**3GPP TSG-SA3 Meeting #108-e *S3-222390***

**e-meeting, 22nd – 26th August, 2022 Revision of S3-22xxxx**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **draft-CR** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | Living document to TS 33.117 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** |  2022-08-22 |
|  |  |  |  |  |
| ***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 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:*** | According to the test case in clause 4.2.3.2.4 of TS 33.117, it is unclear whether the security profile is the same as it in the product documentation. In order to make sure the network element support the exact security profile including correct protocol versions and combinations of cryptographic algorithms etc. in the product document, it’s proposed to clarify it in the execution steps.  |
|  |  |
| ***Summary of change:*** | Add clarification to avoid unsecure profile. |
|  |  |
| ***Consequences if not approved:*** | Test case is incomplete. |
|  |  |
| ***Clauses affected:*** | 4.2.3.2.4 |
|  |  |
|  | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*.

##### 4.2.3.2.4 Protecting data and information in transfer

*Requirement Name*: tba

*Requirement Description*:

- Usage of cryptographically protected network protocols is required.

- The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.

*Security Objective references*: tba

*Test case*:

**Test Name:** TC\_PROTECT\_DATA\_INFO\_TRANSFER\_1

**Purpose:**

Verify the mechanisms implemented to protect data and information in transfer to and from the Network Product's OAM interface.

NOTE: The test is limited to the OAM interface although the requirement does not have this limitation because the protection of standardised interfaces will be covered by regular interoperability testing and the proprietary use of HTTPS is covered in clause 4.2.5.1.

**Procedure and execution steps:**

**Pre-Conditions:**

Network product documentation containing information about supported OAM protocols is provided by the vendor,

A peer implementing the security protocol configured by the vendor (e.g SSH client supporting SSHv2 or HTTPS client) shall be available.

Network product documentation stating which security protocols for protection of data in transit are implemented and which profiles in TS 33.310 [9] and TS 33.210 [15] are applicable is provided by the vendor

For TLS/DTLS, the tester shall base the tests on the profile defined by 3GPP in TS 33.310 [9] and TS 33.210 [15]. For IKE and IPsec, the tester shall base the tests on the profile defined by 3GPP in TS 33.210 [15]. For protocols, for which 3GPP did not define a security profile, e.g. SSH, the tester shall base the tests on a widely recognised and publicly available security profile.

**Execution Steps**

1. The tester shall check that compliance with the selected security profile can be inferred from detailed provisions in the product documentation.
2. The tester shall check that the default security parameters are the same as those stated in the product documentation.

3. The tester shall establish a secure connection between the network product and the peer and verify that all protocol versions and combinations of cryptographic algorithms that are mandated by the security profile are supported by the network product and the network product does not use the deprecated or unsecure protocol versions and algorithms .

4. The tester shall try to establish a secure connection between the network product 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 security profile.

**Expected Results:**

The traffic is properly protected, and insecure options are not accepted by the Network Product.

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