**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212757-r2***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1178** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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:*** | SEPP to verify the source PLMN-ID | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-08-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In a roaming scenario where one SEPP serves a given PLMN, and such PLMN has multiple PLMN-IDs but uses the same N32 connection for all PLMN-IDs, the current specification does not describe the solution how to identify and verify the source PLMN-ID of a message.  Please check S3-212755 DP for more information. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The sending and receiving SEPP shall discard messages if the source PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-Id header) included in the signaling message does not belong to the sending SEPP’s own PLMN. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Roaming scenarios where one SEPP serves a given PLMN, and such PLMN has multiple PLMN-IDs but uses the same N32 connection for all PLMN-IDs, will not work. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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:*** | |  | | | | | | | | |

\*\*\* Start of Change \*\*\*

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

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 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 in the received N32 message.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications.

NOTE 1: Such a differentiation 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 an IPX 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, the message is discarded.

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

If the source PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-Id header) is included in the NF's service/subcription request and notification messages, the sending SEPP shall verify the incoming source PLMN ID. If the PLMN ID does not match any of the PLMN IDs supported bt the sending SEPP, the sending SEPP shall discard the message. If the PLMN ID matches one of the PLMN IDs supported by the sending SEPP, the sending SEPP shall forward the signaling message including the validated PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-Id header) to the receiving SEPP.

In absence of source PLMN ID from the NF, the sending SEPP shall insert the respective PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-ID header) in the signaling message before it sends the message to the receiving SEPP.

Editor's note: It is FFS how to solve the case when the source PLMN ID is not present in the message received from the NF

The receiving SEPP shall validate that the PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-Id header) matches one of the PLMN IDs of the sending SEPP that have been exchanged during the N32-C negotiation. The receiving SEPP shall discard service/subscription request and notification messages if the source PLMN ID (i.e., 3gpp-Sbi-Asserted-Plmn-Id header) included in the signaling message does not match any of the PLMN IDs supported by the sending SEPP.

\*\*\* End of Change \*\*\*