**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220922-r1***

**e-meeting, 16 - 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.558** | **CR** | **0002** | **rev** | **-**  | **Current version:** | **17.0.0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Clarification of access token usage in EC |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eEDGE\_5GC |  | ***Date:*** | 2022-05-09 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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:*** | Access token usage for authorization between EEC and EES has been specified but some details, such as the usage of OAuth 2.0 framework, are missing. The claim used for EEC ID is not aligned with the convention where the "client\_id" is used for client identifiers. |
|  |  |
| ***Summary of change:*** | Details about the usage of access tokens for authorization are added. The claim for EEC ID is changed from "sub" to "client\_id".  |
|  |  |
| ***Consequences if not approved:*** | Misleading and unclear information in TS 33.558. No alignment for the claim used for client identifiers in tokens. |
|  |  |
| ***Clauses affected:*** | 2, 6.2, 6.3 |
|  |  |
|  | **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 1st Change \*\*\*

# 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 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[4] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

[6] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[7] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

 8] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[9] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[10] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[11] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[12] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

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

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

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

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

\*\*\* End of 1st Change \*\*\*

\*\*\* Start of 2nd Change \*\*\*

## 6.2 Authentication and Authorization between EEC and ECS

 The ECS shall be configured with the information of authorization methods (token-based authorization or local authorization) used by EESes.

For authentication between EEC and ECS, TLS authentication methods shall be used. Details of TLS authentication methods (e.g., client certificate, AKMA [11], GBA [12]) are out of scope of the current document. If the EEC sends the GPSI to the ECS, then the ECS shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the current document.

After successful authentication, the ECS shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the ECS decides whether OAuth 2.0 [AA] access tokens are required for the candidate EESes using the configuration information and issues separate EES access tokens to be used for each candidate EESes that use token-based authorization. The ECS, EEC and EES respectively assume the role of authorization server, client and resource server roles defined in [AA]. "Client Credentials" grant type and bearer tokens [BB] shall be used. JSON Web Token (JWT) as specified in IETF RFC 7519 [CC] for encoding and the JSON signature profile as specified in IETF RFC 7515 [DD] for protection of tokens shall be followed. This token profile also applies for clause 6.3 of the present document. The claims of the EES service tokens in the form of JWT [CC] shall include the ECS FQDN (issuer), EEC ID (client\_id), GPSI (subject), expected EES service name(s) (scope), EES FQDN (audience), expiration time (expiration). The ECS shall send the service response back to the EEC, which may include EES access token(s).

\*\*\* End of 2nd Change \*\*\*

\*\*\* Start of 3rd Change \*\*\*

## 6.3 Authentication and Authorization between EEC and EES

For authentication between EEC and EES, TLS authentication methods shall be used. Details of TLS authentication methods (e.g., client certificate, AKMA [11], GBA [12]) are out of scope of the current document. If the EEC sends the GPSI to the EES, then the EES shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the current document.

For authorization of EEC by the EES, the EEC shall send the OAuth 2.0 [AA] access token, if received from the ECS, to the EES. The token profile is specified in clause 6.2 of the present document. If the EES requires access token for authorization, then the EES shall authorize the EEC by using the token. Otherwise, the EES shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the EES shall process the request and send the service response back to the EEC.

\*\*\* End of 3rd Change \*\*\*