**3GPP TSG-SA3 Meeting #118 S3-244505**

**Hyderabad, India, 14th - 18th October 2024  *is the revision of S3-243988***

|  |
| --- |
| *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:***  | Living document to Draft CR TS 33.511 |
|  |  |
| ***Source to WG:*** | Huawei; HiSilicon, CAICT, CTCC, Nokia, |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Maint |  | ***Date:*** | 2024-08-17 |
|  |  |  |  |  |
| ***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 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:*** | Addition of new testcases related to the threat of certificate expiry and peer certificate checking to the gNB network product class. |
|  |  |
| ***Summary of change:*** | Addition of a new testcase for certificate expiry checking by gNB. |
|  |  |
| ***Consequences if not approved:*** | Incomplete SCAS coverage of the certificate enrolment functionality. |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.x(new), 4.2.2.1.y(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)".

[Y] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol".

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

 \*\*\*\*\*\*\*\*\*\*\*\*\* 2nd of Change\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.x Checking expiry certificate

*Requirement Name:* Expired Certificate checking at base station

*Requirement Reference:* TS 33.310 [x], clause 7.2

*Requirement Description*:

Certificate Management Protocol v2 (CMPv2) [Y] may be the supported protocol to provide certificate lifecycle management capabilities for TLS entities. All TLS entities and TLS CAs may support initial enrolment by the TLS entity to the TLS CA via CMPv2, i.e. receiving a certificate from the TLS CA, and updating the key of the certificate via CMPv2 before the certificate expires.

*Threat References*: TBD

*Test case*:

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

**Purpose:**

Verify that the gNB can check whether its certificate issued by operator CA is about to expire and to act accordingly.

**Pre-Conditions:`**

- If the gNB under test does not support handling certificates as defined in clause 9 of TS 33.310[x], this test does not apply.

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

- A TLS CA may be emulated, if needed.

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

- Optionally, the vendor may provide necessary informationin a document, e.g. describing how to handle the case when a gNB checks the operator certificate is about to be expired.

**Execution Steps**

1. The tester configures the gNB with certificates that is assigned by operator CA.

2. The tester configures the UTC timer of gNB to the time when its own certificate is about to be expired.

3. The gNB initiates the CMPv2 procedure to get the new operator certificate.

**Expected Results:**

- The gNB raises an alarm or requests a new certificate from the CA.

- The gNB received a new operator certificate.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change\*\*\*\*\*\*\*\*\*\*\*\*\*

#####  \*\*\*\*\*\*\*\*\*\*\*\*\* 3rd of Change\*\*\*\*\*\*\*\*\*\*\*\*\*4.2.2.1.y Peer certificate checking

*Requirement Name:* Peer certificate checking at base station

*Requirement Reference:* TS 33.310 [x], clause 9.5.1

*Requirement Description*:

- The base station may be pre-provisioned with the operator root CA certificate.

- If the base station is not pre-provisioned with the operator root CA certificate, then the base station takes the operator root certificate from the certificates received in the initialization response. The selection is based on checking which root certificate can be used to validate the received base station certificate.

NOTE1: Examples on validation factors defined in clause 6.3.1 of TS 33.310[x] can be taken into consideration, for example, whether the certificated has been revoked, expired, on the CRL distribution point is empty, etc.

*Test case*:

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

**Purpose:**

Verify that the gNB has the ability to check the peer certificate is valid or not.

**Pre-Conditions:**

- If the gNB under test does not support handling certificates as defined in clause 9 of TS 33.310[x], this test does not apply.

- The gNB is configured with or has obtained an operator root CA certificate.

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

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

NOTE2: according to 5GS, only AMF, SEG/UPF, gNB can connect to a gNB. The peer means the network function that provides the operator assigned certificate to the gNB for establishing the N2, N3, Xn interfaces.

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

- Optionally, the vendor may provide necessary informationin a document, e.g., describing the checking factors and how to handle the case when a gNB validate the certificate is invalid.

**Execution Steps:**

1. The tester configures the peer with an invalid certificate e.g., by using a wrong signature or a certificate that has expired.

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

**Expected Results:**

- The gNB does not connect with the peer and may raise an alarm at the same time.

**Expected format of evidence:**

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

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