**3GPP TSG-SA3 Meeting #112 *S3-234313***

**Goteborg, Sweden, 14 - 18 August 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0168** | **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:*** | Certificate Management for 5GC NFs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Huawei, HiSilicon, Ericsson, AT&T, Cisco | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | ACM\_SBA | | | | |  | ***Date:*** | | | 2023-08-18 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | This CR specifies security procedures and protocols for automated certificate management for 5G Core Network Functions, as concluded in the Study on Automated Certificate Management in SBA (TR 33.876) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Specify procedures and protocols related to the automated certificate management for 5G Core Network Functions, as well as a list of recommendations that may not require normative text, but can be added as a reference and/or good practices for implementations.  Specifically, the following aspects are included:  - Set up of initial trust between NF and operator RA/CA  - Certificate enrolment and renewal for 5G Core NFs  - Validation of usage of X.509 certificates in SBA  - Certification revocation procedures  - NF Certificates updates  - Management of certificate and NF lifecycles  - Certificate Management for Network Slicing  - Key Management | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security procedures for automated certificate management in 5G Core would not be specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | New clause (10), New informative annex (I) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

*\*\*\* START OF FIRST CHANGES \*\*\**

# 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".

[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".

[xx] IETF draft-ietf-lamps-nf-eku-01: “X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions”

*\*\*\* END OF FIRST CHANGES \*\*\**

*\*\*\* START OF SECOND CHANGES\*\*\*\**

# X Certificate Management for 5GC NFs

## X.1 General

This clause specifies the following certificate management procedures in SBA for 5GC NFs:

- Set up of initial trust between NF and operator CA/RA.

- Certificate enrolment and renewal for 5GC NFs.

- Validation of usage of X.509 certificates in SBA.

- Certification revocation procedures.

The validation of the trust chain of CA hierarchy is required, ensuring the legitimacy and credibility of the CA. The solutions to establish the trust chain of CA hierarchy are left to implementation.

Other mechanisms and use cases related to certificate management for 5GC NFs are described in informative annex Y and left to implementation.

NOTE: This clause does not consider infrastructure deployment specifics (e.g., virtualization, cloud, etc.)

## X.2 Set up of initial trust

### X.2.1 General

This clause describes the architecture and the procedures for the set up of the initial trust between the operator CA/RA and the NF or the end entity acting on behalf of the NF for the certificate enrolment.

### X.2.2 Architecture

The protection of the NF certificate enrolment procedure has the prerequisite to build initial trust between the 5GC NF and the operator CA/RA.

OAM facilitates the initial trust establishment between NF and operator CA/RA.

Figure X.2.2-1 depicts the general schema to set up initial trust between 5GC NF and operator CA/RA.



**Figure X.2.2-1: Initial trust general schema**

The assumption is that the OAM system is trusted for the operator CA/RA, i.e., the trust between the OAM system and the operator CA/RA shall have been preestablished.

The OAM system of the 5GC NF, which instantiates the NF, shall provide it with the initial trust to be used during the 5GC NF operator certificate enrolment procedure, as part of the initial configuration of the NF.

Three options are described below on how to set up the initial trust. The initial trust can be implemented by 1) OAM issued certificates, 2) an Initial Authentication Key (IAK), or 3) OAM issued signature of certain NF profile parameters. The initial trust shall be implemented by one of these mechanisms. The requirements are the following:

1. The deployment of the initial trust as OAM certificate requires the configuration of a local CA used for 5GC NFs within SBA domain (specifically within the same security trust domain of the NF managed by the OAM system), and the configuration of the root CA public certificate of the local CA as trust anchor in the operator CA/RA.

2. The deployment of the initial trust as IAK requires the distribution of such key out-of-band between the operator CA/RA and the NF via OAM system. This initial credential is used as initial trust by the operator CA/RA to authenticate the NF. The management aspects of IAK are left to implementation (e.g., provisioning, one time use, etc.).

