**3GPP TSG-SA3 Meeting #100e *S3-201917-r2***

**e-meeting, 17 – 28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **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:*** | Verification of Serving Network Name in AUSF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | |  |
|  | *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 can be 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:*** | | Clause 6.1.2 of TS 33.501 requires that upon receiving and authentication request from the AMF, the AUSF shall check that the requesting SEAF in the serving network is entitled to use the serving network name in the Authentication Request by comparing the serving network name with the **expected serving network name**.  While it is clearly specified how the AMF constructs the serving network name it is not defined at all which is the “expected serving network name” the AUSF shall use to compare it with. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is specified how the AUSF can verify the serving network name provided by the AMF.  The AUSF can consider one of the following information as the “expected serving network name”:   * If the OAuth framework is supported, the AUSF can consider the PLMN ID of the consumer NF if included in the access token presented by the AMF as the expected serving network name.      * For the roaming case, the AUSF can use the remote PLMN ID asserted by the SEPP at the AUSF PLMN as the expected serving network name. This requires that before sending the authentication request to the AUSF, the SEPP includes the PLMN ID of the related N32-f context from which the authentication request was received within the authentication request. * For the non-roaming case, the AUSF may perform the SNN verification based on operator-specific methods within its own PLMN (e.g. by checking the PLMN ID included in the certificate of the serving AMF). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AUSF is not able to verify the serving network name provided by the AMF. AMF may request authentication vectors for a serving network it does not belong to. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2; 13.2.4.7 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE\*\*\*

#### 13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP shall decrypt the JWE ciphertext using the shared session key and the following parameters obtained from the JWE object – Initialization Vector, Additional Authenticated Data value (clearTextEncapsulatedMessage in "aad") and JWE Authentication Tag ( "tag").

The receiving SEPP shall check the integrity and authenticity of the clearTextEncapsulatedMessage and the encrypted text by verifying the JWE Authentication Tag in the JWE object with the JWE AAD algorithm. The algorithm returns the decrypted plaintext (dataToIntegrityProtectAndCipher) only if the JWE Authentication Tag is correct.

The receiving SEPP shall apply the decrypted JSON patch in the dataToIntProtectAndCipher to the clearTextEncapsulatedMessage. The receiving SEPP shall use the NF API data type placement mapping and the encryption policy to verify that the correct information elements have been encrypted.

The receiving SEPP shall next verify IPX provider updates, if included, by verifying the JWS signatures added by the intermediaries. The SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the IPX provider’s security information list obtained during parameter exchange in the related N32-c connection setup or, alternatively, has been configured for the particular peer SEPP. It shall then check that the raw public key or certificate of the JWS signature IPX's Identity in the modifiedDataToIntegrity block matches to the IPX provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the IPX provider security information list.

The receiving SEPP shall check whether the modifications performed by the intermediaries were permitted by the respective modification policies. If this is the case, the receiving SEPP shall apply the patches in the Operations field in order, perform plausibility checks, and create a new HTTP request according to the "patched" clearTextEncapsulatedMessage.

The receiving SEPP shall verify that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context.

Depending on local operator policy, before sending the incoming N32-f message to the receiving NF, the receiving SEPP may include the PLMN ID of the related N32-f context from which the incoming N32-f message was received within the incoming N32-f message. This can be further used at the receiving NF as the remote PLMN ID asserted by the SEPP.

NOTE 1: If there is an SCP between the SEPP and the NF, the NF can trust the PLMN-ID if it trusts the SCP and SEPP.

An SCP that receives a message with a PLMN-ID indicating it has been asserted by the SEPP shall forward the PLMN-ID to the next hop without changes.

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