**3GPP TSG-SA3 Meeting #98Bis-e *S3-200686r2***

**e-meeting, 14-17 April 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** |  | **rev** | **1** | **Current version:** | **16.2.0** |  |
|  |
| *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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | Trust mode in the eSBA |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon, Mavenir?  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5G\_eSBA |  | ***Date:*** | 2020-3-25 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***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:*** | Currently, the authentication and static authorization in the indirect communication model is not clear. A hop-by-hop trust mode is introduced to deal with the authentication and static authorization between NF and NRF, and NF service consumer and NF service producer. |
|  |  |
| ***Summary of change:*** | Adding the clarifications on the authentication and static authorization between NF and NRF, and NF service consumer and NF service producer in clause 13.3.1, and 13.3.2. |
|  |  |
| ***Consequences if not approved:*** | Unclear authentication and static authorization in the indirect communication model |
|  |  |
| ***Clauses affected:*** | 13.3.1, 13.3.2 |
|  |  |
|  | **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 CHANGES \*\*\*\***

### 13.3.1 Authentication and authorization between network functions and the NRF

NRF and NF shall authenticate each other during discovery, registration, and access token request. If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.

During the indirect communication scenario, mutual authentication is implicit by hop by hop TLS transport layer authentication between the NF and SCP, and the SCP and NRF.

NOTE X1: During the indirect communication scenario, authentication NF and NRF in different PLMN is implicit by authentication between NF-SCP as in clause 13.3.6, SCP-SEPP as in clause 13.3.5, SEPP-SEPP as in clause 13.2, SCP-NRF as in clause 13.3.3.

NOTE Y1: .E2E authentication between NF and NRF is not achieved with hop-by-hop security.

If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF service and the type of the NF service consumer, as described in clause 4.17.4 of TS23.502 [8].In the roaming scenario, the NRF of the NF Service Provider shall authorize the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF Service, the type of the NF service consumer and the serving network ID.

If the NRF finds NF service consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

NOTE 1: When a NF accesses any services (i.e. register, discover or request access token) provided by the NRF , the OAuth 2.0 access token for authorization between the NF and the NRF is not needed.

### 13.3.2 Authentication and authorization between network functions

Authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

- If the PLMN does not use protection at the transport layer, authentication between NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

When an NF receives message from other unauthenticated NF, the NF shall support error handling, and may send back an error message.

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

Depending on whether token-based authorization is used or not, authentication between network functions shall be performed in one of the following ways:

- If token-based authorization is used within one PLMN, in the scenario of direct communication, the service consumer NF and the service producer NF shall authenticate each other by the mutual TLS at transport layer before trying to access the service API. In the indirect communication scenario, the mutual authentication is implicit by hop by hop TLS transport layer authentication between the service consumer NF and SCP and the SCP and the service producer NF.

NOTE 1: Authentication of the service consumer NF towards the service producer NF will be implicit by authorization, which can only be granted after successful authentication of the service consumer NF towards the NRF.

- If token-based authorization is not used within one PLMN, service consumer NF and service producer NF shall mutually authenticate before performing access to the service API. The service producer NF shall additionally check authorization of the service consumer NF based on local policy before granting access to the service API.

NOTE 2: During the direct communication scenario, authentication between network functions in different PLMN is implicit by authentication between NF-SEPP as in clause 13.3.3, SEPP-SEPP as in clause 13.3.4 and SEPP-NF as in clause 13.3.3.

NOTE X: During the indirect communication scenario, authentication between network functions in different PLMN is implicit by authentication between NF-SCP as in clause 13.3.6, SCP-SEPP as in clause 13.3.5, SEPP-SEPP as in clause 13.2.

NOTE Y2: .E2E authentication between NF and NF is not achieved with hop-by-hop security.

When local policy check is failed, NF service provider shall support error handling, and may send back an error message.

The present document does not provide a standardised solution for binding 5G SBA REST Service Operations between the PLMN V-SMF and H-SMF over N16 / N32 to GTP-U over N9 in roaming scenarios. To prevent injection or spoofing of UP traffic over N9, it is recommended to use a common firewall that can correlate HTTP/2 methods and GTP-U in order to bind and filter out any malicious traffic on N9. Use of a common firewall may place other implementation restrictions (e.g. co-location of SMF, SEPP and UPF) in order to allow use of a common firewall.

**\*\*\*\* END OF CHANGES \*\*\*\***