|  |  |
| --- | --- |
| 3GPP TR 33.876 V18.0.1 (2023-07) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on automated certificate management in Service-Based Architecture (SBA)  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 7

Introduction 8

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Symbols 11

3.3 Abbreviations 11

4 Architectural and security assumptions 11

4.1 Security Assumption #1: Security requirements of intra NF communications 11

4.1.1 Background 11

4.1.2 Security threats 12

4.1.3 Detailed Assumptions 12

4.2 Security Assumption #2: Protection of private keys at rest 12

4.2.1 Background 12

4.2.2 Security threats 12

4.2.3 Detailed Assumptions 12

5 Key issues 12

5.1 Key Issue #1: Single certificate management protocol and procedures 12

5.1.1 Key issue details 12

5.1.2 Security threats 13

5.1.3 Potential security requirements 13

5.2 Key Issue #2: Security protection of NF certificate enrolment 13

5.2.1 Key issue details 13

5.2.2 Security threats 13

5.2.3 Potential security requirements 13

5.3 Key Issue #3: NF Certificate Update 13

5.3.1 Key issue details 13

5.3.2 Security threats 14

5.3.3 Potential security requirements 14

5.4 Key Issue #4: Trust Chain of Certificate Authority Hierarchy 14

5.4.1 Key issue details 14

5.4.2 Security threats 14

5.4.3 Potential security requirements 14

5.5 Key Issue #5: Certificates revocation procedures 15

5.5.1 Key issue details 15

5.5.2 Security threats 15

5.5.3 Potential security requirements 15

5.6 Key Issue #6: Relation between certificate management lifecycle and NF management lifecycle 15

5.6.1 Key issue details 15

5.6.2 Security threats 16

5.6.3 Potential security requirements 16

5.7 Key Issue #7: Multiples certificates to be associated with a Network Function 16

5.7.1 Key issue details 16

5.7.2 Security threats 16

5.7.3 Potential security requirements 16

5.8 Key Issue #8: Trusted Network Function instances identifiers 17

5.8.1 Key issue details 17

5.8.2 Security threats 17

5.8.3 Potential security requirements 17

5.9 Key Issue #9: Automated Certificate Management for Network Slicing 17

5.9.1 Key issue details 17

5.9.2 Security threats 18

5.9.3 Potential security requirements 18

6 Solutions 19

6.0 Mapping of solutions to key issues 19

6.1 Solution #1: Certificate Enrolment and MAnagement Framework (CEMAF) 19

6.1.1 Introduction 19

6.1.2 Solution details 19

6.1.2.1 General 19

6.1.2.2 Architecture 20

6.1.2.3 Procedures 20

6.1.3 Evaluation 21

6.2 Solution #2: Using CMP protocol for certificate enrolment and renewal 21

6.2.1 Introduction 21

6.2.2 Solution details 21

6.2.2.1 CMPv2 Profiling for SBA 22

6.2.2.1.1 General Requirements 22

6.2.2.1.2 Profile for PKIMessage 23

6.2.2.1.3 Profile for PKIHeader Field 23

6.2.2.1.4 Profile for the PKIBody Field 23

6.2.2.2 CMPv2 Transport 25

6.2.3 Evaluation 25

6.3 Solution #3: Secure initial enrolment of NF certificates 26

6.3.1 Introduction 26

6.3.2 Solution details 27

6.3.3 Evaluation 28

6.4 Solution #4: Cross-Certification Based Trust Chain in the SBA Architecture 29

6.4.1 Introduction 29

6.4.2 Solution details 30

6.4.2.1 General architecture 30

6.4.2.2 Verify certificate in SBA architecture 31

6.4.3 Evaluation 32

6.5 Solution #5: Interconnection CA Based Trust Chain in the SBA Architecture 32

6.5.1 Introduction 32

6.5.2 Solution details 33

6.5.2.1 General architecture 33

6.5.2.2 Verify certificate in SBA architecture 34

6.5.3 Evaluation 35

6.6 Solution #6: OCSP based revocation procedure 35

6.6.1 Introduction 35

6.6.2 Solution details 35

6.6.2.1 General 35

6.6.2.2 Procedure 35

6.6.3 Evaluation 36

6.7 Solution #7: A solution addressing the relation between certificate lifecycle management and NF lifecycle management 36

6.7.1 Introduction 36

6.7.2 Solution details 36

6.7.3 Evaluation 37

6.8 Solution #8: Enhance the security protection for Certificate parameters 38

6.8.1 Introduction 38

6.8.2 Solution details 38

6.8.2.1 General 38

6.8.2.2 Procedure 38

6.8.3 Evaluation 39

6.9 Solution #9: Certificates revocation query procedure based on NRF 39

6.9.1 Introduction 39

6.9.2 Solution details 40

6.9.2.1 General 40

6.9.2.2 NF service Registration procedure 40

6.9.2.3 NF/NF service discovery in the same PLMN 40

6.9.3 Evaluation 41

6.10 Solution #10: Solution to indicate and validate the purpose of the certificate 42

6.10.1 Introduction 42

6.10.2 Solution details 42

6.10.3 Evaluation 43

6.11 Solution #11: OCSP Stapling addressing Key Issues #5 and #6 44

6.11.1 Introduction 44

6.11.2 Solution details 44

6.11.3 Evaluation 45

6.12 Solution #12: Automated Certificate Management for Network Slices 46

6.12.1 Introduction 46

6.12.2 Solution details 46

6.12.3 Evaluation 48

6.13 Solution #13: Build initial trust for NF certificate enrolment 48

6.13.1 Introduction 48

6.13.2 Solution Details 49

6.13.3 Evaluation 50

6.14 Solution #14: Ensuring the management of bulk certificate updates 51

6.14.1 Introduction 51

6.14.2 Solution details 51

6.14.3 Evaluation 52

6.15 Solution #15: Policy based certificate update/renewal 52

6.15.1 Introduction 52

6.15.2 Solution details 52

6.15.3 Evaluation 52

6.16 Solution #16: Using ACME protocol for certificate enrolment and renewal 52

6.16.1 Introduction 52

6.16.2 Solution details 53

6.16.2.1 Solution overview 53

6.16.2.2 ACME Profiling for SBA 54

6.16.2.2.1 General Requirements 55

6.16.2.2.2 Profile for PKI Fields 55

6.16.2.3 ACME Transport 56

6.16.3 Evaluation 57

6.17 Solution #17: Assurance of unique NF identifiers in certificates 57

6.17.1 Introduction 57

6.17.2 Solution details 57

6.17.2 Evaluation 58

6.18 Solution #18: Slice specific initial enrolment procedure 59

6.18.1 Introduction 59

6.18.2 Solution details 59

6.18.3 Evaluation 59

7 Conclusions 60

7.1 KI#1: Single certificate management protocol and procedures 60

7.1.1 Analysis 60

7.1.1 Conclusion 60

7.2 KI#2: Security protection of NF certificate enrolment 60

7.2.1 Analysis 60

7.2.2 Conclusion 61

7.3 KI#3: NF Certificate Update 61

7.3.1 Analysis 61

7.3.2 Conclusion 61

7.4 KI#4: Trust Chain of Certificate Authority Hierarchy 61

7.4.1 Analysis 61

7.4.2 Conclusion 62

7.5 KI#5: Certificates revocation procedures 62

7.5.1 Analysis 62

7.5.2 Conclusion 62

7.6 KI#6: Relation between certificate management lifecycle and NF management lifecycle 62

7.6.1 Analysis 62

7.6.2 Conclusion 63

7.7 KI#7: Multiples certificates to be associated with a Network Function 63

7.7.1 Analysis 63

7.7.2 Conclusion 63

7.8 KI#8: Trusted Network Function instances identifiers 63

7.8.1 Analysis 63

7.8.2 Conclusion 64

7.9 KI#9: Automated Certificate Management for Network Slicing 64

7.9.1 Analysis 64

7.9.2 Conclusion 64

Annex A: Change history 65

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

According to TS 33.501 [2], use of mutual TLS for authentication of NF requires compliance to 3GPP TS 33.310 [3] section 6.1.3c for TLS client and TLS server certificate profiles in addition to TLS profile compliance with section 6.2a of [3].

The use of TLS certificates in 5G SBA is ubiquitous.

However, unlike standardised model using CMPv2 in RAN, SBA does not have a standardised model and set of procedures for automated certificate management.

SBA also does not have a standardised protocol for managing life cycle events of the certificates, e.g., bootstrap, request, issue, enrolment, revocation, renewal etc.

- Lack of standardisation has resulted into number of bespoke methodologies and varying choices of certificate management protocols resulting into inconsistent model.

- Once service slicing and NPN are introduced in service provider network, manual management or lack of standardised procedures for life cycle management of TLS certificates belonging to separate legal entities could further complicate the architecture.

All the above have potential of increasing the security risk and impact the deployment and availability of operators' 5G SBA network.

RAN has benefitted from the standardisation of CMPv2 to be used for eNodeB/gNodeB automated certificate management. The specification defined a bootstrap procedure based on the use of vendor certificate for requesting an operator certificate for the set-up of IPSec IKE2 towards the SeGW. 5G SBA is within the operator core network domain that could benefit from a study that leads to the standardisation of an automated certificate management procedure using a standardised protocol that fits for purpose to serve the 5G Core Network.

