**3GPP TSG-SA3 Meeting #121 S3-251718**

Goteborg, Sweden, 7 – 11 April 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.122** | **CR** | ***draft***  | **rev** | **-**  | **Current version:** | **19.0.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Living CR on Nested API |
|  |  |
| ***Source to WG:*** | Ericsson, Samsung, Xiaomi, Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CAPIF\_Ph3\_sec |  | ***Date:*** | 2025-04-14 |
|  |  |  |  |  |
| ***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 is proposed to specify authorization in nested API invocation. |
|  |  |
| ***Summary of change:*** | A new clause in TS 33.122 to be added to introduce authorization aspects for nested API invocation. |
|  |  |
| ***Consequences if not approved:*** | There will not be an authorization mechanism specific to nested API invocation case.  |
|  |  |
| ***Clauses affected:*** | 2, 6.X (new) |
|  |  |
|  | **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:*** | Adding content of S3-251717 approved in SA3#121. |

\* \* \* Start of the Changes \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[3] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[4] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[5] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[6] IETF RFC 7519: "JSON Web Token (JWT)".

[7] IETF RFC 7515: "JSON Web Signature (JWS)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] Void

[10] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[11] IETF RFC 7636: " Proof Key for Code Exchange by OAuth Public Clients".

[xx] IETF RFC 8693: "OAuth 2.0 Token Exchange".

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

## 6.X Authorization procedure in a nested API invocation

Editor’s Note: This clause will include authorization procedure for nested API invocation cases.

The nested API invocation scenario is a scenario where an API invocation towards a first API exposing function (AEF-1) triggers that API exposing function to request an API invocation towards a second API exposing function (AEF-2), which is in the same API provider domain as the first API exposing function. The authorization of API invocation triggered towards second API exposing function shall use token exchange procedure as specified in IETF RFC 8693 [xx], where the access token of the API invoker to be used towards AEF-1 is used as the subject token as per the IETF RFC 8693 [xx]. AEF-1 before triggering API invocation towards AEF-2, invokes the token exchange request towards the CCF by sending the subject token to receive a new access token. AEF-1 uses the received new access token towards AEF-2 for nested API invocation. This is depicted in figure 6.X-1.



Figure 6.X-1: Authorization for nested API invocation

1. API invoker -1 invokes the AEF-1 service by using the access token obtained from the CCF/Authorization Function.

2. Based on the service API invocation request, API exposing function 1 verifies the access token and decides to invoke another service API exposed by API exposing function 2.

3. The API exposing function 1 sends token exchange request message to CCF, to get a token to invoke the service API in API exposing function 2. The CCF validates the request from API exposing function 1. The CCF validates whether the requesting API exposing function 1 is allowed for accessing service API of API exposing function 2. Also, the CCF validates the access token in the request message that is provided by the API invoker to AEF-1. After successful validation, the CCF responds to API exposing function 1 with token exchange response message that includes a new access token to allow API exposing function 1 to invoke the service API on API exposing function 2.

Editor’s Note: The content of the newly issued token is FFS.

Editor’s Note: The parameters in the token exchange request and response is FFS.

Editor’s Note: How the CCF validates whether the requesting API exposing function 1 is allowed for delegated authorization to access service API of API exposing function 2 is FFS.

4. API exposing function 1, shall send a service API invocation request to API exposing function 2 with the authorization information i.e., access token received in step 7.

5. The API exposing function 1 receives the service API invocation response resulting from the service API invocation once API exposing function 2 has checked whether the API invoker is authorized to invoke that service API based on the received token.

6. The API invoker receives the service API invocation response resulting from the service API invocation.

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