**3GPP TSG-SA3 Meeting #124 draft\_S3-253445-r9**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **2191** | **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:*** | Procedure to making some security parameters visible to RIs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, CableLabs, China Mobile | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | RefinePRINS | | | | |  | ***Date:*** | | | 2025-10-13 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | It was agreed in the Objective of the new WID that some security parameters that are relevant to RIs should be made visible to RIs. A solution is proposed to solve this problem. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding follwing procedures to make some security parameters visible to RIs:  1. Requirement of exchanging the security parameters visible to RIs is included.  2. The procedure to send some security parameters to RIs is also introduced, i.e, basically reusing the procedure in clause 13.2.4, with the requirement that the security parameters shall not be encrypted. How to determine which security parameters and when to send security parameters are also introduced. Note that since in clause 13.2.4, the IEs in the N32-f message that are not encrypted will be integrity protected in clearTextEncapsulationMessage, extra definition of integrity protection of security parameters is not needed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | RIs fail to receive security parameters. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.2.2.2, 13.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

#### 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.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.

After the N32-c handshake procedure, the initiating SEPP shall determine the security parameters (defined in clause 13.2.2.1) visible to the RI based on the contract with its RI, and then include the security parameters IE in cleartext in the N32-f request message to its RI. The responding SEPP will do the same thing when it responds to the initiating SEPP.

\*\*\* 2nd CHANGE \*\*\*

### 13.2.4 N32-f connection between SEPPs

#### 13.2.4.1 General

The SEPP receives HTTP/2 request/response messages from the Network Function. SEPP may initiate message sent over N32-f. It shall perform the following actions on messages received from a Network Function before they are sent on the N32-f interface to the SEPP in the other PLMN:

a) It parses the incoming message and, if present, rewrites the telescopic FQDN of the receiving NF to obtain the original FQDN as described in clause 13.1.

b) It reformats the message to produce the input to JSON Web Encryption (JWE) [59] as described in clause 13.2.4.3.

c) It applies JWE to the input created in b) to protect the reformatted message as described in clause 13.2.4.4.

d) It encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message) and sends the HTTP/2 message to the SEPP in the other PLMN over the N32-f interface.

The message may be routed via the one or two Roaming Intermediaries, e.g., cIPX and pIPX. These RIs may modify messages as follows:

a) The RI recovers the cleartext part of the HTTP message from the JWE object, modifies it according to the modification policy, and calculates an "operations" JSON Patch object. It then creates a temporary JSON object with the "operators" JSON Patch object and some other parameters for replay protection etc. as described in clause 13.2.4.5.1.

b) The RI uses the temporary JSON object as input into JSON Web Signature (JWS) [45] to create a JWS object, as described in clause 13.2.4.5.2.

c) The RI appends the JWS object to the received message and sends it to the next hop.

The JWS objects generated by the two RI providers form an auditable chain of modifications that to the receiving SEPP shall apply to the parsed message after verifying that the patches conform to the modification policy.

Encryption of IEs shall take place end to end between cSEPP and pSEPP.

A SEPP shall not include IEs in the clear that are encrypted elsewhere in the JSON object.

A SEPP shall verify that an intermediate RI has not moved or copied an encrypted IE to a location that would be reflected from the producer NF in an IE without encryption.

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