# 1 Scope

The objectives of this study are to identify key issues, potential security and privacy requirements and solutions with respect to

- Standardise the use of a single automated certificate management protocol and procedures for certificate life cycle events within intra-PLMN 5G SBA (i.e. to be used by all 5GC NFs including NRF, SCP, SEPP etc.).

- Study the impact of service mesh in certificate management within 5G SBA.

- Study which lifecycle events (e.g., enrolment, renewal, revocation (e.g., OCSP, CRLs), status monitoring) of a certificate need to be covered.

- Study the relation between certificate management lifecycle and NF management lifecycle.

- Study to reference at minimum following principles:

- Principle to be reusable when 5G SBA is for NPN (standalone and PNI)

- Principles standardised to be able to support NFs doing mutual TLS in Slicing.

- Principles standardised to support both intra and inter PLMN, in the latter referring to SEPP certificates in N32 interfaces and potential cross-certification considerations.

- Principles involving 'Chain of Trust' of Certificate Authorities hierarchies.

- Principles for security of CA's cryptographic private key.

# 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[4] IETF RFC 7515: "JSON Web Signature".

[5] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[6] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[7] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[8] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[9] IETF RFC 6712:"Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)".

[10] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol".

[11] IETF: Certificate Management Protocol (CMP) Updates, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-cmp-updates-21>.

[12] ETSI GR NFV-SEC 005 V1.2.1: "Network Functions Virtualisation (NFV); Trust; Report on Certificate Management".

[13] ETSI GS-NFV 006 V2.1.1: "Management and Orchestration; Architectural Framework Specification".

[14] 3GPP TS 23.502: " Procedures for the 5G System (5GS)".

[15] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[16] IETF RFC 6961: "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension.

[17] 3GPP TR 33.848: "Study on Security Impacts of Virtualisation".

[18] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

[19] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[20] [draft-ietf-lamps-cmp-algorithms-15 - Certificate Management Protocol (CMP) Algorithms](https://datatracker.ietf.org/doc/draft-ietf-lamps-cmp-algorithms/) "Certificate Management Protocol (CMP) Algorithms".

[21] IETF draft-ietf-lamps-nf-eku-00: "X.509 Certificate Extended Key Usage (EKU) for (JOSE) and CBOR Object Signing and Encryption (COSE)" <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-nf-eku>.

[22] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[23] IETF RFC 8555: "Automatic Certificate Management Environment (ACME)".

[24] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[25] IETF RFC 9110: "HTTP Semantics".

[26] IETF RFC 8738: "Automated Certificate Management Environment (ACME) IP Identifier Validation Extension".

[27] IETF draft-ietf-acme-authority-token-tnauthlist-12: "TNAuthList profile of ACME Authority Token" <https://datatracker.ietf.org/doc/html/draft-ietf-acme-authority-token-tnauthlist-12>.

[28] IETF RFC 8739: "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

## 3.2 Symbols

Void

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ACME Automatic Certificate Management Environment

CA Certification Authority

CCA Client Credential Assertion

CeEF Certificate Enrolment Function

CEMAF Certificate Enrolment and MAnagement Framework

CeMF CEMAF Management Function

CM Certificate Management

CMNE Certificate Management Network Entity

CMP Certificate Management Protocol

CRL Certification Revocation List

CSR Certificate Signing Request

CUO Certificate Update Orchestrator

EE End Entity

EKU Extended Key Usage

IAK Initial Authentication Key

JWS JSON Web Signature

LCM Lifecycle Management

NSCOF Network Slice Certificate Orchestration Function

OAM Operations, Administration and Maintenance

OCSP Online Certificate Status Protocol

PKCS Public Key Cryptography Standards

PKI Public Key Infrastructure

POP Proof of Possession

PSK Pre-Shared Key

RA Registration Authority

SAN Subject Alt Name

STAR Short Term Automatically Renewed

TLS Transport Layer Protocol

UUID Universally Unique IDentifier

VNF Virtual Network Function

# 4 Architectural and security assumptions

## 4.1 Security Assumption #1: Security requirements of intra NF communications

### 4.1.1 Background

It is likely that SBA services will be made up from software components that communicate with each other over a LAN. This "intra-SBA" communication needs to be secured. Even if intra-SBA is not standardised, requirements on the security of this communications need to be present so that suitable certification methods can be created to test the SBA service.

### 4.1.2 Security threats

If the intra-SBA communication is insecure then, depending on the SBA service, user data may be leaked to an attacker, or an attacker may be able to insert information that may cause adverse actions.

### 4.1.3 Detailed Assumptions

Communications that are internal to an SBA service but carried on a LAN connection should be integrity protected.

Communications that are internal to an SBA service but carried on a LAN connection should be confidentiality protected.

Communications that are internal to an SBA service but carried on a LAN connection should be replay protected.

The endpoints for communications that are internal to an SBA service should be mutually authenticated.

## 4.2 Security Assumption #2: Protection of private keys at rest

### 4.2.1 Background

The TLS process produces private keys that need to be kept secure at rest.

### 4.2.2 Security threats

If the private keys are not stored securely, then an attacker can access the keys and then emulate the SBA service as though it is the genuine service leading to data loss and the ability to perform Man in the Middle attacks.

### 4.2.3 Detailed Assumptions

Private keys are securely stored at rest.

Where a private key is stored internally to a service then it should be confidentiality and integrity protected.

Where a private key is stored in a secure central key repository, then the repository should be at least as secure as the key agreement method and the communications between the SBA service and the secure central key repository are also be secured.

# 5 Key issues

## 5.1 Key Issue #1: Single certificate management protocol and procedures

### 5.1.1 Key issue details

Considering virtualization in 5G SBA, it is impossible to manage certificates manually.

If there is no standardized use of an automated cert management protocol, the certificate management needs to be done manually which may lead to missing refreshment of certificates and usage of expired certificates.

It will increase the implementation and deployment complexity when several automated certificate management protocol and procedures are defined. And there will be interoperability issue for different implementation because NF may not be able to have a certificate from CA or may not be able to verify the certificate of other NF.

This KI is to investigate required certificate management capabilities (e.g., enrolment, renewal), to be used for corresponding certificate life cycle events, expected from a certificate management protocol and whether it is feasible to have a single certificate management protocol and procedures for all these certificate life cycle events within intra-PLMN 5G SBA, which is mandatory for implementation.

### 5.1.2 Security threats

Not applicable.

### 5.1.3 Potential security requirements

Not applicable.

## 5.2 Key Issue #2: Security protection of NF certificate enrolment

### 5.2.1 Key issue details

An instantiated NF needs to obtain the certificate from the CA for securing the communication with other NFs, encrypting messages, or signing tokens, among other purposes in SBA. Thus, a secure and automated certificate enrolment procedure is indispensable to obtain the certificates. Before issuing a certificate, operator CA/RA needs to establish an initial trust with the requestor NF instance, ensuring that the requestor NF instance is the correct one and is entitled to request a certificate.

This key issue considers the procedure of certificate enrolment including the establishment of the initial NF trust, the protection of certificate enrolment procedure, and the authentication between NF and CA.

### 5.2.2 Security threats

If the NF cannot obtain a certificate, and the certificate enrolment procedure is not secured, the following problems may occur:

1. The NF cannot communicate with each other.

2. If certificate enrolment parameters are tampered, the CA issues an incorrect certificate.

3. Without pre-established trust between the NF and CA/RA, an attacker claiming to be a trusted NF with connectivity in SBA could apply for a valid operator certificate.

### 5.2.3 Potential security requirements

New NF instances need an automated and secure procedure to build initial trust with the CA/RA during certificate enrolment procedure.

5GS should support the means to secure the automated enrolment of certificates, include integrity protection and Anti-replay protection of enrolment procedure.

5GS should support the mutual authentication between involved parties during the enrolment procedure.5GS should support the verifying of certificate validity for certificate enrolment.

## 5.3 Key Issue #3: NF Certificate Update

### 5.3.1 Key issue details

NF certificate update is a necessary part of an automated certificate management mechanism because the long validity period certificate is considered not secure. Therefore, it is important that each certificate is set with an appropriate period of validity. Furthermore, it is necessary to update the NF certificate when the certificate is about to expire or has expired. Otherwise, NF communication can be disrupted in the middle of operation due to an unhandled certificate expiry.

If a vast number of NF instances and services simultaneously require certificate updates, for example due to same expiration date, or a common CA certificate revocation, or the compromise of a crypto algorithm in use among other causes, the automated certificate management framework may trigger the certificate update procedure for all affected end entities at the same time. If there are no mechanisms to manage this situation, it can bring congestion and/or overload in the automated certificate management framework, leading to temporary service unavailability.

### 5.3.2 Security threats

If the NF certificate is not updated, or the certificate update procedure is not secured, the following problems can occur:

1) An attacker misuses the update mechanism to get hold of valid certificates from CA and mount impersonation attacks.

In some implementations the simultaneous update / renewal of a vast number of certificates may lead to partial or complete disruption of the automated certificate management framework.

### 5.3.3 Potential security requirements

5GS should support to update the NF certificate securely.

## 5.4 Key Issue #4: Trust Chain of Certificate Authority Hierarchy

### 5.4.1 Key issue details

According to the scope of the present document, the study should reference at minimum the following principles:

Principles involving 'Chain of Trust' of Certificate Authorities.

Principles for security of CA's cryptographic private key.

