the service API used to identify the RNAA-related revoked token based on the received resource owner authorization revocation information.
2. The CCF sends resource owner authorization revocation request message to the AEF as defined in clause 8.23.4 of TS 23.222 [3] with the resource owner authorization revocation information to identify the RNAA-related revoked token to perform the related revocation.
3. AEF, storing the resource owner authorization revocation information about the RNAA-related revoked token, shall invalidates the API invoker authorization corresponding to the RNAA-related revoked token. The AEF shall check whether the token presented by an API invoker is revoked or not, before responding to the API invoker’s invocation request.
4. The AEF sends a revoke API invoker authorization response to the CAPIF core function.
5. The CAPIF core function invalidates the API invoker authorization for the resource owner/UE corresponding to the service API and the GPSI.
6. The CCF provided notification message to the API invoker shall include the information to identify the RNAA-related revoked token.

End of Changes