**3GPP TSG-SA3 Meeting #124 S3-253221-r3**

**Wuhan, China, 13 – 17 October 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | 33.501 | **CR** | 2184 | **rev** | **<Rev#>** | **Current version:** | 19.4.0 |  |
|  |
| *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:***  | PRINS Refinement |
|  |  |
| ***Source to WG:*** | CableLabs, Nokia, Charter Communications, China Telecom, Deutsche Telekom, Comcast Communications, Verizon, CMCC, BSI, NTT Docomo, Vodafone, Telecom Italia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | RefinePRINS |  | ***Date:*** | 2025-10-3 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-20 |
|  | *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:*** | GSMA NRG sent an LS (S3-252539) to 3GPP SA3 requesting further refinement of PRINS to make it easier for roaming intermediaries (RIs) to support PRINS and its end-to-end application layer security property. Those changes are to implement the refinements of PRINS requested by GSMA.  |
|  |  |
| ***Summary of change:*** | 1. Protecting HTTP CONNECT requests and response by adding requirement to authenticate by TLS or NDS/IP, and by integrity protection of 3gpp-Connect-Req-info and 3gpp-Connect-Resp-Info headers. This allows an RI to cryptographically authenticate HTTP CONNECT requests and responses. 2. Adding HTTPS as an option for protecting the transport of N32-f, in addition to NDS/IP domain security and TLS VPN. |
|  |  |
| ***Consequences if not approved:*** | Some roaming intermediaries may not be willing to support PRINS due to security and operational concerns. Even if they support PRINS, some fraud (e.g., by misusing HTTP CONNECT) may happen in 5G roaming.  |
|  |  |
| ***Clauses affected:*** | 13.1.2, 13.2.3.4 |
|  |  |
|  | **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 \* \* \* \*

### 13.1.2 Protection between SEPPs

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

If the N32-c TLS is established between the SEPPs over one or more Roaming Intermediaries using HTTP CONNECT, as specified in clause 5.5.2.1 of TS 29.573 [73], the HTTP CONNECT request headers including the 3gpp-Connect-Req-Info header and the HTTP CONNECT response headers including the 3gpp-Connect-Res-Info header shall support integrity protection and replay protection using JWS [45].

Transport layer protection of HTTP CONNECT between the initiating SEPP and the first Roaming Intermediary shall be NDS/IP, TLS VPN, or HTTPS with mutual authentication. 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 ,TLS VPN, or HTTPS 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 3: 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.

The SEPP shall check whether the PLMN-IDs in the header and JSON fields, if any, of incoming N32-f messages, are abnormal by matching the PLMN-ID(s) in the relevant trust anchor or remote PLMN-ID(s) in the N32-f context. If TLS is used for N32-f, then the relevant trust anchor is the one selected during the setup of the correlated N32-c connection and, if PRINS is used, it is the trust anchor selected during the setup of the NDS/IP or TLS VPN. The SEPP should support a mode of logging where mismatches are logged.

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].

- HTTP over TLS (HTTPS) as defined in RFC 9110 [113] with mutual authentication.

During NDS/IP ,TLS VPN, or HTTPS 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 are 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 4: 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.

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

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

#### 13.2.3.4 Modification policy

The SEPP shall contain an operator-controlled policy that specifies which IEs can be modified by the RI provider directly related to this particular SEPP. These IEs refer to the IEs after the sending SEPP has rewritten the message.

Each PLMN-operator shall agree the modification policy with the RI provider it has a business relationship with prior to establishment of an N32 connection. Each modification policy applies to one individual relation between PLMN-operator and RI provider. To cover the whole N32 connection, both involved roaming partners shall exchange their modification policies.

NOTE 1: In order to validate modifications for messages received on the N32-f interface, the operator’s roaming partners will have to know the overall modification policy, e.g., via an API that support authentication and authorization.

NOTE 2: Modification includes removal and addition of new IE. IEs therefore may not be present in the rewritten message.

The IEs that the RI is allowed to modify shall be specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP. Wildcards may be used to specify paths.

This policy shall be specific per roaming partner and per RI provider that is used for the specific roaming partner.

The modification policy shall reside in the SEPP.

For each roaming parter, the SEPP shall be able to store a policy for receiving.

The following basic validation rules shall always be applied irrespective of the policy exchanged between two roaming partners:

- IEs requiring encryption shall not be inserted at a different location in the JSON object.

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