**3GPP TSG-SA3 Meeting #116 *draft\_S3-242458-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **4** | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | Roaming5G | | | | |  | ***Date:*** | | | 2024-05-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | C4-240834 was agreed to allow for SecParamExchReqData to negotiate  secProfiles. When present, this IE shall indicate the candidate list of security profiles that the initiating SEPP is supporting for PRINS.  To align 33.501 with 29.573 it is proposed to remove the example of cipher suite negotiation, because because jwe/jwsCipherSuiteList is already existing at this point.  -r1 moves the rest of the text related to security profiles to the section on N32-c negotiation for the parameter exchange. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Remove the example of pre-selected cipher suites and shifts the text to the respective clause. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Creating confusion since it is not possible to select the cipher suite in this step anymore. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.2.2.2, 13.5. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | ***S3-241862*** | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

#### 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, the SEPP 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.

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

## 13.5 Security capability negotiation between SEPPs

The security capability negotiation over N32-c allows the SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32-f. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service-related signalling over N32-f.

When a SEPP notices that it does not have an agreed security mechanism for N32-f protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP over N32-c in order to determine, which security mechanism to use for protecting NF service-related signalling over N32-f. Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32-c. The TLS connection shall provide integrity, confidentiality and replay protection.



Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection shall issue a POST request to the exchange-capability resource of the responding SEPP including the initiating SEPP’s supported security mechanisms for protecting the NF service-related signalling over N32-f (see Table 13.5-1). The security mechanisms shall be ordered in the initiating SEPP’s priority order.

2. The responding SEPP shall compare the received security capabilities to its own supported security capabilities and selects, based on its local policy (e.g. based on whether there are IPX providers on the path between the SEPPs), a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP shall respond to the initiating SEPP with the selected security mechanism for protecting the NF service-related signalling over N32.

Table 13.5-1: NF service-related signalling traffic protection mechanisms over N32

|  |  |
| --- | --- |
| N32-f protection mechanism | Description |
| Mechanism 1 | PRINS (described in clause 13.2) |
| Mechanism 2 | TLS |
| Mechanism n | Reserved |

If the selected security mechanism is PRINS, the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is TLS, the SEPPs shall behave as specified in clause 13.1.2, tear down the N32-c connection and forward the NF service-related signalling over N32-f using a TLS connection.

If the selected security mechanism is a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the N32-c TLS connection.

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