**3GPP TSG-SA3 Meeting #**115 ***S3-240475***

**Athens, Greece, 26th Feb 2024 - 1st Mar 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.122** | **CR** | **0062** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******LP*** *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 | **X** |

|  |
| --- |
|  |
| ***Title:*** | Alignment of 33.122 for RNAA |
|  |  |
| ***Source to WG:*** | NTT DOCOMO |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** | SNAAPPY |  | ***Date:*** | 2024-02-19 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | Clause 6.5.3.1 contains an editor's note:Editor's Note: The details of access tokens used for RNAA need to be aligned with stage 3 (e.g., claim versus scope).Clause 6.5.3.2 contains the editor's note:Editor's Note: The details of access tokens used for RNAA need to be aligned with stage 3 (e.g., claim versus scope).Clause 6.5.3.3 contains the editor's notes:Editor’s Note: Whether and how the token and/or authorization request can include resource owner ID is left to stage 3.Editor's Note: further details of the token are left for stage 3, this includes how to differentiate RNAA and legacy tokensThese can be removed, as the work has progressed sufficiently.Clause C.1 contains the editor's note:Editor’s Note: Clarification between access tokens used for existing CAPIF implementations and access tokens used for northbound CAPIF implementations are FFS.This can be removed, as all CAPIF tokens are on the northbond interface. |
|  |  |
| ***Summary of change:*** | Resolving editor's notes in 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.5.3.4, and C.1 |
|  |  |
| ***Consequences if not approved:*** | Unresolved editor's notes. |
|  |  |
| ***Clauses affected:*** | 2, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.5.3.4, and C.1 |
|  |  |
|  | **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:*** |  |

FIRST CHANGE

#### 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, but 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 GPSI . The API invoker ID binds the token to the API invoker. To avoid privacy issues, GPSI should be different from MSISDN, SUPI etc.

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 GSPI (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 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 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 supported flows to the API invoker.

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

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

NEXT CHANGE

#### 6.5.3.2 Authorization using oauth client credential flow

If client credential flow is used for authorization of the API invoker by the AEF, the procedures in RFC 6749 [4] shall be followed with the following profile:

- The access token request message may include the resource owner ID.

NOTE 1: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

Editor’s note: the mapping of API Invoker ID and GPSI is left for stage 3.

- The CCF shall check whether the API invoker is entitled to consume the API and allowed to access the resources of the resource owner, by using authorization information available in the CCF.

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. If the API invoker is an AF not on a UE, the check is omitted.

NOTE 2: How to get the authorization from the resource owner and store it in the CCF is out of scope of the present document.

NEXT CHANGE

#### 6.5.3.3 Authorization using authorization code (optional PKCE) flow

If authorization code flow, optionally with PKCE, is used by the AEF for authorization of the API invoker, the procedures in RFC 6749 [4] and optionally RFC 7636 [11] shall be followed, with the following profile:

- The authorization token and/or authorization request may include the resource owner ID.

NOTE: If the API invoker is on a UE, the CCF obtains its GPSI during authentication.

Editor's note: the mapping of API Invoker ID and GPSI is left for stage 3.

- The resource owner dynamically authorizes the API invoker to access the resource owner's resources as described in RFC 6749 [4] and optionally RFC 7636 [11].

- If the API invoker is on a UE, the CCF shall check that the UE is accessing its own resources. The access token shall contain the resource owner ID (i.e. GPSI) and the API invoker ID. If the API invoker is an AF not on a UE, the check is omitted.

NEXT CHANGE

# C.1 General

The information in this annex provides a description of the access token used in the ‘Method 3 – TLS with OAuth token’ authentication and authorisation method (see clause 6.5.2.3) and access token used in RNAA (see clause 6.5.3). Characterization of the access token, how to obtain the access token, how to validate the access token, and how to refresh the access token is explained.

An ‘Method 3 – TLS with OAuth token’ access token has the following chanracterics:

- Shall be encrypted when transported over the CAPIF 1/1e and CAPIF 2/2e interfaces (e.g. using TLS);

- Shall be a bearer type as specified in IETF RFC 6750 [5];

- Shall be encoded as a JSON Web Token as specified in IETF RFC 7519 [6];

- Shall be protected by the JSON signature profile as specified in IETF RFC 7515 [7]; and,

- Shall be validated per OAuth 2.0 [4], IETF RFC 7519 [6] and IETF RFC 7515 [7].

END OF CHANGES