As emphasized in the principles, the legitimacy and credibility of certificate authority are critical for automated certificate management in SBA. Building the legitimacy and credibility relies on a trust chain of CA hierarchy, which specifies the CA hierarchy and their transitive trust relationship. Based on the chain of trust, each CA can be verified by a trusted source. And after the verification is passed, the CA can act as the new trusted source and issue the digital certificate for the child CA or the TLS entity. This transitive trust relationship enables TLS entities in 5G SBA to obtain their own certificates and verify the certificate of other TLS entities. In the study of automated certificate management in 5G SBA, the trust chain of CA hierarchy is indispensable.

Currently, there is no clear requirement about the trust chain of CA hierarchy in TS 33.310 [3]. The TS 33.310 [3] specifies SBA certificate profiles in clause 6.1.3c and the general architecture for issuing TLS certificates in clause 5.1.1.2. However, under the general architecture, it is unclear how to generate different types of SBA certificates and how SBA certificates can be verified between different types of NFs.

### 5.4.2 Security threats

Due to the lack of trust chain, the TLS entity in SBA cannot verify the credibility of SBA certificates sent by other TLS entities. This means that the connection cannot be established.

Under the general architecture for issuing TLS certificates, CAs may not be able to generate all the SBA certificates as specified in TS 33.310 [3] clause 6.1.3c.

### 5.4.3 Potential security requirements

The TLS entity in SBA should be able to verify the received certificate based on the trust chain.

The TLS entity should be able to obtain the corresponding certificate based on its role, e.g. the NF service producer shall be able to obtain the TLS server certificate.

## 5.5 Key Issue #5: Certificates revocation procedures

### 5.5.1 Key issue details

Certificates revocation procedures are a critical part of the overall certificate lifecycle management. Every certificate has a finite validity period, during the one it is expected to be in use. However, during that validity period the certificate owner and/or Certificate Authority may consider and declare that a certificate is not longer trusted, i.e., invalid prior to the expiration of the validity period, due to multiple circumstances (e.g., suspected compromise of the private key).

Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) and OCSP stapling are revocation schemes/functions of certificate revocation. Clauses 6.1a and 6.1b of TS 33.310 [3] provides profiles for CRL and OCSP respectively.

5G Core SBA Network functions and operator PKI need a certificate revocation schema, part of the overall certificate lifecycle management framework, with the following characteristics:

1) Scalable – the number of revoked certificates should not be a concern in terms of latency and/or performance of the SBA architecture and network functions.

2) Providing fast/near real time responses – the revocation function should serve in a highly dynamic environment hosted by virtualized cloud infrastructure.

3) Resilient – in case of operator CA outages, or issues in the communication to revocation infrastructure, the revocation procedures should be minimally affected, and the Network Functions should be able to check the validity status of the certificate to be verified.

### 5.5.2 Security threats

If the process of publishing a new updated CRL is too slow, it can leave the client open to attacks. E.g., a revoked certificate may be maliciously used during the time window between the revocation and the reception of the CRLs.

The lifecycle of ephemeral/short live Network Functions (e.g., in Network Slicing) will likely reduce even more the time window for distributing and retrieve the information on the revocation status of the certificates. There is a risk that the clients are not updated accordingly, creating a security vulnerability.

Lean Network Function designs based on micro-services type of software architectures are aiming to optimize the use of resources. Intensive demand of revocation status checks can generate a severe impact in service availability by downgrading the performance of the Network Function.

### 5.5.3 Potential security requirements

Not Applicable.

## 5.6 Key Issue #6: Relation between certificate management lifecycle and NF management lifecycle

### 5.6.1 Key issue details

Although the NF management lifecycle and certificate management lifecycle can require different management mechanisms and processes, they have some relations because the certificates are issued for the NFs. Thus, it is necessary to investigate the relations and consider these relations while specifying the automated certificate management for SBA.

Generally, since NF lifecycle processes are independent from the validity period of the associated certificates, if certificate management mechanism is designed not considering the NF lifecycle, then there can be some cases such as having NFs with no certificates or existing certificates belonging to no NF. For example, when the certificate of a producer NF instance has been revoked without the knowledge of the NRF, the NRF returns that producer NF instance ID in the discovery procedure. In this case, the consumer NF will try to get service from the producer NF, but it will not be able to get the service because the producer NF's certificate has been revoked. This type of cases will lead to inconsistent status in NRF and reduce the service availability.

Because of the reasons explained above, the relations between NF management and certificate management lifecycles need to be considered in the design of an automated certificate management for SBA. Solutions to this key issue need to explain how the relations between NF management and certificate lifecycles can be considered in automated certificate management for SBA.

### 5.6.2 Security threats

Inconsistencies between the NF management lifecycle and certificate management lifecycle processes can lead to severe vulnerabilities in the system. For example, if after decommissioning of a NF instance, cryptographic keys and certificates are still valid, they can be compromised by a potential attacker and used to access the network and corresponding services. Furthermore, an NF instance with an expired certificate can still be discovered by NFs in SBA. Such NF with expired certificate in hands of a potential attacker can compromise other NFs.

### 5.6.3 Potential security requirements

In the certificate lifecycle management, NF lifecycle should be considered.

## 5.7 Key Issue #7: Multiples certificates to be associated with a Network Function

### 5.7.1 Key issue details

In SBA the Network Functions (NFs) could require to support multiple operator certificates, which can be issued by different operator sub-CAs or root CAs depending on the established CA hierarchies and predefined network domains, for different purposes and interfaces.

Each type of certificate per Network Function could have different security considerations. The type of certificates in Network Functions of SBA are the following:

1) TLS client EE certificates (for NF consumers)

2) TLS server EE certificates (for NF producers)

NOTE: Clause 6.1.3 of TS 33.310 [3] profiles the TLS entity certificates to be used for 5GC SBA.

3) Certificates for signing the access tokens for authorization (JSON Web Signature (JWS) as described in RFC 7515 [4]) (for NRFs)

4) Certificates for encrypting HTTP messages between SEPPs (clause 13.2.4.4 of TS 33.501 [2])

5) Certificates for signing Client credentials assertion (CCA) tokens (clause 13.3.8.2 of TS 33.501 [2])

### 5.7.2 Security threats

If the purpose of the issued certificates is not restricted, i.e., the type of operations for which a public key contained in the certificate can be used are not specified, those certificated could be used for another purpose than intended, violating the CA policies, and increasing the risk of cross-protocol attacks.

Failure to ensure proper segregation of duties means that a NF who generates the encryption keys and applies for a certificate to the operator CA, could obtain a certificate which can be misused for tasks that this NF is not entitled to perform. E.g., a consumer could impersonate producers using their own client certificate.

### 5.7.3 Potential security requirements

The Network Functions should be able to indicate the purpose of the certificate being requested in the CSR (Certificate Signing Request) to the operator CA.

The certificate management framework, i.e., the set of protocols and procedures for automated certificate management, in 5G SBA shall be able to provide means for identifying, monitoring, and validating the usage of the issued certificates.

## 5.8 Key Issue #8: Trusted Network Function instances identifiers

### 5.8.1 Key issue details

Service mesh describes a network of microservices, in which applications are shared and interaction between applications is possible. To gain operational control over such distributed microservice architecture, a service needs to be identified.

SBA can be implemented as a service mesh architecture. In SBA Network Function (NF) instances offer services to other NFs or NF instances. In order for a requested NF type, NF service, or NF service instance, to be discovered via the NRF, the NF instance needs to be registered in the NRF. After registration, the NRF maintains NF profiles of available NF instances and their supported services. The NF is identified by a NF instance ID. The Information Element (IE) NFInstanceID among other IEs is included in the NF profile maintained in the NRF are specified in TS 23.501[5] clauses 6.2.6 and 6.3.1, and in TS 29.510 [6].

When a NF requests a X.509 certificate needs to send a Certificate Signing Request (CSR) message to the operator CA in order to get a X.509 certificate created. A CSR is often generated by the same NF on which the certificate is to be installed, although it can also be generated by other trusted intermediary entity acting on behalf of the NF if the NF does not have such capability. The public key is included in the CSR and used by the CA to create the certificate, and the private key is used to sign the information contained in the CSR (integrity protection). Apart from the public key, the CSR can have other information (e.g., Common Name, Organization, location, etc.).

TS 23.501 [5] defines an NF instance as an identifiable instance of the NF. CSRs need to contain a trusted and unique identity of the NF instance requesting the certificate. TS 33.310 [3] in clause 6.1.3c describes that, as part of the SBA NF certificate profile, the subjectAltName (SAN) field should contain a URI-ID with the URI for the NF instance ID as an URN. This URI-ID needs to contain the identifier of the NF (e.g., SCP, SEPP, NRF, AF, etc.) instance (nfInstanceID), only using the format of clause 5.3.2 of TS 29.571 [7], what is a Universally Unique IDentifier (UUID). Thus, the flexibility that a service mesh could offer by integrating different types of services across heterogeneous environments (and in case of 5GS across different operator domains) is limited by the use of UUID as identifier.

Operator RA/CA would need to keep track on UUIDs in order to be able to verify and accept the CSRs, only based on those identifiers.

### 5.8.2 Security threats

A malicious or compromised NF instance can send a rogue CSR message using a compromised NF Instance Id. Thus, same UUIDs would be used for various NF instances, including the potential malicious or compromised NF. If the operator RA/CA does not have the mechanisms to verify and accept a trusted NF instance identity, then that malicious or compromised NF instance would fetch a valid certificate and cause different types of attacks in the SBA.

