**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220242-r1***

e-meeting, 14-25 February 2022

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** | **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 of the format of the URN string in the NF certificate profile | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | |  |
|  | *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 format of URN string "urn: uuid:" is wrong as there is an extra blank character. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Remove the extra blank character from the string "urn:uuid:". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Potentially diverging implementations of unclear specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 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 OF CHANGES \*\*\*

#### 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 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.

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] servers  NF 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 | 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. |
| 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:

- 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 OF CHANGES \*\*\*