**3GPP TSG-SA3 Meeting #116 *draft\_S3-242383-r3***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Johns Hopkins University APL, Cisco | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2024-05-13 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | The 5G Core NFs in SBA might need to support multiple operator certificates for different purposes. Accordingly, the SBA profile defined in clause 6.1.3c of TS 33.310 needs to be updated to ensure the certificates include the information about the purpose to be validated as indicated in clause 10.4 of TS 33.310.  IETF RFC 9509 has been published in March 2024, thus the existing references to draft-ietf-lamps-nf-eku should be updated with the new RFC.  RFC 6125 has been obsoleted by IETF and should be updated with RFC 9525. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The change updates the SBA certificate profile as defined in TS 33.310 to include additional purposes of the 5GC NFs in SBA, namely certificates for use in OAuth and CCA (JWT based authentication).  Update to remove obsolete references. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The usage of the X.509 certificates in 5G Core NFs cannot be validated if the information on the purpose of the certificate is not present.  Obsoleted references would be present in 3GPP TS 33.310. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 6.1.3c | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3-234550, S3-240580 | | | | | | | | |

\* \* \* 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] Void

[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-2.0.4, April 2024, <https://cabforum.org/working-groups/server/baseline-requirements/documents/TLSBRv2.0.4.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".

[65] IETF RFC 9525: "Service Identity in TLS".

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

\* \* \* Second Change \* \* \* \*

### 6.1.3c SBA Certificate profiles

#### 6.1.3c.1 Introduction

Clause 6.1.3c profiles the certificates to be used for 5GC Service Based Architecture (SBA). Those end entity certificates may be used for the following purposes:

- TLS client and server certificates.

- Signing validation of OAuth tokens.

- Signing validation of CCA (JWT based authentication) tokens.

Different end entity certificate profile requirements may be applied to intra-domain and/or inter-domain SBA for NF producers, NF consumers and NRF instances, Service Communication Proxy (SCP) nodes, and Security Edge Protection Proxy (SEPP) nodes applicable to 3GPP 5GC roaming.

A separate end entity certificate profile is also needed to cover the usage of the certificates issued by the Interconnection CA(s) for inter-domain SBA context for TLS connections between SEPP nodes.

Furthermore, separate end entity certificate profile requirements may be applied for Service Communication Proxy (SCP) needed for 3GPP 5GC SBA Indirect Communication models C and D.

#### 6.1.3c.2 General SBA Certificate profile

The following additions and deviations to the common profiles shall hold for all SBA-related entities (NFs, SCPs, SEPPs):

- Signature algorithm: RSAEncryption need not be supported.

- ECDSA is recommended for end entity certificates in 5GC Service Based Architecture (SBA).

#### 6.1.3c.3 NF Certificate profile

End entity certificates shall be directly signed by the CA in the operator domain that the entity belongs to.

NOTE: RFC 9525 [64] describes guidelines and procedures for representing and verifying the identity of application service using X.509 PKIX certificates with TLS. The server identity can only be expressed in the subjectAltName extension; it is not valid to use CN-ID. Additionally, CA-browser forum [59] marks CN-ID as “NOT RECOMMENDED”, and it has the following requirement: if CN-ID is present, this field contains exactly one entry that is one of the values contained in the certificate’s subjectAltName extension.

In addition to clause 6.1.1 and the provisions of RFC 5280 [14], the following table captures the certificate profiles for NF TLS client and server:

Table 6.1.3c.3-1: NF TLS Client and Server Certificate Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NF TLS Client and Server Certificate Profile | | | | |
| Version | | v3 | | |
| Serial Number | | Unique Positive Integer in the context of the issuing Root CA and not longer than 20 octets. | | |
| Subject DN | | C=<Country>  O= Home Domain Name (e.g., in "5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" format) as defined in clause 28.2 of TS 23.003 [55]) | | |
| Validity Period | | 3 years or less | | |
| Signature | | See clause 6.1.1 for the list of supported signature algorithms. | | |
| Subject Public Key Info | | See clause 6.1.1 for the list of supported public key types. | | |
| Extensions | OID | Mandatory | Criticality | Value |
| keyUsage | {id-ce 15} | TRUE | TRUE | digitalSignature for TLS clients and servers |
|  |
| extendedKeyUsage | {id-ce 37} | TRUE | FALSE | id-kp-clientAuth TLS clients |
| id-kp-serverAuth for TLS servers  NF that may be both client and server shall have both OIDs set. |
| authorityKeyIdentifier | {id-ce 35} | TRUE | FALSE | This shall be the same as subjectKeyIdentifier of the Issuer’s certificate. CA shall utilitize the method (1) as defined in clause 4.2.1.2 of RFC 5280 [14] to generate the value for this extension. |
| subjectKeyIdentifier | {id-ce 14} | FALSE | FALSE | This shall be calculated by the issuing CA utilitizing the method (1) as defined in clause 4.2.1.2 of RFC 5280 [14] to generate the value for this extension. |
| cRLDistributionPoint | {id-ce 31} | TRUE | FALSE | distributionPoint  Ac cording to RFC 5280 [14] this indicates if the CRL is available for retrieval using access protocol and location with LDAP or HTTP URI. |
| subjectAltName | {id-ce 17} | TRUE | TRUE | Multiple subjectAltName entries can be used as a sequence, see below for the detailed instructions. |
| nfTypes | {id-pe 34} | TRUE | FALSE | id-pe-nftypes specified in RFC 9310 [61] enables including Network Function types (NFTypes) for the 5G System in X.509 v3 public key certificates. |
| authorityInfoAccess | {id-pe 1} | FALSE | FALSE | id-ad-caIssuers  According to RFC 5280 [14] id-ad-caIssuers describes the referenced description server and the access protocol and location, for example, using one or multiple HTTP and/or LDAP URIs. |
| id-ad-ocsp  According to RFC 5280 [14] id-ad-ocsp defines the location of the OCSP responder using HTTP URI. |
| TLS feature extension | {id-pe 24} | FALSE | FALSE | id-pe-tlsfeature  This can be used according to RFC 7633 [53] to prevent downgrade attacks that are not otherwise prevented by the TLS protocol; also to be used with OCSP stapling with TLS server end-entity certificates. |