### 5.8.3 Potential security requirements

The certificate management framework should be able to manage and track the NF instance identifiers per end entity.

## 5.9 Key Issue #9: Automated Certificate Management for Network Slicing

### 5.9.1 Key issue details

A network slice can be understood as a logical network on top of a shared infrastructure. Network slicing is a key feature of 5G wireless network standards and allows operators to manage and orchestrate different logical networks for different kinds of service level requirements. For example, the communication services using network slicing may include:

- V2X services

- 5G seamless eMBB service with FMC

- massive IoT connections

There can be different network slices logically isolated based on Slice Service Type (SST) value, as shown in the following diagram:

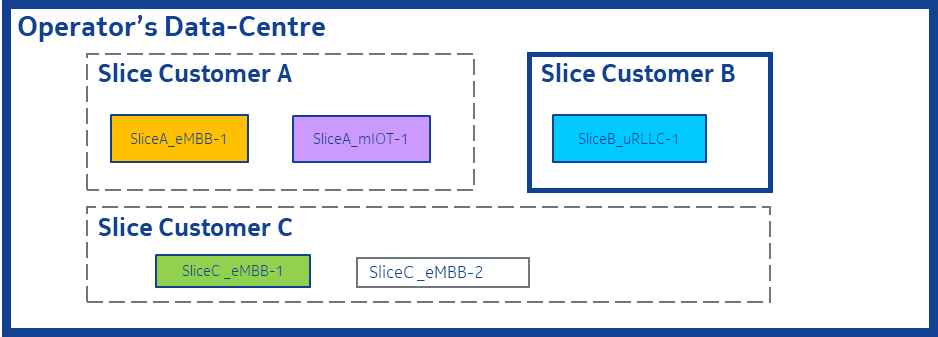


Figure 5.9-1: Different slices logically isolated for different slice customers

Network slicing facilitates a lot of vertical industries to create and manage logically separated resources across the 5G system dedicated for their own applications, while ensuring the desired service level agreements are always met.

Different slices allocated to different slice customers may have different requirements for automated certificate management. Generally, network slices need to rely on operator-provided services for automated certificate management services. Nevertheless, certain slices allocated to slice customers can require to perform management and operation tasks over operator CA, or even to use their own CA and certificate management procedures for all or part of the slice-specific services and NFs. For the latter case, both operator and slice customer need to agree on how establish the trust between operator and customer domain and interconnect their CAs, e.g., via cross-certification.

There are also several approaches to address access control and authorization of NFs for slicing in SBA. The NF can be deployed to serve a dedicated slice or multiple slices, and network slices can be dynamically or statically created and removed as per business needs. Depending on NF deployment option, the lifecycle of a NF can be different from a lifecycle of network slices assigned to the NF. Therefore, when considering the alignment between NF lifecycle and certificate lifecycle, the network slicing lifecycles can also need to be taken into account depending on NF and network slices deployment solution.

### 5.9.2 Security threats

A potential compromise or malfunction in the certificate management framework of the operator may impact in the certificate management framework of the slice and vice versa. E.g., if automated certificate updates are not completed before the expiration dates, it can lead to service / slice un-availability, requiring manual administration of certificates.

Misalignment between lifecycles of certificate and slices could lead to service unavailability for customer specific slices.

### 5.9.3 Potential security requirements

The framework should take into account the fact that certificates might belong to different domains, e.g. in deployment where different 3rd party slices co-exist and interoperate.

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | | | | | |
|  | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 |
| #1: Certificate Enrolment and MAnagement Framework (CEMAF) | X |  |  |  |  |  |  |  |  |
| #2: Using CMP protocol for certificate enrolment and renewal | X |  |  |  |  |  |  |  |  |
| #3: Secure initial enrolment of NF certificates |  | X |  |  |  |  |  |  |  |
| #4: Cross-Certification Based Trust Chain in the SBA Architecture |  |  |  | X |  |  |  |  |  |
| #5: Interconnection CA Based Trust Chain in the SBA Architecture |  |  |  | X |  |  |  |  |  |
| #6: OCSP based revocation procedure |  |  |  |  | X |  |  |  |  |
| #7: A solution addressing the relation between certificate lifecycle management and NF lifecycle management |  |  |  |  |  | X |  |  |  |
| #8: Enhance the security protection for Certificate parameters |  | X |  |  |  |  |  | X |  |
| #9: Certificates revocation query procedure based on NRF |  |  |  |  |  | X |  |  |  |
| #10: Solution to indicate and validate the purpose of the certificate |  |  |  |  |  |  | X |  |  |
| #11: OCSP Stapling addressing Key Issues #5 and #6 |  |  |  |  | X | X |  |  |  |
| #12: Automated Certificate Management for Network Slices |  |  |  |  |  |  |  |  | X |
| #13: Build initial trust for NF certificate enrolment |  | X |  |  |  |  |  |  |  |
| #14: Ensuring the management of bulk certificate updates |  |  | X |  |  |  |  |  |  |
| #15: Policy based certificate update/renewal |  |  | X |  |  |  |  |  |  |
| #16: Using ACME protocol for certificate enrolment and renewal | X |  |  |  |  |  |  |  |  |
| #17: Assurance of unique NF identifiers in certificates |  |  |  |  |  |  |  | X |  |
| #18: Slice specific initial enrolment procedure |  |  |  |  |  |  |  |  | X |

## 6.1 Solution #1: Certificate Enrolment and MAnagement Framework (CEMAF)

### 6.1.1 Introduction

The solution addresses key issue 1. The solution presents an overall architecture and the building blocks of an automated Certificate Enrolment and MAnagement Framework henceforth referred to as CEMAF. For some of the building blocks, the details are left out and deferred to potential other solutions addressing different key issues. The solution does take a stand on the protocols used.

### 6.1.2 Solution details

#### 6.1.2.1 General

It is assumed that the operator has already a PKI infrastructure supporting normal CA/RA operations similar to those required for base station or TLS entity enrolment as described in TS 33.310 [3]. Since this framework pertains to SBA entities, it is assumed that all of the framework's communications is HTTP-based and hence security can be provided by TLS. This would not incur big impact on NFs since they are expected to already support such protocols. OCSP [8] is HTTP based and CMPv2 can be encapsulated in HTTP messages [9]. Therefore, this assumption does not preclude re-using such protocols.

#### 6.1.2.2 Architecture

Figure 6.1.2.2-1 below illustrates the reference point based architecture of the framework. The ce1 reference point is used for enrolment and any other procedures related to certificate provisioning and updates. The ce2 reference point is used for certificate status checking. Accordingly, the corresponding functionalities have been split over two NFs. The CEMAF Enrolment Function CeEF is expected to support all the necessary functionality for provisioning and update of certificates to enrolling NFs. The CEMAF Management Function CeMF is expected to support maintenance functionalities such as revocation and certificate status information provisioning. The proposed grouping does not preclude that the functions are collocated or fully integrated in the CA/RA. This will depend on the final solutions.

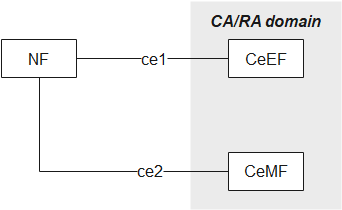


Figure 6.1.2.2-1 CEMAF reference point architecture

The motivation behind this split of the reference points is that most likely different credentials would be used to secure them. On the one hand, the CeEF needs to be able to interact with enrolling NFs that are yet to be provisioned by operator certificates. How trust is initially established and the credentials used to secure the enrolment procedures with the CeEF are deferred to other solutions. On the other hand, the CeMF is expected to be involved after the enrolment procedure and hence is expected to interact with NFs that have been already provisioned with valid certificates.

#### 6.1.2.3 Procedures

Figure 6.1.2.3-1 illustrates the grouping of the different CEMAF procedures. The description of the different blocks is given below.

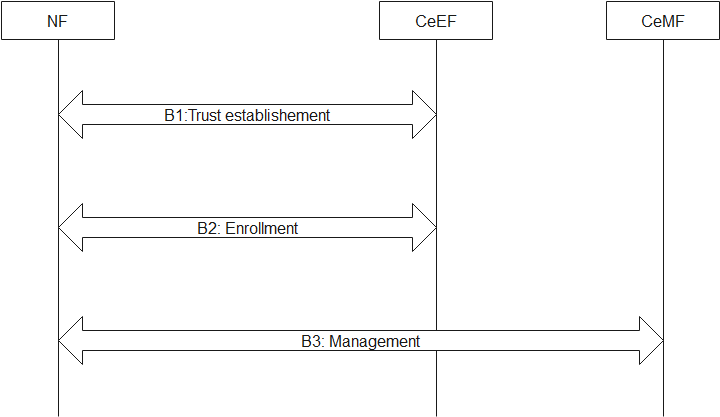


Figure 6.1.2.3-1 CEMAF procedures

- B1: This is the set of mechanisms and procedures that enables the CeEF and enrolling NFs to establish trust for the remaining operations. Solutions addressing key issue #2 will provide the means to realize this block.

- B2: This is the set of mechanisms and procedures that enables the CeEF to provision NFs with new certificates. Solutions addressing key issue #2 will provide the means to realize this block.

- B3: This is the set of mechanisms and procedures that enables the CeMF to manage certificates including updates, revocation, status notification and any other maintenance operation. Solutions addressing key issue #3, #5 and #6 will provide the means to realize this block. Observe that trust establishment may be needed as well for CeMF interaction.

