**3GPP TSG-SA3 Meeting #117 S3-242xxx**

Maastricht, Netherlands 19 - 23 August 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0000** | **rev** | **-** | **Current version:** | **18.6.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******LP*** *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 |  |

|  |
| --- |
|  |
| ***Title:*** | Trust anchoring for N32-f/PRINS |
|  |  |
| ***Source to WG:*** | Federal Office for Information Security (BSI) |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | Roaming5G |  | ***Date:*** | 2024-07-29 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel- |
|  | *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:*** | While trust anchoring for N32-c is specified, it is not specified for N32-f/PRINS. Moreover, checking that a given N32-f connection (both TLS and PRINS) only carries traffic for PLMNs according to the trust anchors is not specified. This CR closes these gaps. |
|  |  |
| ***Summary of change:*** | Specify trust anchoring for N32-f/PRINS as well as PLMN-ID crosschecks for N32-f (both TLS and PRINS). |
|  |  |
| ***Consequences if not approved:*** | While trust anchoring is supported with granularity of individual PLMNs for N32-c and direct (non-mediated) roaming relations, this is not the case for mediated roaming relations (i.e. with N32-f/PRINS). Moreover, checking that N32 signalling over a given N32-f connection is consistent with trust anchors with granularity of individual PLMN-IDs was not specified so far. These aspects are detrimental to security and will continue to exist if this CR is not approved. |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications | TS/TR ... CR ... |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ... |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ... |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 13.1.2 Protection between SEPPs

TLS shall be used for N32-c connections between the SEPPs.

The SEPP shall maintain a set of trust anchors for N32-c, each consisting of a list of trusted root certificates and a list of corresponding PLMN-IDs. Any given PLMN-ID shall appear in at most one trust anchor. During N32-c connection setup, the SEPP shall map the PLMN-ID of the remote SEPP end entity certificate to the associated trust anchor for the purposes of certificate chain verification. Only the root certificates in the associated list shall be treated as trusted during certificate chain verification. If the remote SEPP certificate contains multiple PLMN-IDs that are mapped to different trust anchors, then that certificate shall be rejected (also see clause 4.2.5 of TS 33.517). Moreover, the SEPP shall raise an alarm and should tear down the connection if any of the PLMN-IDs it receives from the remote peer during N32-c negotiation does not match the PLMN-IDs in the selected trust anchor.

Operator Group Roaming Hubs SEPPs are equivalent to a network operator SEPP when they are in the same security domain and are not considered Roaming Intermediaries as detailed in this clause. The communication between a group network operator's SBA network border element and the Operator Group Roaming Hub SEPP is out of scope of the present document.

If there are no Roaming Intermediaries between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. Different TLS connections are used for N32-c and N32-f. If there are Roaming Intermediaries which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

If TLS is selected, the SEPP shall correlate the N32-f TLS connection with the N32-c connection. If the peer network is a PLMN, the SEPP compares the PLMN-IDs contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections. Specifically, if the certificate used for N32-f contains one or more PLMN-IDs that are not contained in the TLS certificate used for the corresponding N32-c, the N32-f certificate shall be rejected. If the peer network is an SNPN, the SEPP compares the SNPN-ID contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections. The SEPP shall perform crosschecks that ensure that signalling received over the established N32-f/TLS connection is not associated to any PLMN other than those in the trust anchor selected during the setup of the correlated N32-c connection. In case of a mismatch the SEPP should reject the signalling message and raise an alarm.

If there are Roaming Intermediaries which, in addition to IP routing, offer other services that require modification or observation of the information and/or additions to the information sent between the SEPPs, PRINS shall be used for protection of N32-f connections between the SEPPs.

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs allows SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32, and provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.

If PRINS is used on the N32-f interface, one of the following additional transport protection methods shall be applied between SEPP and Roaming Intermediary for confidentiality and integrity protection:

- NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5], or

- TLS VPN with mutual authentication following the profile given in clause 6.2 of TS 33.210 [3] and clause clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 9113 [47].

Irrespectively of which of the above mechanisms is used, the SEPP shall support multiple trust anchors for N32-f/PRINS. More precisely, the SEPP shall maintain a set of trust anchors for N32-f/PRINS, each consisting of a list of trusted root certificates, a list of unique identifiers for a given Roaming Intermediary (RI), and a list of PLMN-IDs that are reachable via that RI. Any given RI identifier shall appear in at most one trust anchor. During N32-f/PRINS connection setup, the SEPP shall map the RI identifier as extracted from its end entity certificate to the associated trust anchor for the purposes of certificate chain verification. Only the root certificates in the associated list shall be treated as trusted during certificate chain verification. If the remote end entity certificate contains multiple RI identifiers that are mapped to different trust anchors, then that certificate shall be rejected. Subsequently, the SEPP shall use the trust anchor to perform crosschecks that ensure that PRINS signalling received over the established NDS/IP or TLS connection is not associated to any PLMN other than those indicated by the PLMN-IDs in the selected trust anchor. In case of a mismatch the SEPP should reject the message and raise an alarm.

The RI identifier may or may not include the PLMN-IDs that correspond to the roaming partners that are reachable via the given RI. The SEPP shall support offering N32-f/PRINS at an FQDN/port combination that differs from the combination where it offers N32-c in order to enable PLMN-ID based trust anchoring for N32-c while enabling RI-identifier-based trust anchoring for N32-f/PRINS.

NOTE 1: Void

NOTE 2: Void.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*