With (intra-domain) SBA, the following rules are applied:

- The certificates for use in OAuth and CCA tokens may be configured with the following values for the keyUsage and extendedKeyUsage extensions (the rest of extensions remains the same as in table 6.1.3c.3-2, except for TLS feature extension that it is not applicable in this case):

Table 6.1.3c.3-2: NF Oauth and CCA Token Certificate Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Extensions | OID | Mandatory | Criticality | Value |
| keyUsage | {id-ce 15} | FALSE | TRUE | digitalSignature for JWS signing keys in OAuth 2.0 with JWT access tokens and CCA tokens.  nonRepudiation (also known as “contentCommitment) is optional when digitalSignature is used instead. |
| extendedKeyUsage | {id-ce 37} | TRUE | FALSE | id-kp-jwt for validating the JWS signature in JWT [63], for example for CCA token. |
| id-kp-oauthAccessTokenSigning for signing OAuth 2.0 access tokens [63]. |

- subjectAltName shall (in TLS client and server certificates, and also in X.509 PKIX certificates used for signing validation of JWT access tokens and/or CCA tokens) contain a URI-ID with the URI for the NF Instance ID as an URN; this URI-ID shall contain the nfInstanceID of the Network Function instance using the format of the NFInstanceId as described in clause 5.3.2 of TS 29.571 [57].

NOTE 1: According to clause 5.3.2 of TS 29.571 [57], "The format of the NF Instance ID shall be a Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [64]".The URN formed using the UUID is the string "urn:uuid:" followed by a hexadecimal representation of the UUID. According to IETF RFC 4122 [64], in a version 4 UUID, the 13th hex digit is '0100' i.e., '4' and the 17th hex digit is '10xx' i.e., in the range '8'-'b'. For example, "urn:uuid: c84792af-f99f-4eca-a17c-ed0c9699e225" is the string representation of the NF Instance ID " c84792af-f99f-4eca-a17c-ed0c9699e225" as a URN.

NOTE 1a: Without URI for the NF Instance ID in subjectAltName in the TLS client and/or server certificates, the identity of the NF instance can not be securely validated when using the NF instance certificate by the receiving peer.

NOTE 1b: Without URI for the NF Instance ID in subjectAltName in the X.509 PKIX certificates used for signing, the identity of the NRF in JWT access token “iss” Issuer claim (i.e., in the context of Home Domain Name defined in Subject DN) cannot be securely validated by NF producers as part of the JWS signature and trust path validation procedures.

- subjectAltName should (in TLS server certificates) contain URI-ID with the HTTPS URI(s) for the apiRoot of a Network Function producer instance for the NF service API(s) that it provides; using wildcard URIs should be avoided.

- subjectAltName may (in X.509 PKIX certificates used for signing validation of JWT access tokens) contain URI-ID with the HTTPS URI for the “Token Endpoint” URI (“{nrfApiRoot}/oauth2/token”) of an NRF instance for the Nnrf\_AccessToken service API that it provides according to clause 5.4.2.2 in TS 29.510 [56]; using wildcard URIs shall be avoided.

- subjectAltName should (in TLS server certificates) contain DNS-ID with the FQDN(s) (host DNS name) of the NF service callback URI(s) that a Network Function consumer instance provides; the rules for using wildcard certificates in DNS-ID are described in RFC 9525 [65].

- subjectAltName should (in TLS client certificates) or shall (for TLS server certificates) contain a DNS-ID with the FQDN (host DNS name) for the Network Function instance, for example, using the instructions for Network Function (host DNS) names in FQDN format as used for Network Function producers in NFProfile and/or in NFService profile according to clause 6.1.6.2 in TS 29.510 [56], and in general as described in clause 28.3 of TS 23.003 [55] (regardless if DNS is available or not); for AMF, this is the AMF Name as described in clause 28.3.2.5 of TS 23.003 [55]; for NRF, this is the NRF FQDN as described in clause 28.3.2.3.2 of TS 23.003 [55]; the rules for using wildcard certificates in DNS-ID are defined in RFC 9525 [65].

NOTE 2: RFC 9113 [50] mandates to use the Server Name Indication (SNI) extension to TLS with HTTP/2. RFC 6066 [51], which is applicable to TLS 1.2, defines that currently only server names supported in SNI extension to TLS are DNS hostnames where "HostName" contains the fully qualified DNS hostname (FQDN) of the TLS server. RFC 6066 [51] also defines that literal IPv4 and IPv6 addresses are not permitted in "HostName". In practice, this means that at least one subjectAltName attribute with FQDN is to be included in server-side TLS end-entity certificates.

- nfTypes shall contain NF types for the Network Function instance formatted according to RFC 9310 [61] using the Enumerated NF Type format according to clause 6.1.6.3.3 of TS 29.510 [56].

NOTE 3: Void.

- subjectAltName shall not contain only IP address in TLS server certificates.

NOTE 4: Void

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