NOTE: NFs are not expected to have the permission or ability to perform or trigger revocation by themselves.

### 6.1.3 Evaluation

This solution is a high-level description of the building blocks of a complete certificate management framework, here denoted by CEMAF. The solution does not propose any technical requirements and all the details for the building blocks have been left to other solutions.

## 6.2 Solution #2: Using CMP protocol for certificate enrolment and renewal

### 6.2.1 Introduction

This solution addresses Key Issue 1: Single certificate management protocol and procedures.

It is beneficial to have a single certificate management protocol and procedures for the certificate enrolment and renewal, to avoid manual certificate management which may lead to missing refreshment of certificates and usage of expired certificates.

CMP family is a good candidate to support automatic certificate enrolment and renewal procedure. CMP provides built-in integrity protection and authentication. CMP also provides revocation support with the operation of Revocation Request/Response, Revocation Announcement and CRL Announcement [10].

The CMP is a very solid and capable protocol, but the protocol offers a too large set of features and options which means implementation of all options is not realistic because this would take undue effort. And many details of the CMP protocol have been left open or have not been specified in full preciseness which increases burden on interoperability. Furthermore, automated scenarios for a machine-to-machine communication are not covered sufficiently. CMP is under update to overcome some limitations [11]. Also, 3GPP can specify a profile of CMP that specifies clearly which options and features of CMP are used and how they are used.

### 6.2.2 Solution details

#### 6.2.2.0 General

It is assumed that the secure communication channel setup and initial trust between NF and CA/RA is solved by the solution for Key Issue 2, so the solution of Key Issue 2 need also be taken into account as a complete solution for Key Issue 1.

Transport of CMP messages between end entities (network elements) and CA/RA uses HTTP-based protocol as specified in IETF RFC 6712 [9].

The NF entities use CMP protocol or out-of-band procedures to register at the CA/RA.

The NF entities use CMP protocol to initiate the certificate request to the CA/RA, and receive the certificate from the CA/RA in a secure and automated procedure.

The NF entities use CMP protocol to update the key and certificate to the CA/RA, and receive the renewed certificate from the CA/RA before the certificate expires in a secure and automated procedure.

NOTE 1: The CA/RA can be:

- either a stand-alone CA implementing a CMP server; or

- a CA having delegated certain tasks to an RA, which is in this solution operating the CMP server.

NOTE 2: The parameters embedded in the CMP certificate request need to be verified by the CA/RA for the supplied information by the NF in its request. So relevant information for the NF needs to be pre-provisioned out of band in CA/RA for NF's CMP certificate request validation.

#### 6.2.2.1 CMPv2 Profiling for SBA

##### 6.2.2.1.0 General

The following CMPv2 procedures are in the scope of certificate management for SBA:

- Certificate Enrolment:

- Certificate request: "CMPv2 Initialization Request" (for initial certificate requests) "CMPv2 Certification Request" (for subsequent certificate requests)

- Certificate Renewal:

- Key updates: "CMPv2 Key Update Request"

##### 6.2.2.1.1 General Requirements

The following requirements applies to CMPv2 usage in Service Based Architecture:

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

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

- 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 takes the operator root certificate from the certificates received in the initialization response. The selection is 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 supports 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]).

NOTE 1a: The secure communication channel setup and initial trust between NF and CA/RA is expected to be solved by the solutions for Key Issue 2, so the solution of Key Issue 2 needs also be taken into account as a complete solution for Key Issue 1. More precisely the initial authentication mechanisms to be used for initialization requests are subject to KI#2 conclusions.

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

- The RA/CA is configured with the root certificate of the operator.

- The RA/CA is 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 is 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 are configured into the RA/CA.

- The hash algorithms used before generating signatures in the protection field of PKIMessage and for proof-of-possession are the same as the hash algorithms specified in subclause 6.1.1 of TS 33.310 [3] for certificate signatures. The signature algorithms are the same as that used in the related certificate profile.

NOTE 2: [draft-ietf-lamps-cmp-algorithms-15 - Certificate Management Protocol (CMP) Algorithms](https://datatracker.ietf.org/doc/draft-ietf-lamps-cmp-algorithms/) [20] 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 of TS 33.310 [3].

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.

##### 6.2.2.1.2 Profile for PKIMessage

The following profile is applied to the PKIMessage as specified in IETF RFC 4210 [10]:

- 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 6.2.2.1.4 of TS 33.310 [3] in the profiling of the single PKI message bodies for requests sent by the NF. For the RA/CA the RA/CA private key is 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 6.2.2.1.4 of TS 33.310 [3] in the profiling of the single PKI message bodies.

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

##### 6.2.2.1.3 Profile for PKIHeader Field

The following profile is applied to the PKIHeader field as specified in IETF RFC 4210 [10]:

- The sender field contains the identity of the NF as EE. This identity is 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 contains 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 is of type MSG\_SIG\_ALG. The signature algorithm is 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 follows the same specification as given for usage before certificate signing in clause 6.1.1 of TS 33.310 [3].

- The usage of the transactionID field is mandatory. The recommended procedures for handling of the transactionID given in IETF RFC 4210 [10] are followed. The NF sets 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 IETF RFC 4210 [10] is used. The recipNonce in the very first message in the transaction is set to 0 by the sender and is disregarded by the recipient of the message.

##### 6.2.2.1.4 Profile for the PKIBody Field

6.2.2.1.4.1 General

The NF Instance certificate enrolment supports 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 [10] and IETF RFC 4211 [18] apply.

6.2.2.1.4.2 Initialization Request

The Initialization Request as specified in IETF RFC 4210 [10] contains exactly one CertReqMessages as specified in IETF RFC 4210 [10] and IETF RFC 4211 [18], i.e., the size of the sequence for CertReqMessages is 1 in all cases.

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

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

- The publicKey field of the CertTemplate is mandatory and contains 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 follows IETF RFC 5280 [19].

- The CertReqMessage contains a POP field of type ProofOfPossession. The POP field contains a signature field of type POPOSigningKey. The algorithmIdentifier field of the POPOSigningKey field contains 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 is mandatory and contains 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 [18], the sender field of POPOSigningKeyInput is used only if an authenticated identity has been established by the sender.

NOTE 3: The secure communication channel setup and initial trust between NF and CA/RA is expected to be solved by the solutions for Key Issue 2, so the solution of Key Issue 2 needs also be taken into account as a complete solution for Key Issue 1. More precisely the initial authentication mechanisms to be used for initialization requests are subject to KI#2 conclusions.

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

6.2.2.1.4.3 Initialization Response

The Initialization Response as specified in RFC 4210 [10] contains exactly one generated NF certificate, i.e., the size of the sequence for CertResponse is 1 in all cases.

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

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

The extraCerts field of the PKIMessage carrying the initialization response is mandatory and contains 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 is included in the extraCerts field.

NOTE: It is sufficient to use ExtraCerts field to contain the NF certificates chain and CMP message signing certificate chain. Using both ExtraCerts and caPubs fields will increase the complexity of implementation.

6.2.2.1.4.4 Certification request and Certification Response

The Certification Request (cr) and Certification Response (cp) messages as specified in RFC 4210 [10] and RFC 4211 [18] 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 apply equally, with the following exceptions:

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

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

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

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

6.2.2.1.4.6 Certificate Confirm Request and Confirmation Response

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

The PKIMessage sent by the NF is 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 is omitted.

#### 6.2.2.2 CMPv2 Transport

Transport of CMPv2 messages between end entities (network elements) and RA/CA is done using HTTP-based protocol as specified in IETF RFC 6712 [9], 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 [25] or virtual private networks see IETF RFC 6712 [9].

NOTE 2: Further details on the CMPv2 profiling will be addressed during normative work.

### 6.2.3 Evaluation

CMP family is a good candidate to support automatic certificate enrolment and renewal procedure. CMP provides built-in integrity protection and authentication.

The NF entities use CMP protocol to initiate the certificate request to the CA/RA and receive the certificate from the CA/RA in a secure and automated procedure.

The NF entities use CMP protocol to update the key and certificate to the CA/RA and receive the renewed certificate from the CA/RA before the certificate expires in a secure and automated procedure.

Transport of CMP messages between end entities (network elements) and CA/RA uses HTTP-based protocol as specified in IETF RFC 6712 [9], and the usage of HTTP over TLS (HTTPS) according to RFC 9110 [25] enhance the security of the transportation of CMP messages.

The CMP is a very solid and capable protocol, but the protocol offers a too large set of features and open options which increases burden on implementation and interoperability. Further details on the CMPv2 profiling need be addressed during normative work.

## 6.3 Solution #3: Secure initial enrolment of NF certificates

### 6.3.1 Introduction

To achieve automated certificate management for NFs in SBA, the establishment of the initial trust between NF and operator CA is a prerequisite to proceed with the certificate enrolment procedure (e.g., using CMPv2). Every NF is expected to have an initial trust identifier to establish that relation. For that purpose, the solution proposes to use an initial certificate, issued by a private CA in the same security (trust) domain of the NF. This private CA acts as an initial trust anchor function for the NFs in the initial enrolment. The private CA's root certificate is configured as trust anchor in the CA in the operator PKI.

The solution concept is represented in the figure 6.3.1-1.