3. The deployment of the signature of certain NF profile selected parameters requires the pre-configuration of such signature out-of-band in the NF. The signature is used by the operator CA/RA to authenticate the NF. The selection of the parameters considered in the signature is left to implementation.

NOTE 1: When the pre-configured signature option is used, the signature can be carried in the regToken control field. The regInfo field may indicate that the certificate request message carries a trusted entity’s signature for certain NF profile parameters.

NOTE 2: If the initial trust is established by certificate, care needs to be taken to avoid the misuse of such certificate (e.g., by revoking the certificate, limiting the validity, etc.).

The operator CA/RA shall be able to verify that the NF Instance Id in the certificate enrolment request belongs to the NF instance requesting the certificate.

### X.2.3 Procedure

Figure X.2.3-1 depicts the procedure for the set-up of initial trust in 5GC NFs.



**Figure X.2.3-1: Procedure for set up of initial trust**

Prerequisites of the procedure:

- If the initial trust has been established by initial digital certificate or OAM signature, the public root certificate of the OAM local CA shall be configured as trust anchor in the operator CA/RA.

- If the initial trust has been established by IAK, the key shall have been securely distributed to the NF by OAM.

- All other necessary parameters to enable the communication with operator CA/RA such as the address shall have been configured by OAM.

1. The OAM system shall configure the initial trust used for the enrolment of the operator certificate in the 5GC NF. If the initial trust is established by an initial certificate during or after the NF initialization, the local CA in the OAM system should issue such initial certificate to the NF as part of its configuration. This certificate shall be configured with the NF Instance Id in SubjectAltName field. The fetching procedure of this certificate by the NF is left to implementation.

2. The 5GC NF generates the private-public key pair and the request of an EE operator certificate to the operator CA/RA. The Certificate Signing Request (CSR) shall include the initial trust (initial OAM issued certificate, signature of NF profile parameters, or IAK) fetched in step 1 and the NF Instance Id in SubjectAltName field. The NF shall sign the request with its private key and includes the digital signature in the request.

If the initial trust is established by an initial certificate, the request shall include the certificate chain of local CA.

If the initial trust is established by IAK, the Operator CA/RA shall validate CSR using the IAK.

If the initial trust is established by a signature of NF profile parameters, the operator CA/RA shall verify the signature in the CSR.

NOTE: Some 5GC NF implementations may include separate certificate management function(s) acting on behalf of the NF towards the CA/RA. The requirements of this procedure are applicable to those functions.

3. Certificate enrolment request is sent to the operator CA/RA.

4. The operator CA/RA shall verify the initial trust in the request from the NF and the identity of the NF (NF Instance Id). If verified, the operator CA/RA shall generate the EE operator certificate for the NF. Specifically, by checking the digital signature on the certificate enrolment request against the trust anchor configured in step 1, and the proof of possession of the private key for the requested operator certificate. It shall verify as well that the NF Instance Id in the SubjectAltName field of the Certificate Enrolment Request corresponds to the NF Instance Id of the initial OAM issued certificate. If those verifications are successful, the operator CA/RA shall generate an EE certificate for the 5GC NF.

5. The operator CA/RA shall include the EE certificate for the requestor NF in certificate enrolment response.

## X.3 Certificate enrolment and renewal for 5GC NFs

This clause describes the protocols and corresponding procedures for certificate enrolment and renewal for 5G Core Network Functions based on CMP protocol.

NOTE: At the time of writing IETF is working in a new version 3 of CMP protocol. The profiling of CMP for 5G Core Network Functions in X.3.1 might be updated accordingly if required.

### X.3.1 CMPv2 Profiling

The following CMPv2 procedures are specified for 5GC NFs:

- Certificate Enrolment.

- Certificate Renewal.

#### X.3.1.1 General Requirements

The following requirements shall apply to CMPv2 usage in Service Based Architecture:

- This CMPv2 profile shall only include certificate request and key update functions. Revocation processing, Cross-Certification and PKCS#10 requests shall not be part of this CMPv2 profile.

