**,**

Orlando, USA 11 - 15 November 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **2053** | **rev** | **2** | **Current version:** | **19.0.0** |  |
|  |
| *For* [***HE***](http://www.3gpp.org/3G_Specs/CRs.htm#_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 | **x** |

|  |
| --- |
|  |
| ***Title:*** | Trust anchoring for N32-f/PRINS |
|  |  |
| ***Source to WG:*** | Federal Office for Information Security (BSI), Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | Roaming5G |  | ***Date:*** | 2024-11-15 |
|  |  |  |  |  |
| ***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 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. This is, among other things, due to the lack of PLMN-IDs in TLS certificates associated with Roaming Intermediaries. Moreover, checking that a given N32-f connection (both TLS and PRINS) carries traffic only for roaming partners that were previously configured to be associated with that connection is not well-specified. This CR closes these gaps.The clarifications and mechanisms described in this CR enable anomaly detection if traffic on a specific roaming partner (PLMN ID) arrives over the wrong N32 route. Anomalies can be detected by the operator, if an attacker (which could be also wrongly configured roaming partner or intermediary) is using the wrong tunnel |
|  |  |
| ***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:*** | 13.1.2, 13.2.4.7 |
|  |  |
|  | **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 CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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 and N32-f when the selected security method is “TLS”, each trust anchor consists of a list of trusted root certificates and a list of corresponding PLMN-IDs. For NDS/IP or TLS VPN used for N32-f when the selected security method is “PRINS”, each trust anchor may also include a list of unique identifiers for a given Roaming Intermediary (RI). Any given PLMN-ID and any given RI identifier shall appear in at most one trust anchor

NOTE X: The PLMN-IDs in a given trust anchor for N32-c represent a particular PLMNThe PLMN-IDs in a given trust anchor for N32-f when the selected security method is PRINS represent the PLMNs that are reachable via a particular RI.

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.

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.

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 the selected security method for 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].

During NDS/IP or TLS VPN connection setup, the SEPP should map the RI identifier as extracted from its end entity (i.e., RI) certificate to the associated N32-f/PRINS trust anchor for the purposes of certificate chain verification. Only the root certificates in the associated list may be treated as trusted during certificate chain verification. If the end entity certificate contains multiple RI identifiers that are mapped to different trust anchors, then that certificate should be rejected.

NOTE 1: Void.

NOTE 2: Void.NOTE 3: Whether or not a given RI identifier includes the PLMN-IDs that correspond to the roaming partners that are reachable via that RI, is not specified in 3GPP.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP determines that the received message is an error message generated by the Roaming Hub as Roaming Intermediary based on the reformattedData IE.

If the received messages is not generated by a Roaming Hub :

- 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 refers to the NF API in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

- The receiving SEPP shall next verify RI provider updates, if included, by verifying the JWS signatures added by the Roaming Intermediaries. The SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the Roaming Intermediary’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.

- The receiving SEPP shall then check that the raw public key or certificate of the JWS signature RI's Identity in the modifiedDataToIntegrity block matches to the RI provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the RI provider security information list.

- The receiving SEPP shall check whether the modifications performed by the Roaming Intermediaries, i.e. cRI and pRI, were permitted by the respective modification policies. The receiving SEPP shall use the modification policy of the cRI obtained during parameter exchange in the related N32-c connection setup, and use the modification policy of pRI configured within the receiving SEPP.

- 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. The receiving SEPP may also verify that the PLMN-ID contained in the incoming N32-f message matches the RI identifier in the TLS VPN. In case of a mismatch the SEPP should log the event.

NOTE X: The above mismatch logging can be seen as an anomaly detection mechanism. As such, it can both miss logging some anomalous events (false negatives) and log events that do not represent anomalies (false positives). False negatives occur, for example, when attack signalling carrying a particular PLMN-ID arrives over the TLS VPN or DNS/IP connection that is indeed associated with that PLMN-ID (e.g. generated by a compromised SEPP or an attacker with a fraudulently issued certificate), and false positives occur if signalling for a given PLMN-ID that previously arrived over a particular TLS VPN or NDS/IP connection starts arriving over a different one without this representing an attack. Such a change could be, for example, a result of contractual changes between PLMNs and RIs that were not configured before coming into effect. Dealing with false negatives and false positives is subject to operator policy. If the received message is an error message generated by a Roaming Hub:

- The receiving SEPP shall check that the raw public key or certificate of the JWS signature RI's identity in the modifiedDataToIntegrityProtect block matches the adjacent Roaming Hub identity.

- The receiving SEPP dertermines the message in which the error occurred, based on the N32-f message ID.

- If the receiving SEPP determines from the error message that the Roaming Hub requires a modified request message, it can modify if allowed by the MNO's policy, and can resend the modified request message.

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