Figure 6.3.1-1: Secure initial enrolment through Private CA

An alternative and/or complementary implementation of the solution may include a certificate management NF in the same security trust domain of the NF(s) and private CA, that is capable to deliver end entity certificates issued by the private CA to the NFs as a central certificate management entity in the security trust domain. When certificate management NF is used, the private keys need to be known by this entity, since it acts on behalf of NFs.

The alternative implementation of the solution is represented in figure 6.3.1-2.



Figure 6.3.1-2: Secure initial enrolment through Private CA and Certificate Management NF

### 6.3.2 Solution details

For NFs in 5GC SBA to fetch end entity X.509 certificates signed by an operator CA, the NFs are expected to have an identity that is trusted and accepted by the operator CA. The initial certificate for an NF, required to establish the initial trust between NF and operator CA can be obtained with the following procedure:



Figure 6.3.2-1: Procedure for secure initial enrolment

Precondition: A private CA is created and deployed within the same network/security (trust) domain of the NFs in 5GC SBA.

1) The public root certificate of the private CA is configured as trust anchor in the operator PKI

NOTE 1: The private CA could be a CA or sub-CA created by the operator PKI, or completely different CA deployed by the operator. In either case, the root CA public certificate of the private CA is installed in the operator CA as a trust anchor.

2) The NF generates a private-public key pair (if not pre-provisioned by NF management system) and the sends the Certificate Signing Request (CSR), that contains the public key, to the Private CA (e.g., PKCS#10, CMPv2).

NOTE 2: Since the NF and private CA are in the same security domain, implicit trust can be assumed. If initial trust needs to be enabled as per deployment security requirements, several implementation options may be considered. For example, the CSR in step 2a) may include the NF Instance Id, which would need to be pre-provisioned in Private CA to allow the validation. Alternatively, a pre-shared key along with a reference number (refnum) can be pre-configured at both ends.

3) The private CA signs the public key and issue a certificate for the NF.

4) The NF, or the Certificate Management NF on behalf of the NF, fetches the certificate and the trust chain from the private CA. This certificate is used by the NF as initial certificate for authentication to the operator CA.

5) The NF, or the Certificate Management NF on behalf of the NF, generates a new private-public key pair, if this is not pre-provisioned, to obtain the operator signed end entity certificate on its own public key from RA/CA using for example CMPv2.

6) The NF, or the Certificate Management NF on behalf of the NF, generates a certificate enrolment request, in case of CMPv2 Initialization Request (ir), which specifies the requested certificate (e.g., TLS entity certificate to be used in 5GC SBA (clause 6.1.3c of TS 33.310 [3])). The request includes proof of possession of the public key be verified by the operator CA (e.g., in CMPv2 by signing the POPOSigningKey field of the CertReqMsg with the relate private key to the public key to be certified by the operator CA), the Private CA signed initial certificate, and the certificate chain of the Private CA. The NF, or the Certificate Management NF on behalf of the NF, signs the request using the initial private key generated (or pre-provisioned) in step 2), and includes the digital signature in the request message.

7) The NF, or the Certificate Management NF on behalf of the NF, sends the signed certificate enrolment request to the operator CA.

9) The operator CA verifies the digital signature on the certificate enrolment request against the Private CA root certificate (trust anchor) using the initial certificate sent by the NF, and also verifies the consistency between the identity of the initial certificate and the requested entity certificate as well as the proof of possession of the private key for the requested certificate.

9) The operator CA generates the certificate for the NF and sends a signed response to the NF (or to the Certificate Management NF) which includes the issued certificate, the operator public root CA certificate, the signature of the response, and the operator CA certificate corresponding to the private key used to sign the response. The appropriate certificate chains for authenticating the operator CA certificates are also included.

NOTE 3: After the entity certificate is successfully issued by the CA through above steps, the private CA may revoke the initial certificate in order to mitigate the risk of misuse of such certificates.

### 6.3.3 Evaluation

The solution addresses the first security requirement of KI#2 related to building the initial trust with the operator CA/RA. It proposes a procedure to secure the initial enrolment of the NF certificates, as a pre-requisite to proceed with the certificate enrolment procedure when the NF fetches an operator certificate.

NOTE 1: The term 'Private CA' refers to a local CA used for NFs within SBA domain and may be managed by OAM system.

The procedure proposes to use an initial certificate for authentication to the operator CA, signed by a private CA within the same security trust domain of the NF.

This solution proposes as an alternative and/or complementary implementation, to use a certificate management NF to act on behalf of other SBA NFs. This would have limited impact on these NFs.

NOTE 2: The prerequisite of acquiring trustworthiness of the NF that is requesting the initial certificate to the private CA is assumed to be viable since the private CA may be managed by OAM system.

The solution requires the implementation of a private CA within the same security trust domain of the NF, so implicit trust between the private CA and NF is assumed. The root certificate of that private CA is pre-configured as trust anchor in the operator CA to enable the authentication of the NF during the initial certificate enrolment in operator CA.

The introduction of a local CA in the same trust domain as the NF may increase the threat surface, since the local CA is subject to the same threats and attack vectors as the NF. If multiple local CAs need to be implemented, the risk may consequently increase.

## 6.4 Solution #4: Cross-Certification Based Trust Chain in the SBA Architecture

### 6.4.1 Introduction

Before performing the automated certificate management protocol, the NFs in the SBA architecture need to obtain the corresponding certificate based on their role, which requires the trust chain of CA. Based on the proposed trust chain in this solution, the SBA entities can verify their obtained certificate and establish the TLS connection.

As per TS 33.310 [3], cross-certification can be used to establish the trust relationship between two authorities. When an authority A is cross-certified with authority B, the authority A has chosen to trust certificates issued by the authority B. Cross-certification process enables the users under both authorities to trust the other authority's certificates, which could benefit the certificate verification between SEPPs.

The proposed solution describes the cross-certification based CA trust chain. Based on the CA trust chain, the certificate of SBA entities can be verified. The solution addresses Key Issue #4: Trust Chain of Certificate Authority Hierarchy. This solution focuses on the certificate verification in terms of the chain of trust.

### 6.4.2 Solution details

#### 6.4.2.1 General architecture

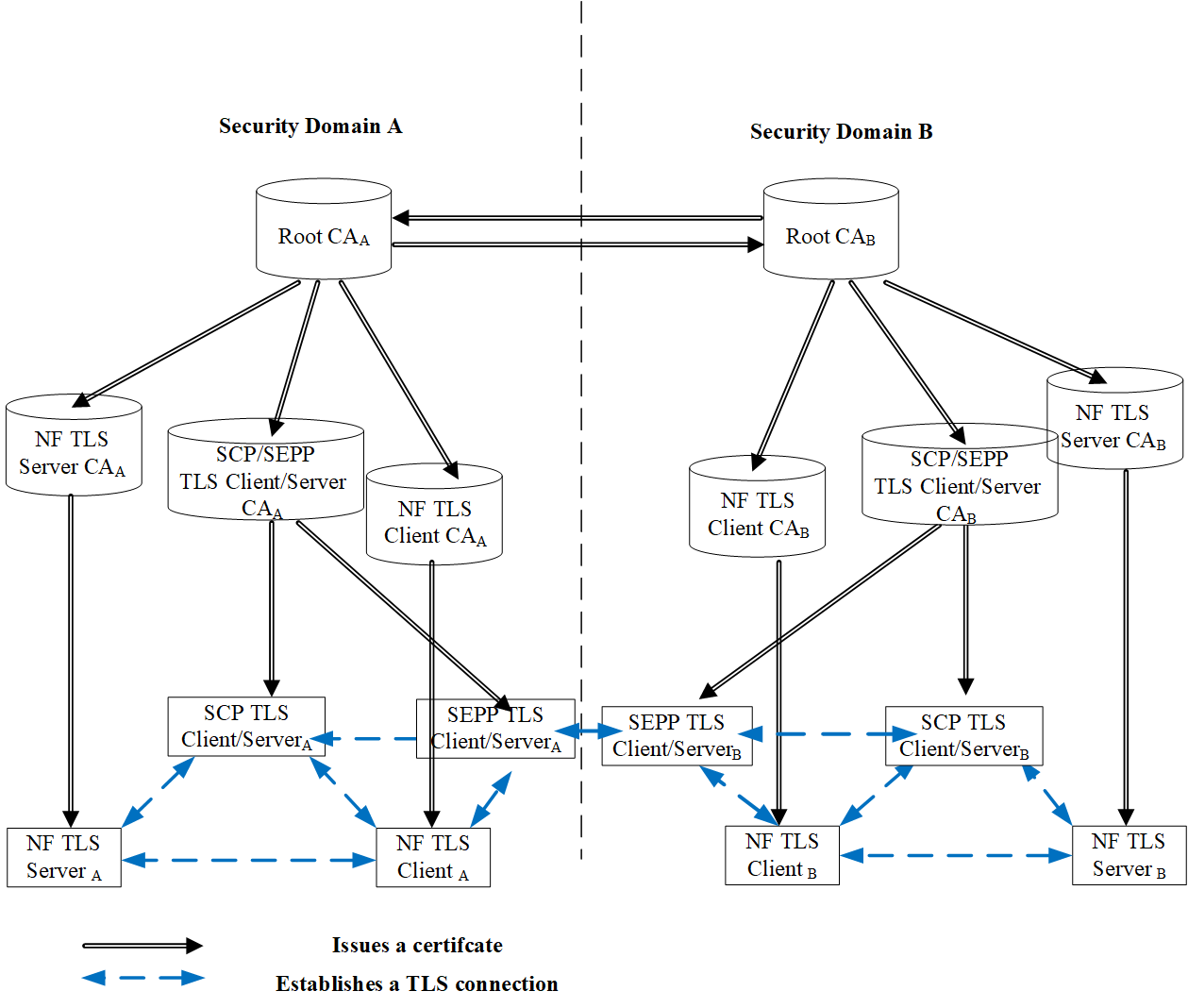


Figure 6.4.2.1-1: General Architecture

In the following, the architecture for issuing SBA certificates using TLS CAs is described.

