**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220954-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **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:*** | Clarification of SNI usage for NF clients and servers | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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 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:*** | | RFC 7540, "Hypertext Transfer Protocol Version 2 (HTTP/2)", clause 9.2 states: "The TLS implementation MUST support the Server Name Indication (SNI) [TLS-EXT] extension to TLS."  It is however not clear how the "support" shall be interpreted. What does the NFc need to support? Can the SNI field be empty in the NFc or must it be used? | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Client NFs shall include the SNI field in the TLS profile.  For server NFs it is a vendor decision how to use it. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Services may be failing when the server is expecting an SNI and it is not sent by the client. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 13.1.0 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## \*\*\*\*\*\*\* FIRST CHANGE \*\*\*\*\*\*\*\*\*\*\*\*

### 13.1.0 General

All network functions shall support mutually authenticated TLS and HTTPS as specified in RFC 7540 [47] and RFC 2818 [90]. The identities in the end entity certificates shall be used for authentication and policy checks. Network functions shall support both server-side and client-side certificates. TLS client and server certificates shall be compliant with the SBA certificate profile specified in clause 6.1.3c of TS 33.310 [5].

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 clients shall include the SNI extension as specified in RFC 7540 [47], see also TS 33.210 [3] clause 6.2 and TS 33.310 [5] clause 6.1.3c.3.

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.

NOTE X: It is a vendor implementation decision how the SNI extension is being used in TLS servers.

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