**3GPP TSG-SA3 Meeting #119 *draft\_S3-244752-r1***

**Orlando, US, 11th - 15th November 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **2069** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  | | | | | | | | |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm" \l "_blank)*** *on using this form: comprehensive instructions can be found at  <http://www.3gpp.org/Change-Requests>.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Security aspects for Indirect Network Sharing | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE Corporation, China Unicom | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI19 | | | | |  | ***Date:*** | | | 2024-10-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to LS C4-244497, how to set the PLMN ID in the 3gpp-Sbi-Originating-Network-Id header in the Indirect Network Sharing case is unclear. It is propose to clarify that the PLMN ID in the 3gpp-Sbi-Originating-Network-Id header set by the source NF of the hosting operator network can be the selected PLMN ID which represents the participating operator or the PLMN ID of the hosting operator (i.e. VPLMN ID) during the UE authentication. When there is no roaming agreement between the hosting operator and the participating operator, the PLMN ID in 3gpp-Sbi-Orginating-Network-Id header is set to the selected PLMN ID which represents the participating operator.  In order to support the 2 kinds of PLMN ID in 3gpp-Sbi-Originating-Network-Id header in the Indirect Network Sharing case, several clarifications shall be added to relevant clauses. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add notes to relevant clauses to support Indirect Network Sharing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | the PLMN ID may be regarded as misconfigured, leading to service interruption. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.9.3.2, 5.9.3.5, 6.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The feature of supporting Roaming Hubs by SEPPs introduced in the present Release, i.e. in TS 33.501 (the present document) and TS 29.573 [73], addresses the requirements that may be applicable to SEPPs starting from Release 16.

In order to support PRINS functionality using Roaming Intermediaries, the feature specified in this document may be supported by Release 16 and 17 implementations of SEPPs.

NOTE: It is implementation specific on how to support the scenario where the Rel 16 and 17 SEPP of the roaming partners are not aligned regarding the support of Roaming Intermediaries.

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication with the SEPP in the other network.

The SEPP shall perform negotiation of cipher suites with the SEPP in the other network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID or SNPN ID in the received N32 message.

The SEPP to SEPP communication may go via up to two Roaming Intermediaries. The changes made by Roaming Intermediaries to messages originated by a SEPP, based on the originating PLMNs policy, shall be identifiable by the receiving SEPP.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of Roaming Intermediaries performing message modifications. The SEPP shall support multiple trust anchors.

NOTE 1: Such a differentiation and support of multiple trust anchors could be done, e.g. , by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The sending SEPP shall reject messages received from the NF (directly or via SCP) with JSON including "encBlockIndex" (regardless of the encoding used for that JSON request).

The receiving SEPP shall reject any message in which a Roaming Intermediary has inserted or relocated references to encBlockIndex.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP’s own PLMN (or SNPN), the message is discarded.

The SEPP shall be able to use one or more PLMN IDs (or SNPN IDs). In the situation that a PLMN (or SNPN) is using more than one PLMN ID (or SNPN ID), this PLMN’s SEPP (or SNPN’s SEPP) may use the same N32-connection for all of the networks PLMN IDs (or SNPN IDs), with each of the PLMN’s (or SNPN’s) remote partners. If different PLMNs (or SNPNs) are represented by the PLMN IDs (or SNPN IDs) supported by a SEPP, the SEPP shall use separate N32-connections for each pair of home and visited PLMN (or SNPN).

NOTE 3: If a given PLMN uses a Roaming Hub (RH) for the purposes of roaming with multiple other PLMNs, then a single TLS connection between the PLMN’s SEPP and the RH can be used for carrying the N32-f PRINS signalling for some or all the other PLMNs.

NOTE 4: void

Error messages may be originated from either PLMN SEPPs or Roaming Hubs to adjacent Roaming Hubs or adjacent PLMN SEPPs, in an identifiable way.

If allowed by the PLMN policy, the SEPP shall be able to send error messages on the N32 interface to a Roaming Hub.

Specific error messages relevant to Roaming Hubs shall be supported (such as 'an IE is encrypted while it was expected to be available in the clear', 'an IE is not encrypted while its availability in the clear is not required', 'the N32 connection cannot be setup due to contractual reasons', 'the N32 connection cannot be setup due to a connectivity issue' and 'the message was not delivered due to contractual reasons'). See details in clause 5.9.3.2a.

Sending SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header:

- If the sending NF or the SCP has inserted the 3gpp-Sbi-Originating-Network-Id header in the signaling message (service/subscription request or notification message), the sending SEPP shall compare the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header in the received signaling message with the PLMN ID(s) or SNPN ID(s) that the sending SEPP represents by its certificate.

- If the PLMN ID or SNPN ID does not match with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall discard the received signaling message.

- If the PLMN ID or SNPN ID matches with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall forward the signaling message to the receiving SEPP.

- If the sending NF and the SCP have not included the 3gpp-Sbi-Originating-Network-Id header in the signalling message, the sending SEPP shall include the 3gpp-Sbi-Originating-Network-Id header and send the updated signaling message to the receiving SEPP.

- If the sending SEPP only represents one PLMN ID or SNPN ID, the sending SEPP shall insert the 3gpp-Sbi-Originating-Network-Id header with this ID.