- Root CA: A CA serves as the trust anchor in a chain of trust within a security domain. Each security domain can have only one root CA. The root CA generates the self-signed certificate as the root certificate. All certificates in this security domain are signed by the root certificate directly or indirectly. When the operators make an interconnection agreement, the root CA creates cross-certificates to ensure TLS entities of two different security domains are able to establish a secure connection. The created cross-certificates may be configured locally in each domain and be stored with the self-signed root certificate in the TLS entities.

- NF TLS client CA: A CA that issues end entity TLS client certificates to TLS entities within a particular operator's security domain.

- NF TLS server CA: A CA that issues end entity TLS server certificates to TLS entities within a particular operator's security domain.

- SCP TLS client/server CA: A CA that issues intra-domain certificates to SCP TLS client/server.

- SEPP TLS client/server CA: A CA that issues inter-domain certificates to SEPP TLS client/server.

- NF TLS server: TLS entities acting as 5G NF producers (e.g., AMF, SMF) are provisioned with TLS server certificates issued by the TLS server CA.

- NF TLS client: TLS entities acting as 5G NF consumers (e.g., AMF, SMF) are provisioned with TLS client certificates issued by the TLS client CA.

- SCP TLS client/server or SEPP TLS client/server: The SCP TLS client/server or SEPP TLS client/server act as the intermediary point between the NF TLS client and NF TLS server, assisting TLS entities to establish intra-domain or inter-domain TLS connections. Network functions (e.g., SCP, SEPP) that act as proxy functions in SBA architecture are provisioned with intra-domain or inter-domain certificates issued by the SCP TLS client/server or SEPP TLS client/server CA.

NOTE 1: Considering that some TLS entities can act as both NF producers and NF consumers, they may need both TLS client certificates and TLS server certificates.

NOTE 2: The dynamical management of cross certification is not supported in this solution.

NOTE 3: The PKI domain is related to the security domain defined by the operator, i.e., one PKI domain per security domain.

#### 6.4.2.2 Verify certificate in SBA architecture

**Verify the TLS certificate between intra-domain TLS entities:**

It is assumed that the NF TLS client and the NF TLS server are within the same security domain and are provisioned with the root CA's self-signed certificate before establishing the TLS connection. The certificate provisioning may be pre-configured or be provisioned during the enrolment. When the NF TLS client receives the certificate of the NF TLS server as part of the SSL/TLS handshake, NF TLS client performs the following procedure. If the mutual TLS for authentication of NF is used, both the NF TLS client and NF TLS server perform the following procedure.

1. The receiver checks to ensure that the sender's certificate is not expired. Considering that the sender's certificate is signed by the intermediate CA, the receiver tries to get the intermediate CA's certificate. Once the intermediate CA's certificate is obtained, the receiver uses the intermediate CA's public key to verify that the sender's certificate is properly signed.

2. Then, the receiver attempts to verify that the intermediate CA's certificate is trusted. Considering that the intermediate CA's certificate is signed by the Root CA, the receiver uses the provisioned self-signed root certificate to verify the signature of the intermediate CA's certificate.

3. In a successful transaction, the receiver will come to a self-signed root certificate that the receiver implicitly trusts. At this point, the receiver verifies the identity of sender, builds the chain of trust to the sender, and the intra-domain SSL/TLS handshake can proceed.

Note: The intermediate CA can be seen as the NF TLS server CA, the NF TLS client CA or the SCP TLS client/server CA.

**Verify the TLS certificate between inter-domain TLS proxy:**

It is assumed that the SEPP TLS client/serverA and the SEPP TLS client/serverB are in different security domains and are provisioned with their root CA's self-signed certificate (e.g., SEPP TLS client/serverA is provisioned with the Root CAA's self-signed certificate and SEPP TLS client/serverB is provisioned with the Root CAB's self-signed certificate). When the SEPP TLS client/serverA receives the certificate of the SEPP TLS client/serverB as part of the SSL/TLS handshake, the SEPP TLS client/serverA performs the following procedure. If the mutual TLS for authentication of NF is used, both SEPP TLS clients/servers perform the following procedure.

1. The receiver (i.e., SEPP TLS client/serverA) checks to ensure that the sender's (i.e., SEPP TLS client/serverB) certificate is not expired. Considering that the sender's certificate is signed by the SEPP TLS client/server CAB, the receiver will get the SEPP TLS client/server CAB's certificate. Once the SEPP TLS client/server CAB's certificate is obtained, the receiver uses the SEPP TLS client/server CAB's public key to verify that the sender 's certificate is properly signed.

2. Then, the receiver attempts to verify that the SEPP TLS client/server CAB's certificate is trusted. Considering that the SEPP TLS client/server CAB 's certificate is signed by the root CAB, the receiver tries to get the Root CAB's certificate. Once the Root CAB's certificate is obtained, the receiver uses the Root CAB's public key to verify that the SEPP TLS client/server CAB's certificate is properly signed.

3. Then, the receiver attempts to verify that the Root CAB's certificate is trusted. Considering that the Root CAB's certificate is signed by the Root CAA, the receiver uses the provisioned self-signed root certificate to verify the signature of the Root CAB's certificate.

4. In a successful transaction, the receiver will come to a self-signed root certificate that the receiver implicitly trusts. At this point, the receiver verifies the identity of sender, builds the chain of trust to the sender, and the inter-domain SSL/TLS handshake can proceed.

Note: The Root CAA issues the certificate of Root CAB, which is called cross-certificate. The TLS entities may request the cross-certificate as needed or be provisioned with the cross-certificate (store with the self-signed root certificate).

### 6.4.3 Evaluation

This solution proposes a cross-certification based trust chain in the SBA architecture, which fulfils the requirements of Key Issue #4: Trust Chain of Certificate Authority Hierarchy.

This solution supports the intra-domain SBA connection and the inter-domain SBA connection. For the intra-PLMN SBA connection, TLS entities can verify the received certificate by using the self-signed root certificate. For the inter-PLMN SBA connection, TLS entities can verify the received certificate by using the cross-certificate.

In this solution, each TLS entity can obtain the corresponding certificate based on its role. 5G NF producers (e.g., AMF, SMF) are provisioned with TLS server certificates. 5G NF consumers (e.g., AMF, SMF) are provisioned with TLS client certificates. The proxy functions in SBA architecture (i.e., SCP, SEPP) are provisioned with intra-domain or inter-domain certificates.

The TLS certificates used for intra-domain SBA connection are from different trust anchor than the TLS certificates used for inter-domain SBA connection because they are two separate security domains.

## 6.5 Solution #5: Interconnection CA Based Trust Chain in the SBA Architecture

### 6.5.1 Introduction

Before performing the automated certificate management protocol, the NFs in the SBA architecture need to obtain the corresponding certificate based on their role, which requires the trust chain of CA. Based on the proposed trust chain in this solution, the SBA entities can verify their obtained certificate and establish the TLS connection.

As per TS 33.310 [3], the interconnection CA can be used to issue certificates to the SEG CAs, TLS client CA or TLS server CA, of other domains with which the operator's SEGs and TLS entities have interconnection. Based on the certificate issued by the interconnection CA, the TLS entities under both authorities can trust the other authority's certificates, which could benefit the certificate verification between SEPPs.

The proposed solution describes the interconnection CA based trust chain. Based on the trust chain, the certificate of SBA entities can be verified. The solution addresses Key Issue #4: Trust Chain of Certificate Authority Hierarchy. This solution focuses on the certificate verification in terms of the chain of trust.

