**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220945-r1***

**e-meeting, 16 - 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.310** | **CR** | **0127** | **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:***  |  in the certificate |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2022-05-09 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-16 |
|  | *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:*** | The usage of CN-ID is discouraged.Current specification indicate that:a client does not seek a match for a reference identifier of CN-ID if the presented identifiers include a DNS-ID, SRV-ID, URI-ID, or any application-specific identifier types supported by the client.However, following practice like required by the CA-browser forum, it requires a match between CN-ID and one of the SAN:If present, this field MUST contain exactly one entry that is one of the values contained in the Certificate’s subjectAltName extension.If the match required by CA-browser forum is taken into account in the implementation of opensource software and some 5G applications but not others, it may cause TLS handshake failure. |
|  |  |
| ***Summary of change:*** | Addition of the check required by CA-browser forum when CN-ID is presented. |
|  |  |
| ***Consequences if not approved:*** | Inconsistent implementation which may cause interoperability problems. |
|  |  |
| ***Clauses affected:*** | 2, 6.1.3c.3 |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN CHANGES 1 \*\*\*

# 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 7540: "Hypertext Transfer Protocol Version 2 (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"

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

\*\*\* END CHANGES 1 \*\*\*

\*\*\* BEGIN CHANGES 2 \*\*\*

#### 6.1.3c.3 NF Certificate profile

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

NOTE: RFC 6125 [52] describes guidelines and procedures for representing and verifying the identity of application service using X.509 PKIX certificates with TLS. It mandates use of subjectAltName entries (DNS-ID, SRV-ID, URI-ID, etc.) over the use of the subject field (CN-ID) where available. Furthermore, it is stated that a client does not seek a match for a reference identifier of CN-ID if the presented identifiers include a DNS-ID, SRV-ID, URI-ID, or any application-specific identifier types supported by the client. Additionally, CA-browser forum [X] has the following requirement on the CN-ID: 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 profile for NF:

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 |
| keyEncipherment for TLS 1.2 [54] serversNF that may be both TLS 1.2 [54] client and server shall have both flags set. |
| 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 | distributionPointAc 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. |
| authorityInfoAccess | {id-pe 1} | FALSE | FALSE | id-ad-caIssuersAccording 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-ocspAccording 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-tlsfeatureThis 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:

- subjectAltName should (in TLS client and server certificates) 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: Since the format of the NF instance ID according to clause 5.3.2 of TS 29.571 [57] is a universally unique identifier (UUID), the URN formed using the UUID is the string "urn:uuid:" followed by a hexadecimal representation of the UUID. For example, "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6" is the string representation of the NF Instance ID "f81d4fae-7dec-11d0-a765-00a0c91e6bf6" as a URN.

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

- 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 6125 [51].

NOTE 2: RFC 7540 [50] mandates using 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.

- subjectAltName should (in TLS client certificates) contain NF type as DNS-ID (that is, using dNSName subjectAltName) for the Network Function instance using the Enumerated NF Type format according to clause 6.1.6.3.3 of TS 29.510 [56].

NOTE: If NF type is used in DNS-ID format in subjectAltName then it is considered as case-insensitive.

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

Editor’s Note: It is ffs whether subjectAltName contains URI for the NF Instance ID mandatory or optional in the TLS client and server certificates.

\*\*\* END CHANGES 2 \*\*\*