- For PKI Message integrity protection, this CMP profile shall only use asymmetric algorithms, or alternatively use shared secret information established via out-of-band means as defined in RFC 4210 [10].

If shared secret information is used, it is recommended to use individual one-time secrets. Shared secrets for all NFs shall not be used.

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

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

NOTE 1: Certificate renewal for operator root certificates is not in scope of this clause. Thus, it is assumed that the NF always has a valid operator root certificate available for validation of key update responses.

- The RA/CA shall support the authentication of initialization requests (ir) based on the verification of out-of-band distributed Initial Authentication Key (IAK) and reference value (mandatory scheme in RFC 4210 [10]).

- The RA/CA shall authenticate key update requests based on signatures which are validated against the operator root CA.

- The RA/CA shall be configured with the SBA root certificate of the operator.

- The RA/CA shall be configured with a RA/CA certificate which is signed either by the operator root CA or by an intermediate CA under the operator root CA.

- If the RA/CA uses different private keys to sign the generated certificates and the CMPv2 messages, the RA/CA shall be configured with the two related certificates, i.e., the RA/CA certificate for signing signatures and the RA/CA certificate for signing CMP messages.

- If the RA/CA certificate or certificates (two in case separate private keys are used for signing of certificates and CMP messages) are not signed directly by the operator root CA, also the certificates of the intermediate CAs shall be configured into the RA/CA.

- The hash algorithms used before generating signatures in the protection field of PKIMessage and for proof-of-possession shall be the same as the hash algorithms specified in subclause 6.1.1 for certificate signatures. The signature algorithms shall be the same as that used in the related certificate profile.

The certificate profiles are specified in subclause 6.1.3c.

NOTE 2: These certificate profiles implicitly specify which algorithms are to be used for the different signatures for proof-of-possession and PKIMessage signing specified in the following subclauses.

NOTE 3: Policies within RA/CA governing the generation and issuing of certificates are not in scope of the present document and left to operator decision.

#### X.3.1.2 Profile for PKIMessage

The following profile is applied to the PKIMessage as specified in IETF RFC 4210 [4]:

- The support and usage of the optional protection field of type PKIProtection is required by this profile. The message-specific private key to be used in the NF is specified in the subclause X.3.1.4 in the profiling of the single PKI message bodies for requests sent by the NF. For the RA/CA the RA/CA private key shall be used, or the separate RA/CA private key for signing CMP messages, if NF certificates and CMPv2 messages are signed by different private keys.

- The support of the optional extraCerts field is required by this profile. The certificates within this field may be ordered in any order. The message-specific content of this field is specified in the subclause X.3.1.4 in the profiling of the single PKI message bodies.

- All CMPv2 messages used within this profile shall consist of exactly one PKIMessage, i.e., the size of the sequence for PKIMessages shall be 1 in all cases.

#### X.3.1.3 Profile for PKIHeader Field

The following profile is applied to the PKIHeader field as specified in IETF RFC 4210 [4]:

- The sender field shall contain the identity of the NF as EE. This identity shall be identical to the subject name of the NF instance present in the certificate for the public key whose related private key is used to sign the PKIMessage.

- The recipient field shall contain the identity of the RA/CA.

NOTE: The subject name of RA/CA needs to be available before the CMPv2 run.

- As the field “protection” of PKIMessage is mandatory, also the field “protectionAlg” of PKIHeader is mandatory. The protectionAlg shall be of type MSG\_SIG\_ALG. The signature algorithm shall be based upon the algorithm contained in the algorithm field of the SubjectPublicKeyInfo field of the signer’s certificate (belonging to the NF or the RA/CA). The hash algorithm used before signing the PKIMessage shall follow the same specification as given for usage before certificate signing in clause 6.1.1 of the present document.

- The usage of the transactionID field is mandatory. The recommended procedures for handling of the transactionID given in [4] shall be followed. The NF shall set this field to a random number that is at least 8 bytes long for the first message and use the same random number in any subsequent message in the transaction.

