**3GPP TSG-SA3 Meeting #111 *S3-233269***

**Berlin, Germany, 22 - 26 May 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **Draft 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:***  | Living document for ACM\_SBA (Automated Certificate Management in SBA) |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | ACM\_SBA |  | ***Date:*** | 2023-05-15 |
|  |  |  |  |  |
| ***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 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:*** | This living draftCR 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.  |
|  |  |
| ***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, as per conclusions reached so far within TR 33.876, the following aspects are included:- Certificate enrolment and renewal- Set up of initial trust- Certificate lifecycle management- Validation of usage of X.509 certificate- NF Certificates Updates (informative annex)More aspects will be added as per further conclusions and corresponding WID objectives have been reached.  |
|  |  |
| ***Consequences if not approved:*** | Security procedures for automated certificate management in 5G Core not specified |
|  |  |
| ***Clauses affected:*** | New chapter (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 \*\*\**

# X Certificate Management for 5GC NFs

 Editor's Note: This clause does not consider infrastructure deployment specifics thus may not be applicable to some deployment scenarios (e.g., 5GC NFs deployed on Cloud Native platform).

## X.1 General

Editor's Note: This clause introduces the new chapter and the specific contents to be included in the next sub-clauses. The list of contents to be included in the normative text is not closed yet, so the current outline can be extended with new clauses.

## X.2 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

### X.2.1 CMPv2 Profiling

The following CMPv2 procedures are specified for 5GC NFs:

- Certificate Enrolment

- Certificate Renewal

#### X.2.1.1 General Requirements

Editor's Note: How to handle duplicate content is FFS.

Editor's Note: Clarifications related to the End Entity are FFS.

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].

Editor's Note: The use of shared secrets is FFS

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 as End Entity (EE) 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.

Editor's Note: Further requirements are ffs.

NOTE 2: [draft-ietf-lamps-cmp-algorithms-15 - Certificate Management Protocol (CMP) Algorithms](https://datatracker.ietf.org/doc/draft-ietf-lamps-cmp-algorithms/) [xx] lists current cryptographic algorithms usable with CMP to offer an easier way maintaining the list of suitable algorithms over time.

The certificate profiles are specified in subclause 6.1.3c.

NOTE 3: 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 4: 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.2.1.2 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.2.1.4 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.2.1.4 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.2.1.3 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.2.1.4 Profile for PKIBody Field

##### X.2.1.4.1 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.2.1.4.2 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.2.1.4.3 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.

Editor’s Note: Use of extraCerts and caPubs is FFS.

##### X.2.1.4.4 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.2.1.4.5 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.2.1.4.6 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.2.2 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: 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].

## X.3 Set up of initial trust

Editor's Note: This clause describes the procedure and mechanisms recommended to set up the initial trust between NF and operator CA/RA to proceed with the certificate enrolment.

## X.4 Certificate lifecycle management

Editor's Note: This clause describes several procedures dealing with the certificate’s lifecycle management.

### X.4.1 Certificates revocation procedures

Editor's Note: This clause describes the recommended certification revocation schemas to be supported in 5GC, in principle CRLs, and potentially (to be evaluated) OCSP and OCSP stapling. Corresponding sub-clauses can be added if required.

## X.5 Validation of usage of X.509 certificate

Editor's Note: The location of the content of this clause is FFS

The 5G Core NFs in SBA may 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.).

Editor's Note: The formulation of the requirements below is FFS.

The following procedure may be applied to indicate and validate the purpose of the X.509 certificates used in SBA by using the Extended Key Usage (EKU) extension of the certificate as defined in IETF RFC 5280 [14] and IETF draft-ietf-lamps-nf-eku-00 [xx].

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-00 [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.

Editor's Note: The addition of an explanatory flow and procedure is FFS.

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

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

Annex Y (Informative): Guidance in the certificates management procedures left to implementation

# Y.1 Introduction

Editor's Note: This clause introduces the new informative annex dedicated to procedures that do not require normative text, but they are rather recommendations in the implementation of the certificate management framework. The list of contents to be included in this annex is not closed yet, so the current outline can be extended with new clauses.

# Y.2 NF Certificate Updates

Editor's Note: This clause describes some approaches to be considered in the NF certificate updates in special circumstances (e.g., outages, simultaneous update of a vast number of certificates, etc.)

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