**3GPP TSG-SA3 Meeting #123 S3-252590-r1**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | 33.501 | **CR** | Draft-CR | **rev** |  | **Current version:** | 19.3.0 |  |
|  | | | | | | | | |
| *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:*** | PRINS Refinement | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CableLabs, Nokia, Charter Communications, China Telecom, Deutsche Telekom, Comcast Communications | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | DUMMY | | | | |  | ***Date:*** | | | 2025-07-30 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | 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 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. Allowing some parameters exchanged in N32-c procedures (e.g., protection policy) that are relevant to RIs to be sent over N32-f. Note that clause 13.2.2.3 of TS 33.501 already allows error messages to be sent over N32-f if they are relevant to RIs.  3. 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:*** | | 5.9.3.2a, 13.1.2, 13.2.2.2, 13.2.3.4, 13.2.3.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* 1st Change \* \* \* \*

#### 5.9.3.2a Support for Messages generated by Roaming Intermediaries

A PLMN SEPP that makes use of Roaming Intermediaries shall be able to handle error messages generated by Roaming Intermediaries, delivered over the N32 connection.

The following error messages relevant to Roaming Hub shall be supported,

- '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'.

The mechanism used for setting up N32-c via a chain of Roaming Intermediaries shall contain sufficient information such that a) the Roaming Intermediaries can determine the identities of the initiating and target PLMN in order to make authorization decision, b) the Roaming Intermediaries can authenticate the initiating PLMN, and c) the initiating PLMN and the target PLMN can authenticate each other.

NOTE 1: The Roaming Intermediary can reject the N32-c connection if no roaming relation exists. In this case, the expected error is "the N32 connection cannot be setup due to contractual reasons".

Additionally, it shall be possible for the Roaming Hubs to generate application layer control plane messages in order to reject traffic. Application layer control plane messages may be generated by the Roaming Hubs in order to reject registration attempts (refer to TS 23.502 [8] clause 4.2.2.2), to terminate sessions (see TS 23.502 [8] clause 4.3.4.3) and/or deregister the UE (refer to TS 23.502 [8] clause 4.2.2.3.3) and shall be sent using the corresponding NF Service operation to the NF, when relevant decisions are enforced by the Roaming Hub.

In this case, such messages are transparent to the SEPP and the SEPP shall act on them as any other message on the N32-f interface not making use of Roaming Intermediaries. How the SEPP authorizes such messages is left to implementation.

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

\* \* \* 2nd 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 3gpp-Connect-Req-Info header in the HTTP CONNECT request message and the 3gpp-Connect-Res-Info header in the HTTP CONNECT response message shall support integrity protection and replay protection.

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 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 3: In HTTPS mutual authentication, how an RI authenticates PLMN SEPP or another RI is not specified in 3GPP.

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 2nd Change \* \* \* \*

\* \* \* 3rd Change \* \* \* \*

### 13.2.2 N32-c connection between SEPPs

#### 13.2.2.1 General

When the negotiated security mechanism to use over N32, according to the procedure in clause 13.5, is PRINS (described in clause 13.2), the SEPPs use the established TLS connection (henceforth referred to as N32-c connection) to negotiate the N32-f specific associated security configuration parameters required to enforce application layer security on HTTP messages exchanged between the SEPPs. A second N32-c connection is established by the receiving SEPP to enable it to not only receive but also send HTTP Requests.

The N32-c connection is used for the following purposes:

- Key agreement: The SEPPs independently export keying material associated with the first N32-c connection between them and use it as the pre-shared key for generating the shared session key required.

- Parameter exchange: The SEPPs exchange security related configuration parameters that they need to protect HTTP messages exchanged between the two Network Functions (NF) in their respective networks.

- Error handling: The receiving SEPP sends an error signalling message to the peer SEPP when it detects an error on the N32-f interface.

~~If the exchanged parameters such as protection policy or security profile are relevant for the Roaming intermediaries, they shall be sent over N32-f to the peer SEPP.~~

The following security related configuration parameters may be exchanged between the two SEPPs:

a. Modification policy. A modification policy, as specified in clause 13.2.3.4, indicates which IEs can be modified by a Roaming Intermediary (RI) of the sending SEPP.

b. Data-type encryption policy. A data-type encryption policy, as specified in 13.2.3.2, indicates which types of data will be encrypted by the sending SEPP.

c. Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.

d. N32-f context ID. As specified in clause 13.2.2.4.1, N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

#### 13.2.2.2 Procedure for Key agreement and Parameter exchange

1. The two SEPPs shall perform the following cipher suite negotiation to agree on a cipher suite to use for protecting NF service related signalling over N32-f.

1a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s supported cipher suites. The cipher suites shall be ordered in initiating SEPP’s priority order. The SEPP shall provide an initiating SEPP’s N32-f context ID for the responding SEPP.

