**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220728-r2***

**e-meeting, 16 - 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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:***  | Clarification on N32-f connection establishment with TLS |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2022-05-20 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-16 |
|  | *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 proposed CR aims to clarify an implicit security requirement related to N32-c and N32-f correlation, pointed out by CT4 in CR C4-221541 and agreed in Feb 2022, TSG-CT WG4 Meeting #108-e:‘This CR was postponed at the Aug 2021 105e CT4 meeting because we found an issue with N32c and N32f correlation. At that time, the correlation was not possible because the SEPP TLS profile was not defined in the standards. Recently, SA3 has agreed on the CR: 'S3-214440 Certificate profile for SCP and SEPP", which defines the SEPP TLS profile. And this TLS SEPP profile may contain a Subject DN as 'PLMN ID'. So this PLMN ID can be used for correlation and the correlation problem will be solved.’Using the PLMN-ID of the SEPP TLS profile information, the correlation between a PLMN ID specific N32-c connection and its related N32-f connection can be achieved. . |
|  |  |
| ***Summary of change:*** | Adding a paragraph for clarification on N32-c and N32-f correlation after agreement of SA3 CR S3-214440. |
|  |  |
| ***Consequences if not approved:*** | Ambigiouty in specification text |
|  |  |
| ***Clauses affected:*** | 13.1.2 |
|  |  |
|  | **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:*** | S3-220728 |

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

13.1.2 Protection between SEPPs

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

If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. If there are IPX providers 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 by comparing the PLMN-IDs contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections.

If there are IPX providers 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 used on the N32-f interface, one of the following additional transport protection methods should be applied between SEPP and IPX provider 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 7540 [47].

NOTE 1: Void

NOTE 2: Void.

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