**3GPP TSG-SA3 Meeting #100e *S3-202164***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0946** | **rev** | **-** | **Current version:** | **15.9.0** |  |
|  |
| *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:***  | Error handling by the receiving NF |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-SEC |  | ***Date:*** | 27.8.2020 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-15 |
|  | *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:*** | Clarification needed on NF being the receiving NF |
|  |  |
| ***Summary of change:*** | Adding “receiving” NF |
|  |  |
| ***Consequences if not approved:*** | Ambiguity of spec |
|  |  |
| ***Clauses affected:*** | 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

### 13.3.2 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 a message from an unauthenticated NF, the receiving 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, the service consumer NF shall authenticate the service producer NF at transport layer before trying to access the service API. The service producer NF may authenticate the service consumer NF at transport layer.

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: 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 13.2 and SEPP-NF as in clause 13.3.3.

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