**3GPP TSG-SA3 Meeting #100e *S3-201610-r1***

**e-meeting, 17-28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0879** | **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 |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Access Token Signature using MAC with symmetric key |
|  |  |
| ***Source to WG:*** | Mavenir, Deutsche Telekom |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2020-08-17 |
|  |  |  |  |  |
| ***Category:*** | A |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In the case of access token based authorization, TS33.501 mandate the support of Access Token signature using MAC based on symmetric keying. No further information is provided in TS33.501.This CR provides clarification that the symmetric keys are pairwise summetric keys between the NRF and the NF service Producer and the provisioning of such keys are outside the scope of this document. |
|  |  |
| ***Summary of change:*** | Adding the following Note for clarity:NOTE: Securing the access token using Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a pairwise pre shared symmetric key between the NRF and the NF service producer. The provisioning of such pre-shared symmetric key(s) is outside the scope of this document. |
|  |  |
| ***Consequences if not approved:*** | Confusion of what is required to support Access Token Signature based on MAC with symmetric keys. |
|  |  |
| ***Clauses affected:*** | 13.4.1.0 |
|  |  |
|  | **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 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 13.4.1 OAuth 2.0 based authorization of Network Function service access

#### 13.4.1.0 General

The authorization framework described in clause 13.4.1 allows NF service producers to authorize the requests from NF service requestors.

The authorization framework uses the OAuth 2.0 framework as specified in RFC 6749 [43]. Grants shall be of the type Client Credentials Grant, as described in clause 4.4 of RFC 6749 [43]. Access tokens shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45].

NOTE x: Securing the access token using Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a pairwise pre-shared symmetric key between the NRF and the NF Service Producer. The provisioning of such pre-shared symmetric key is outside the scope of this document.

The basic extent provided by the authorization token is at service level (i.e. the "scope" claim includes allowed services per NF type). Depending on the NF service producer configuration, higher level of granularity for the authorization token can be defined adding "additional scope" information within the token e.g. to authorize specific service operations and/or resources/data sets within service operations per NF consumer type.

NOTE 1: The additional scope(s) included within the access token add additional security checks at the NF service producer that authorizes the services operations, resources and NF consumer type related to the additional scope(s).

The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.

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