- The usage of the senderNonce and the recipNonce fields is mandatory. The length of the fields as recommended in [4] shall be used. The recipNonce in the very first message in the transaction should be set to 0 by the sender and shall be disregarded by the recipient of the message.

#### X.3.1.4 Profile for PKIBody Field

##### X.3.1.4.1 General

The NF Instance certificate enrolment shall support the following CMPv2 PKI message bodies:

- Initialization Request (ir).

- Initialization Response (ip).

- Certification Request (cr).

- Certification Response (cp).

- Key Update Request (kur).

- Key Update Response (kup).

- Confirmation (pkiconf).

- Certificate confirm (certconf).

Profiles for the single message bodies above are given in the subclauses below. If no specific profile is given, the provisions of IETF RFC 4210 [4] and IETF RFC 4211 [19] apply.

##### X.3.1.4.2 Initialization Request

The Initialization Request as specified in IETF RFC 4210 [4] shall contain exactly one CertReqMessages as specified in IETF RFC 4210 [4] and IETF RFC 4211 [19], i.e., the size of the sequence for CertReqMessages shall be 1 in all cases.

The following profile shall be applied to the CertReqMessage field and its sub-fields:

- The subjectAltName field of the CertTemplate contains the nfInstanceID of the NF.

- The publicKey field of the CertTemplate is mandatory and shall contain the public key of the NF to be certified by the RA/CA. The private/public key pair may be pre-provisioned to the NF, or generated inside the NF, or generated by a certificate management NF acting on behalf of the NF, for the CMPv2 protocol run. The format of this field shall follow IETF RFC 5280 [14].

- The CertReqMessage shall contain a POP field of type ProofOfPossession. The POP field shall contain a signature field of type POPOSigningKey. The algorithmIdentifier field of the POPOSigningKey field shall contain the signing algorithm which is used by the NF to produce the Proof-of-Possession value, i.e., the signature within POPOSigningKey field.

- If the poposkInput field of type POPOSigningKeyInput within POPOSigningKey field is used, the sender field within POPOSigningKeyInput shall be mandatory and shall contain the identity of the NF Instance (“nfInstanceID”).

NOTE 1: According to IETF RFC 4211 [19], the poposkInput field is mandatory if either the subject field or the publicKey field of the CertTemplate field is omitted.

NOTE 2: According to IETF RFC 4211 [19], the sender field of POPOSigningKeyInput is used only if an authenticated identity has been established by the sender.

The PKIMessage sent by the NF is signed by the generated or provided private key.

##### X.3.1.4.3 Initialization Response

The Initialization Response as specified in RFC 4210 [4] shall contain exactly one generated NF certificate, i.e., the size of the sequence for CertResponse shall be 1 in all cases.

The following profile shall be applied to the CertRepMessage field and its sub-fields:

- The generated certificate shall be transferred to the NF in the certifiedKeyPair field of the CertResponse field. The transfer shall not be encrypted (i.e., the certificate field in CertorEncCert is mandatory).

The extraCerts field of the PKIMessage carrying the initialization response shall be mandatory and shall contain the operator root certificate (or ‘full chain’ if NF contacted to SubCA using CMPv2) and the RA/CA certificate (or certificates if separate private keys are used for signing of certificates and CMP messages). If the RA/CA certificate(s) are not signed by the operator root CA, also the intermediate certificates for the chain(s) up to the operator root certificate shall be included in the extraCerts field. If additional (self-signed) Root CA certificates are required, they shall be carried in the extraCerts field or caPubs field of the PKIMessage. Since extraCerts field is not under CMP message integrity protection, CMP over TLS should be used as a security transport mechanism. Since CMP already supports integrity protection for caPubs field, the use of security transport mechanisms is optional.

##### X.3.1.4.4 Certification request and Certification Response

The Certification Request (cr) and Certification Response (cp) messages as specified in RFC 4210 [4] and RFC 4211 [19] are intended to be used when additional certificates with specific purpose are required by the NF.