1b. The responding SEPP shall compare the received cipher suites to its own supported cipher suites and shall select, based on its local policy, a cipher suite, which is supported by both initiating SEPP and responding SEPP.

1c. The responding SEPP shall send a Security Parameter Exchange Response message to the initiating SEPP including the selected cipher suite for protecting the NF service-related signalling over N32. The responding SEPP shall provide a responding SEPP’s N32-f context ID for the initiating SEPP.

2. The two SEPPs may perform the following exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store protection policies sent by the peer SEPP.

2a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP’s Data-type encryption policies, as described in clause 13.2.3.2, and Modification policies, as described in clause 13.2.3.4.

2b. The responding SEPP shall store the policies if sent by the initiating SEPP.

2c. The responding SEPP shall send a Security Parameter Negotiation Response message to the initiating SEPP with the responding SEPP’s suite of protection policies.

2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP.

Alternatively to exchanging complete policies in steps 2a and 2c, the SEPPs may indicate a security profile.

NOTE: A security profile can for example include default modification policies and default data\_type encryption policies and/or a list of IEs to be protected, during the N32-c negotiation process. PRINS security profile specification is out of scope in 3GPP.

If the exchanged protection policy or security profile are relevant for the Roaming intermediaries, they shall be sent over N32-f to the responding SEPP.

3. The two SEPPs shall exchange Roaming Intermediary (RI) security information lists that contain information on RI public keys or certificates that are needed to verify RI modifications at the receiving SEPP.

4. The two SEPPs shall export keying material from the TLS session established between them using the TLS export function. For TLS 1.2, the exporter specified in RFC 5705 [61] shall be used. For TLS 1.3, the exporter described in section 7.5 of RFC 8446 [60] shall be used. The exported key shall be used as the master key to derive session keys and IVs for the N32-f context as specified in clause 13.2.4.4.1.

5. When the responding SEPP needs to initiate traffic, e.g., error reporting, in the reverse direction to the sending SEPP, the responding SEPP in the first N32-c connection shall now setup a second N32-c connection by establishing a mutually authenticated TLS connection with the peer SEPP.

NOTE: The second N32-c connection setup by the responding SEPP does not perform the negotiation of steps 1-4.

6. The two SEPPs start exchanging NF to NF service-related signalling over N32-f and tear down the N32-c connection. The SEPPs may initiate new N32-c TLS sessions for any further N32-c communication that may occur over time while application layer security is applied to N32-f.

\* \* \* End of 3rd Change \* \* \* \*

\* \* \* 4th 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

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.

#### 13.2.3.5 Provisioning of the policies in the SEPP

The SEPP shall contain an interface that the operator can use to manually configure the protection policies in the SEPP.

The SEPP shall be able to store and process the following policies for outgoing messages:

- A generic data-type encryption policy;

- Roaming partner specific data-type encryption policies that will take precedence over a generic data-type encryption policy if present;

- NF API data-type placement mappings;

- Multiple modification policies, to handle modifications that are specific per RI provider and modification policies that are specific per RI provider and roaming partner.

The SEPP shall also be able to store and process the following policies for incoming messages during the initial connection establishment via N32-c:

- Roaming partner specific data-type encryption policies;

- Roaming partner specific modification policies that specify which fields can be modified by which of its RI providers.

\* \* \* End of 4th Change \* \* \* \*

\* \* \* 5th Change \* \* \* \*

#### 13.2.3.6 Precedence of policies in the SEPP

This clause specifies the order of precedence of data-type encryption policies and modification policies available in a SEPP.

In increasing order of precedence, the following policies apply for a message to be sent on N32:

1. The set of default rules specified in the present specification:

- For the data-type encryption policy, the rules on data-types that are mandatory to be encrypted according to clause 5.9.3.3.

- For the modification policy, the basic validation rules defined in clause 13.2.3.4.

2. Manually configured policies:

- For the data-type encryption policy: rules according to clause 13.2.3.2, on a per roaming partner basis.

- For the modification policy: rules according to clause 13.2.3.4, per roaming partner and per RI provider that is used for the specific roaming partner.

NOTE 1: It is assumed that operators agree both data-type encryption and modification policy in advance, for example as part of their bilateral roaming agreement. The protection policies exchanged via N32-c during the initial connection establishment only serve the purpose of detecting possible misconfigurations.

NOTE 2: It is assumed that the default rules and manually configured policies do not overlap or contradict each other. The manually configured policies are used to extend the protection by the default rules in the present document and are applied on top of them.

When a SEPP receives a data-type encryption or modification policy on N32-c or N32-f as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and RI provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy:

- Send the error message as specified in TS 29.573 [73], clause 6.1.4.3.2, to the peer SEPP.

- Create a local warning.

\* \* \* End of 5th Change \* \* \* \*