**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220067-r1***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** |  | **rev** | **-** | **Current version:** | **2** |  |
|  |
| *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:***  | Clarification when the responder SEPP establish a second N32-C connection |
|  |  |
| ***Source to WG:*** | Mavenir, Nokia, Nokia Shanghai Lab |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2022-02-14 |
|  |  |  |  |  |
| ***Category:*** |  **A** |  | ***Release:*** | Rel-17 |
|  | *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:*** | The current text in TS33.501 is not clear and confusion may be generated whether new cipher suite is being negotiated whe the responder start the stablishment of the second N32-c connection.Further, the reverse N32-c connection is only established when needed; “now” is creating further confusion. |
|  |  |
| ***Summary of change:*** | The revers N32-c connection is established as needed and “now’ is deleted in clause 13.2.2.2. Adding a NOTE to indicate that when the corresponding SEPP setup a second N32-c connection, it uses the already negotiated cipher suite and other parametrs that have been negotiated duing the first N32-c connection. In other words, it does not repeate steps 1-4. |
|  |  |
| ***Consequences if not approved:*** | Propable misinterpretation that could lead to Interoperability issues between different implemntations. |
|  |  |
| ***Clauses affected:*** | 13.2.2.2 |
|  |  |
|  | **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 Change No. 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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.

3. The two SEPPs shall exchange IPX security information lists that contain information on IPX public keys or certificates that are needed to verify IPX 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 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 may keep the TLS session open for:

- any further N32-c communication that may occur over time while application layer security is applied to N32-f, or

- any further N32-c and N32-f communication, if TLS is used to protect N32-f.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change No. 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*