**3GPP TSG SA Meeting #103SP-240499**

**Maastricht, NL, 19 - 22 Mar. 2024**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1972** | **rev** | **2** | **Current version:** | **18.4.0** |  |
|  |
| *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:***  | Support of Modified PRINS in earlier releases |
|  |  |
| ***Source to WG:*** | - |
| ***Source to TSG:*** | Vodafone |
|  |  |
| ***Work item code:*** | Roaming5G |  | ***Date:*** | 2024-03-20 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Following agreements according to the endorsed S3-240313, and agreed CRs in S3-234764 and [S3-235069](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_113_Chicago/docs/S3-235069.zip), text to support Modified PRINS functionality for earlier releases is introduced. |
|  |  |
| ***Summary of change:*** | Introducing support Modified PRINS for releases 16 and onwards |
|  |  |
| ***Consequences if not approved:*** | Roaming Hubs will not work to 3GPP specifications leading to potential market issues. |
|  |  |
| ***Clauses affected:*** | 5.9.3.2 |
|  |  |
|  | **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:*** | Rev 1: Draft indication on support in release 16 and 17Rev 2: Correct typos and adding note for the applicability to release 16 and 17 |

\*\*\*\* First Change\*\*\*\*

####

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

The feature of supporting roaming hubs by SEPPs introduced in Release 18, 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 hub/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 and negotiation of cipher suites with the SEPP in the roaming 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 for the purposes of roaming with multiple other PLMNs, then a single TLS connection between the PLMN’s SEPP and the roaming hub 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').

Sending SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header specified in TS 29.500 [74]:

- 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 receving 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.

\*\*\*\* End of Changes\*\*\*\*