The structure and content of these messages is identical to initialization requests and responses, thus the profiling given in the previous subclauses for Initialization Request and Initialization Response shall equally apply, with the following exceptions:

- The PKIMessage sent by the NF shall be signed with the private key which is related to the last received operator provided NF certificate. The extraCertsField is mandatory and shall contain the NF certificate related to the private key used for signing the PKIMessage. Any intermediate CA certificates shall also be included if the NF certificate is not signed directly by a root CA.

- The PKIMessage carrying the certification response should not contain the operator root certificate in the extraCerts field.

##### X.3.1.4.5 Key Update Request and Key Update Response

The structure and content of these messages is identical to initialization requests and responses, thus the profiling given in the previous subclauses for Initialization Request and Initialization Response apply equally, with the following exceptions:

- The PKIMessage sent by the NF shall be signed with the private key which is related to the last received operator provided NF certificate. The extraCertsField is mandatory and shall contain the NF certificate related to the private key used for signing the PKIMessage. Any intermediate CA certificates shall also be included, if the NF certificate is not signed directly by a root CA.

- The PKIMessage carrying the key update response should not contain the operator root certificate in the extraCerts field.

##### X.3.1.4.6 Certificate Confirm Request and Confirmation Response

Initialization responses and key update responses shall always be followed by a Certificate Confirm request and Confirmation response message exchange.

The PKIMessage sent by the NF shall be signed by the same private key which was used in the preceding initialization request or key update request.

The extraCerts field of the PKIMessage carrying the Certificate Confirm request and Confirmation response shall be omitted.

### X.3.2 CMPv2 transport

Transport of CMPv2 messages between end entities (network elements) and RA/CA shall be done using HTTP-based protocol as specified in IETF RFC 6712 [18], with the exception that support for TLS is not mandated.

Support is mandatory for communication initiated by the end entities where every CMP request triggers a CMP response message from the CA or RA. Support for RA/CA initiated HTTP requests (i.e., announcements) is not mandatory.

NOTE 1: CMP provides built-in integrity protection and authentication. For optional usage of HTTP over TLS (HTTPS) according to RFC 9110 or virtual private networks see IETF RFC 6712 [18].

NOTE 2: If CMP over TLS is implemented, the certificates used in this TLS communication are to be provided offline.

### X.3.3 Trusted Network Function instances identifiers

Operator RA/CA should be able to verify that the nfinstanceID in the certificate signing request (‘ir’ and ‘cr’ messages in CMP protocol) belongs to the NF instance requesting the certificate.

During the set up of initial trust between NF and operator RA/CA, the operator RA/CA gets to know the NF identity (nfInstanceID), that can be verified at the certificate enrolment and renewal procedures. Note that the nfInstanceID is included in Subject Alt Name field as per the SBA certificate profile in 6.3.1c.

## X.4 Validation of usage of X.509 certificate

The 5G Core NFs in SBA might need to support multiple operator certificates for different purposes, such as TLS authentication, JSON signing and JSON encryption (e.g., for signing access tokens for service access authorization, signing CCA tokens, etc.).

The Extended Key Usage (EKU) extension of the X.509 certificate as defined in IETF RFC 5280 [14] and IETF draft-ietf-lamps-nf-eku-01 [xx] can 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).

NOTE: RFC 5280 [14] specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates, but there are not extended key purpose identifiers explicitly assigned for JSON Web Signature (JWS) and JSON Web Encryption, used in 5GC. IETF draft-ietf-lamps-nf-eku-01 [xx] defines extended key purpose identifiers for JWS, JWE. This is work in progress in IETF at the time of writing, therefore the procedure of validation of usage of X.509 certificate is currently applicable only to TLS authentication.

## X.5 Certificates revocation procedures

The possible certificate revocation procedures are profiled in clauses 6.1a and 6.1b of the present document.

*\*\*\*\* END OF SECOND CHANGES\*\*\*\**

*\*\*\* START OF THIRD CHANGES \*\*\**

# Annex Y (Informative): Guidance for 5GC certificates management procedures left to implementation.

## Y.1 Introduction

This clause provides guidance to consider in the deployment of 5GC certificate management procedures that have been left to implementation.

