**3GPP TSG-SA3 Meeting #114e *ad-hoc draft\_S3-240054-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.117** | **CR** | **0167** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Remove the additional can in the evidence | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei; HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph3 | | | | |  | ***Date:*** | | | 2024-01-22 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Delete “can” in “**Expected can Results”** | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Delete “can” in “**Expected can Results”** | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The meanning is unclear, or all other “Expected Results” have to be changed to “Expected can Results” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

 \*\*\*\*\*\*\*\*\*\*\*\*\* 1st of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.*2*.2 Protection at the transport layer

*Requirement Name:* Protection at the transport layer

*Requirement Reference:* TS 33.501 [10], clause 5.9.2.1, clause 13.1, clause 13.3.2

*Requirement Description*:

NF Service Request and Response procedure supports mutual authentication between NF consumer and NF producer as specified in TS 33.501 [10], clause 5.9.2.1 .

All network functions support TLS. Network functions support both server-side and client-side certificates. The TLS profile follows the profile given in Annex E of TS 33.310 [9] with the restriction to be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11] as specified in TS 33.501 [10], clause 13.1.

Authentication between network functions within one PLMN uses one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution is used for authentication between NFs as specified in TS 33.501 [10], clause 13.3.2.

*Threat References*: TR 33.926 [4], clause 5.3.6.3, Weak cryptographic algorithms

*Test case*:

**Test Name:** TC\_PROTECT\_TRANSPORT\_LAYER

**Purpose:**

Verify that TLS protocol for NF mutual authentication and NF transport layer protection is implemented in the network products based on the profile required.

**Procedure and execution steps:**

**Pre-Conditions:**

Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the profile defined by 3GPP in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11].

**Execution Steps**

1. The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.

2. The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test.

3. The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile.

**Expected Results:**

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the profile requirements in TS 33.310 [9] Annex E and RFC 7540 [11].

- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in TS 33.310 [9] Annex E or RFC 7540 [11].

**Expected format of evidence:**

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change\*\*\*\*\*\*\*\*\*\*\*\*\*