- If the sending SEPP represents multiple PLMN IDs or SNPN IDs, it is up to configuration and deployment to determine which PLMN ID or SNPN ID value should be included in the header.

Receiving SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header:

- The receiving SEPP shall check whether the 3gpp-Sbi-Originating-Network-Id header included in the signalling message belongs to the sending SEPP’s own PLMN or SNPN. It does this by verifying that the asserted PLMN ID in the 3gpp-Sbi-Originating-Network-Id header matches one of the sending SEPP's own PLMN ID(s) or SNPN ID(s) either in the N32-f context, the sending SEPP's certificate, or a locally configured list of PLMN IDs or SNPN-IDs that the sending SEPP represents.

- If the 3gpp-Sbi-Originating-Network-Id header does not match with any of the PLMN IDs or SNPN IDs belonging to the peer sending SEPP, the receiving SEPP shall discard the received signaling message.

- If the 3gpp-Sbi-Originating-Network-Id header matches with any PLMN ID of the PLMN or SNPN IDs belonging to the peer sending SEPP, the header is successfully verified, and the receiving SEPP shall forward the received signaling message to the target NF.

NOTE 5: Details on SEPP behaviour are specified in TS 29.500 [74].

NOTE X: In the case of Indirect Network Sharing as specified in clause 5.18 of TS 23.501[x], the PLMN ID in the 3gpp-Sbi-Originating-Network-Id header set by the source NF of the hosting operator network can be the selected PLMN ID which represents the participating operator or the PLMN ID of the hosting operator based on the coordination and agreement between the hosting operator and the participating operator.

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

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

### 6.1.2 Initiation of authentication and selection of authentication method

The initiation of the primary authentication is shown in Figure 6.1.2-1.



Figure 6.1.2-1: Initiation of authentication procedure and selection of authentication method

The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

The Nausf\_UEAuthentication\_Authenticate Request message shall contain either:

- SUCI, as defined in the current specification, or

- SUPI, as defined in TS 23.501 [2].

The SEAF shall include the SUPI in the Nausf\_UEAuthentication\_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf\_UEAuthentication\_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf\_UEAuthentication\_Authenticate Request shall furthermore contain:

- the serving network name, as defined in sub-clause 6.1.1.4 of the present document.

NOTE 1: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs.

The Nausf\_UEAuthentication\_Authenticate Request may furthermore contain:

- Disaster Roaming service indication, as specified in TS 23.502[8] clause 4.2.2.2.

Upon receiving the Nausf\_UEAuthentication\_Authenticate Request message, the AUSF shall check that the requesting SEAF in the serving network identified by the 3gpp-Sbi-Originating-Network-Id header specified in TS 29.500 [74] is entitled to use the serving network name in the Nausf\_UEAuthentication\_Authenticate Request. For the case that the 3gpp-Sbi-Originating-Network-Id header is not included, the AUSF may authorize the serving network based on its name available in the Nausf\_UEAuthentication\_Authenticate Request message..

NOTE 1a: As described in clause 5.9.3.2, the SEPP in the AUSF's network verifies the correctness of the 3gpp-Sbi-Originating-Network-Id header and the SEPP in the SEAF's network ensures that the 3gpp-Sbi-Originating-Network-Id is included.

NOTE 1X: In the case of Indirect Network Sharing as specified in clause 5.18 of TS 23.501[x], the PLMN ID in the 3gpp-Sbi-Originating-Network-Id header set by the source NF of the hosting operator network can be the selected PLMN ID which represents the participating operator or the PLMN ID of the hosting operator. How AUSF checks the 3gpp-Sbi-Originating-Network-Id header is based on the local configuration considering the coordination and agreement between the hosting operator and the participating operator.

The AUSF shall store the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF shall respond with "serving network not authorized" in the Nausf\_UEAuthentication\_Authenticate Response.

NOTE 2: The AUSF and the UDM may be configured with Disaster Condition via OAM based on operator policy and the request by the government agencies.

For the Disaster Roaming, the AUSF shall check the local configuration and, if allowed, the AUSF sends Nudm\_UEAuthentication\_Get Request to the UDM.

The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;

- the serving network name;

- if received from SEAF, Disaster Roaming service indication;

Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

Based on SUPI, the UDM/ARPF shall choose the authentication method.

NOTE 3: The Nudm\_UEAuthentication\_Get Response in reply to the Nudm\_UEAuthentication\_Get Request and the Nausf\_UEAuthentication\_Authenticate Response message in reply to the Nausf\_UEAuthentication\_Authenticate Request message are described as part of the authentication procedures in clause 6.1.3.

For the Disaster Roaming, the UDM shall check the local configuration and, if allowed, the UDM proceeds with the chosen authentication method.

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

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

#### 5.9.3.5 Requirements for Network Functions (NF)

The NF that sends a signalling message (service/subscription request or notification message) shall include its PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header.

If an NF supports multiple PLMN IDs or SNPN IDs, the sending NF shall include the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header on behalf of which the message is sent.

The handling of the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header at the receiving NF is up to configuration and deployment.

NOTE: A misconfigured PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header can lead to service interruption.

NOTE: Setting 3gpp-Sbi-Originating-Network-Id header as the selected PLMN ID which represents the participating operator only applies to the scenario when there is no roaming agreement between the hosting operator and the participating operator.

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