## Y.2 NF Certificate Updates

The normal procedure of update and renewal of 5GC NF certificates is managed by CMP protocol as described in clause X.3.1.

Nevertheless, the certificate management framework can be severely impacted by special critical circumstances, which can derive in simultaneous updates of vast number of certificates, causing a potential partial or complete disruption of the service. For example, a compromised security algorithm, the disclosure of broken cryptographic primitives, the revocation of CA root certificates or multiple certificates with same expiration data, are some of the special circumstances triggering the certificate update procedure.

This clause lists a few practical recommendations to be considered in NF certificate update procedure with the aim of mitigating potential issues or disruptions due to outages or overload situations. These recommendations can be deployed and implemented via internal configuration, operator policies and other mechanisms and functionalities in the operator PKI infrastructure, OAM systems, orchestration systems, etc.

- The NF certificate updates can be configured in the operator PKI, and consequently the procedure can be initiated in advance before the certificate expiration time. For example, making use of different time interval/periodicity based on the NF type when configuring certificate update policies. Observe that the NF type is included in the certificates as per the profile in clause 6.1.3c and hence can be checked there while configuring such policies.

- The operator PKI does not have to update the certificates with the same or similar expiration time simultaneously. Furthermore, the certificate update policies can take into consideration the expiration time and the triggers of the procedure being configured in advance. Certificate updates policies can be configured, for example in the operator PKI, to create different batches of certificates to be updated sequentially or with certain prioritization criteria.

- Certificate expiry related alarms reported by network management systems, operator CA announcements for certificate revocations (e.g., via CRL, OCSP, etc.), and any other type of certificate related event, can be monitored with the purpose of mitigating the risk of service unavailability due to above mentioned special circumstances.

## Y.3 Certificate lifecycle management

In the implementation of a certificate lifecycle management framework, the NF lifecycle can be considered.

For example, when the certificate of an NF producer instance has been revoked without the knowledge of the NRF, the NRF might return that instance to the NF consumer during the discovery procedure, leading to unnecessary signalling due to the use of non-valid certificates. In that case, during the NF discovery procedure, the NRF may check that the potential producers, to be included in the response, do have valid certificates. How such a check is performed is left to implementation. For example, it can be based on locally stored information or by querying other network entities such as OCSP/CRL servers.

## Y.4 Certificate Management for Network Slicing

The certificate management framework in 5G Core might need to work with certificates that belong to different domains, such as customer 3rd party slices, possibly with different requirements in terms of certificate lifecycles, CA(s) security policies potentially managed by administrators of multiple stakeholders (e.g., 5G Core operator, network slice customers/tenants) etc.

Network slice customers being offered certain slices can require performing management and operation tasks for the certificates of slice-specific NFs over operator’s CA, or even to use their own CA and certificate management procedures for all or part of the slice-specific NFs. In this case, operator and slice customer may need to agree on mechanisms to establish the trust between operator and customer domain and automate certification lifecycle management across operator CAs/RAs and third parties CAs specific for slice(s).

Trust relationship and secure communication between the different entities involved in the network slicing certificate management, i.e., NF management functions (OAM), operator RA/CA and CAs (root CAs, or sub-CAs) specific for slice(s), may need to be established. Operator and slice customer may need to support capabilities to allocate a root CA/sub-CA to sign slice specific certificate for a NF, and may need to be able to manage such slice-specific certificates within the slicing orchestration framework to align with the network slice lifecycle.

## Y.5 Key Management

Service Based Architecture (SBA) is likely to be deployed in an all-software multivendor environment. It is imperative that the underlying virtualized infrastructure hosting SBA NF is secured for confidentiality, integrity, and replay protection between authenticated endpoints.

Also, the security of the certificate management relies on robust secure key management. It includes confidentiality and integrity of the private key while at rest. All the life cycle stages of the cryptographic key, such as key generation and key rotation, need to follow secure practices.

*\*\*\* END OF THIRD CHANGES\*\*\*\**