**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211759-r2***

**e-meeting, 17 - 28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | 33.501 | **CR** |  | **rev** |  | **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:*** | **Clarify the usage of TLS and PRINS between SEPPs** | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2021-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | Clarify the usage of TLS and PRINS between SEPPs which is motivated by GSMA's directions in the LS S3-211446: "Clarify whether the negotiation of direct TLS connection on N32-f between the SEPPs of the roaming partners is allowed by 3GPP specifications.". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that TLS or PRINS may be used between SEPPs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Inflexibility for the choice of security protocol on N32. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

### \*\*\* BEGIN CHANGES \*\*\*

## 13.1 Protection at the network or transport layer

All network functions shall support TLS. Network functions shall support both server-side and client-side certificates.

The TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [3] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

TLS shall be used for transport protection within a PLMN unless network security is provided by other means.

NOTE 1: Regardless of whether TLS is used or not, NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5] can be used for network layer protection.

NOTE 2: If interfaces are trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to use cryptographic protection.

To allow for TLS protection between the SEPP and Network Functions within a PLMN, the SEPP shall support TLS wildcard certificate for its domain name and generation of telescopic FQDN based on an FQDN obtained from the received N32-f message.

A telescopic FQDN is an FQDN with a single label as the first element and the SEPP’s domain as the trailer component. The label uniquely represents the original FQDN.

NOTE 3: The structure of telescopic FQDN is defined in 3GPP TS 23.003 [19], clause 28.5.2.

The SEPP shall generate a telescopic FQDN for the following messages received over N32-f:

a. Nnrf\_NFDiscovery\_Get response HTTP message with FQDNs of a set of the discovered NF or NF service instance(s) (cf. TS 29.510). The cSEPP generates a telescopic FQDN for each target Network Function FQDN in the Discovery response, rewrites the original FQDN with the telescopic FQDN and forwards the modified Discovery response to the NRF.

b. Subscription message with the Callback URI in the payload of the message (cf. TS 29.501). The pSEPP generates a telescopic FQDN from the Callback URI in the Subscription message, rewrites the original FQDN in the callback URI, and forwards the modified Subscription message to the producer Network Function.

c. Nsmf\_PDUSession\_POST HTTP message from a V-SMF with PduSessionCreateData containing the URI representing the PDU session in the V-SMF (cf. TS 29.502). The pSEPP generates a telescopic FQDN from the Callback URI in the message, rewrites the original FQDN in the callback URI, and forwards the modified message to the target H-SMF.

The following procedure illustrates how SEPPs use telescopic FQDN and wildcard certificate to establish a TLS connection between a Network Function and the SEPP:

1. When the SEPP receives one of the messages identified in a-c above, it shall rewrite the FQDN from the received message with a telescopic FQDN and forwards the modified HTTP message to the target Network Function inside the PLMN.

2. When the Network Function that received the telescopic FQDN in step 1 is ready to communicate with the target Network Function in another PLMN, it uses the telescopic FQDN in the Request URI of the HTTP Request. During TLS setup between the Network Function and the SEPP, the SEPP shall authenticate towards the Network Function using the wildcard certificate.

3. When the SEPP receives a HTTP request from the Network Function, the SEPP shall rewrite the telescopic FQDN with the original FQDN by replacing the unique delimiter in the label with the period character and removing its own suffix part.

If there are no IPX providers between SEPPs, TLS shall be used between the SEPPs. If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security on the N32-f interface) shall be used for protection between the SEPPs. If there are IPX providers which offer other services in addition to IP routing between SEPPs, PRINS shall be used for protection between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

NOTE 3: 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, following the profile given in clause 6.2 of TS 33.210 [3], with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

NOTE 4: Void

NOTE 5: Void.

### \*\*\* END CHANGES \*\*\*