**3GPP TSG-SA3 Meeting #116 *S3-242328***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.511** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **18.3.0** |  |
|  | | | | | | | | |
| *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:*** | New test for peer certificate checking at gNB | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei; HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Maint | | | | |  | ***Date:*** | | | 2024-05-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | Addition of a new test for peer certificate checking that corresponds to a new threat introduced in a parallel contribution S3-242329 to the gNB network product class annex in TR 33.926. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a new test case for peer certificate checking by gNB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete SCAS coverage of certificate related functionality. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.1.x(new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[4] Void

[5] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[6] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

[7] 3GPP TS 23.501: "System Architecture for 5G System (5GS)".

[8] 3GPP TS 38.300: "NR and NG-RAN Overall Description".

[9] 3GPP TS 33.523: "5G Security Assurance Specification (SCAS); split gNB product classes".

[x] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

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

##### \*\*\*\*\*\*\*\*\*\*\*\*\* 2nd of Change\*\*\*\*\*\*\*\*\*\*\*\*\*4.2.2.1.x Peer certificate checking

*Requirement Name:* Peer certificate checking at base station

*Requirement Reference:* In accordance with industry best practice

*Requirement Description*:

The gNB is expected to support some capability for checking the validity of communication peer's certificates.

*Test case*:

**Test Name:** TC\_PEER\_CERT\_CHCK

**Purpose:**

Verify that the gNB can check the peer certificate is valid or not.

**Procedure and execution steps:**

**Pre-Conditions:**

- If the gNB under test does not support handling certificates as defined in TS 33.310[x], this test does not apply.

- The gNB that does the verification is configured with a root CA.

- The gNB network product shall be connected in emulated/real network environments.

- A peer, e.g. AMF, SEG, gNB may be emulated.

NOTE: according to 5GS, only AMF, SEG/UPF, gNB can connect to a gNB. The peer means the network funcation that provides the operator certificate to the gNB for establishing the N2, N3, Xn interfaces.

- The gNB is configured the necessary information to connect with the peer.

**Execution Steps:**

1. The tester configures the peer with the invalid certificate, e.g. expired certificate, wrong signature.

2. The tester triggers the gNB to connect to the peer.

3. The peer providing the operator certificate to the gNB.

4. The gNB verifies the trust chain of operator certificate.

**Expected Results:**

- The gNB does not establish a connection and may raise an alarm that the peer certificate is invalid.

**Expected format of evidence:**

The logs and the communication flow in a .pcap file.

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