3GPP TSG-SA3 Meeting #116 draft\_S3-242384

Jeju, Korea 20 - 24 May 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.310** | **CR** | **0199** | **rev** | **2** | **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 | **x** |

|  |
| --- |
|  |
| ***Title:***  | Correction to validation of usage of X.509 certificate procedure |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson, Johns Hopkins University APL, Cisco |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | ACM\_SBA |  | ***Date:*** | 2024-05-13 |
|  |  |  |  |  |
| ***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:*** | Removal of the NOTE in clause 10.4 as per publication of new IETF RFC 9509, thus no explanation of the earlier draft RFC is needed. Clarification of the requirements in clause 10.4 of TS 33.310. Update of references.  |
|  |  |
| ***Summary of change:*** | Removal of NOTE in clause 10.4. Reformulation of the paragraph introduced in SP-231325 and updates of references to IETF RFC 9509.  |
|  |  |
| ***Consequences if not approved:*** | 33.310 would reference an obsolete draft RFC, and if the RFC reference is updated, then the associated note would be irrelevant.  |
|  |  |
| ***Clauses affected:*** | 2, 10.4 |
|  |  |
|  | **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:*** | S3-240583, S3-240993 |

**\*\*\* START OF FIRST 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 TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[2] IETF RFC 2986: "PKCS#10 Certification Request Syntax Specification Version 1.7".

[3] Void.

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

[5] IETF RFC 2252: "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions".

[6] Void.

[7] "PKI basics – A Technical Perspective", November 2002, <http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf>.

[8] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[9] 3GPP TS 33.203: "Access security for IP-based services".

[10] 3GPP TS 33.220: "Generic Authentication Architecture: Generic Bootstrapping Architecture".

[11] Void.

[12] Void.

[13] Void.

[14] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[15] IETF RFC 4945: "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX".

[16] Void.

[17] Void.

[18] IETF RFC 6712: "Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)".

[19] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

[20] IETF RFC 2818: "HTTP Over TLS".

[21] IETF RFC 5922: "Domain Certificates in the Session Initiation Protocol (SIP)".

[22] IETF RFC 5924: "Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates".

[23] Void.

[24] Void.

[25] IETF RFC 1035: "Domain Names - Implementation and Specification".

[26] Void.

[27] Void.

[28] Void.

[29] Void.

[30] Void.

[31] 3GPP TS 23.251: "Network sharing; Architecture and functional description".

[32] 3GPP TS 32.508: "Telecommunication management; Procedure flows for multi-vendor plug-and-play eNode B connection to the network".

[33] 3GPP TS 32.509: "Telecommunication management; Data formats for multi-vendor plug and play eNode B connection to the network".

[34] Void.

[35] Void.

[36] Void.

[37] Void.

[38] Void.

[39] Void.

[40] Void.

[41] Void.

[42] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[43] IETF RFC 7427: "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)".

[44] Void.

[45] Void.

[46] Void.

[47] IETF RFC 6960: " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[48] IETF RFC 8201: "Path MTU Discovery for IP version 6".

[49] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[50] IETF RFC 9113: "HTTP/2".

[51] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[52] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

[53] IETF RFC 7633: "X.509v3 Transport Layer Security (TLS) Feature Extension".

[54] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[55] 3GPP TS 23.003: "Numbering, addressing and identification".

[56] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[57] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[58] IETF RFC 6979: " Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)".

[59] CA-Browser-Forum-BR-1.8.0, August 2021, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.0.pdf>.

[60] GSMA FS.34 Key Management for 4G and 5G inter-PLMN Security, <https://www.gsma.com/security/resources/fs-34-key-management-for-4g-and-5g-inter-plmn-security/>.

[61] IETF RFC 9310: "X.509 Certificate Extension for 5G Network Function Types".

[62] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[63] IETF RFC 9509: "X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions".

[64] IETF RFC 4122:" A Universally Unique Identifier (UUID) URN Namespace".

**\*\*\*END OF FIRST CHANGE\*\*\***

**\*\*\* START OF SECOND CHANGE \*\*\***

## 10.4 Validation of usage of X.509 certificate

The 5G Core NFs in SBA may need to support multiple operator certificates for different purposes, such as TLS authentication, signing OAuth access tokens, or validating the JSON Web Signature in JSON Web Tokens (Client Credentials Assertion).

The Extended Key Usage (EKU) extension of the X.509 certificate as defined in IETF RFC 5280 [14] and IETF RFC 9509 [63] may be used to indicate the purpose of the X.509 certificates used in SBA. Accordingly, the CA is expected to be configured with policies to validate the purpose of the certificate and add it to the issued certificate, thus the usage of the certificate can be further verified in corresponding procedures (e.g., TLS authentication).

If the initial trust between the operator RA/CA and the NF, the options for which are listed in clause 10.2.2, is set up by an OAM certificate, then that OAM certificate may also include the EKU extension. If the initial trust is setup by OAM issued signature of certain NF profile parameters, these NF profile parameters may include the EKU extension. During the setup of initial trust procedure described in clause 10.2.3, the EKU extension may be used to indicate the usage of the end entity certificate that will be issued by the operator RA/CA. In that case, the operator RA/CA verifies that the EKU extension of the certificate enrolment request corresponds to that included in the initial trust before generating the final end entity certificate for the 5G Core NF.

NOTE: This clause does not preclude to use the X.509 certificate for different purposes. In that case, the EKU extension would have several values. Implementations can opt in to deploy a different certificate per each purpose, of one certificate with multiple purposes. This note applies to both initial trust (e.g., OAM certificate) and final end entity certificate for 5G Core NF.

**\*\*\* END OF SECOND CHANGE \*\*\***