### 6.5.2 Solution details

#### 6.5.2.1 General architecture

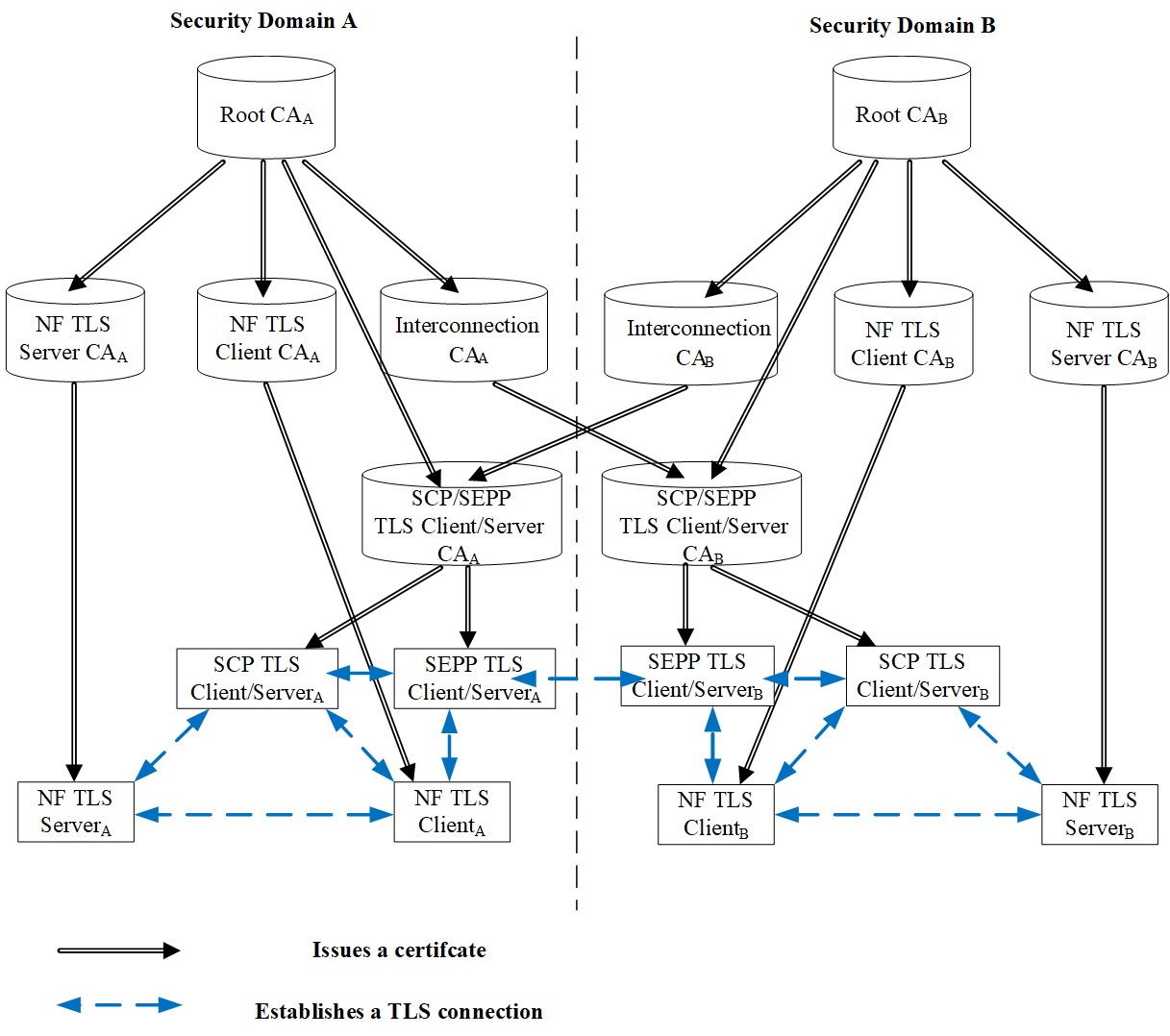


Figure 6.5.2.1-1: General Architecture

In the following, the architecture for issuing SBA certificates using TLS CAs is described.

- Root CA: A CA serves as the trust anchor in a chain of trust within a security domain. Each security domain can have only one root CA. The root CA generates the self-signed certificate as the root certificate. All certificates in this security domain are signed by the root certificate directly or indirectly.

- NF TLS client CA: A CA that issues end entity TLS client certificates to TLS entities within a particular operator's security domain.

- NF TLS server CA: A CA that issues end entity TLS server certificates to TLS entities within a particular operator's security domain.

- Interconnection CA: A CA that issues cross-certificates on behalf of a particular operator to SEPP TLS client/server CAs of other domains with which the operator's TLS entities have interconnection.

- SCP TLS client/server CA: A CA that issues intra-domain certificates to SCP TLS client/server.

- SEPP TLS client/server CA: A CA that issues inter-domain certificates to SEPP TLS client/server.

- NF TLS server: TLS entities acting as 5G NF producers (e.g., AMF, SMF) are provisioned with TLS server certificates issued by the NF TLS server CA.

- NF TLS client: TLS entities acting as 5G NF consumers (e.g., AMF, SMF) are provisioned with TLS client certificates issued by the NF TLS client CA.

- SCP TLS client/server or SEPP TLS client/server: The SCP TLS client/server and SEPP TLS client/server act as the intermediary point between the TLS client and TLS server, assisting TLS entities to establish intra-domain or inter-domain TLS connections. Network functions (e.g., SCP, SEPP) that act as proxy functions in SBA architecture are provisioned with intra-domain or inter-domain certificates issued by the SCP TLS client/server CA or SEPP TLS client/server CA.

NOTE 1: Considering that some TLS entities can act as both NF producers and NF consumers, they may need both TLS client certificates and TLS server certificates.

NOTE 2: The PKI domain is related to the security domain defined by the operator, i.e., one PKI domain per security domain.

#### 6.5.2.2 Verify certificate in SBA architecture

**Verify the TLS certificate between intra-domain TLS entities:**

It is assumed that the NF TLS client and the NF TLS server are within the same security domain and are provisioned with the root CA's self-signed certificate before establishing the TLS connection. The certificate provisioning may be pre-configured or be provisioned during the enrolment. When the NF TLS client receives the certificate of the NF TLS server as part of the SSL/TLS handshake, NF TLS client performs the following procedure. If the mutual TLS for authentication of NF is used, both the NF TLS client and NF TLS server perform the following procedure.

1) The receiver checks to ensure that the sender's certificate is not expired. Considering that the sender's certificate is signed by the intermediate CA, the receiver will get the intermediate CA's certificate. Once the intermediate CA's certificate is obtained, the receiver uses the intermediate CA's public key to verify that the sender's certificate is properly signed.

2) Then, the receiver attempts to verify that the intermediate CA's certificate is trusted. Considering that the intermediate CA's certificate is signed by the Root CA, the receiver uses the provisioned self-signed root certificate to verify the signature of the intermediate CA's certificate.

3) In a successful transaction, the receiver will come to a self-signed root certificate that the receiver implicitly trusts. At this point, the receiver verifies the identity of sender, builds the chain of trust to the sender, and the intra-domain SSL/TLS handshake can proceed.

NOTE: The intermediate CA can be seen as the NF TLS server CA, the NF TLS client CA or the SCP TLS client/server CA.

**Verify the TLS certificate between inter-domain TLS proxy:**

It is assumed that the SEPP TLS client/serverA and the SEPP TLS client/serverB are in different security domains and are pre-provisioned with their root CA's self-signed certificate (e.g., SEPP TLS client/serverA is provisioned with the Root CAA's self-signed certificate and SEPP TLS client/serverB is provisioned with the Root CAB's self-signed certificate). When the SEPP TLS client/serverA receives the certificate of the SEPP TLS client/serverB as part of the SSL/TLS handshake, the SEPP TLS client/serverA performs the following procedure. If the mutual TLS for authentication of NF is used, both SEPP TLS clients/servers perform the following procedure.

1) The receiver (i.e., SEPP TLS client/serverA) checks to ensure that the sender's (i.e., SEPP TLS client/serverB) certificate is not expired. Considering that the sender's certificate is signed by the SEPP TLS client/server CAB, the receiver will get the SEPP TLS client/server CAB's certificate. Once the SEPP TLS client/server CAB's certificate is obtained, the receiver uses the SEPP TLS client/server CAB's public key to verify that the sender's certificate is properly signed.

2) Then, the receiver attempts to verify that the SEPP TLS client/server CAB's certificate is trusted. Considering that the SEPP TLS client/server CAB's certificate is signed by the Interconnection CAA, the receiver will get the Interconnection CAA's certificate. Once the Interconnection CAA's certificate is obtained, the receiver uses the Interconnection CAA's public key to verify that the SEPP TLS client/server CAB's certificate is properly signed.

3) Then, the receiver attempts to verify that the Interconnection CAA's certificate is trusted. Considering that the Interconnection CAA's certificate is signed by the Root CAA, the receiver uses the provisioned self-signed root certificate to verify the signature of the Interconnection CAA's certificate.

4) In a successful transaction, the receiver will come to a self-signed root certificate that the receiver implicitly trusts. At this point, the receiver verifies the identity of sender, builds the chain of trust to the sender, and the inter-domain SSL/TLS handshake can proceed.

### 6.5.3 Evaluation

This solution proposes an interconnection CA based trust chain in the SBA architecture, which fulfils the requirements of Key Issue #4: Trust Chain of Certificate Authority Hierarchy.

This solution supports the intra-domain SBA connection and the inter-domain SBA connection. For the intra-PLMN SBA connection, TLS entities can verify the received certificate by using the self-signed root certificate. For the inter-PLMN SBA connection, TLS entities can verify the received certificate by using the interconnection CA certificate.

In this solution, each TLS entity can obtain the corresponding certificate based on its role. 5G NF producers (e.g., AMF, SMF) are provisioned with TLS server certificates. 5G NF consumers (e.g., AMF, SMF) are provisioned with TLS client certificates. The proxy functions in SBA architecture (i.e., SCP, SEPP) are provisioned with intra-domain or inter-domain certificates.

The TLS certificates used for intra-domain SBA connection are from different trust anchor than the TLS certificates used for inter-domain SBA connection because they are two separate security domains.

## 6.6 Solution #6: OCSP based revocation procedure

### 6.6.1 Introduction

The solution addresses key issue 5. The provisioning of new certificates is left out for other solutions addressing key issue 1 and 2.

### 6.6.2 Solution details

#### 6.6.2.1 General

The solution relies on the use of the Online Certificate Status Protocol OCSP [8]. The necessary parameters for OCSP usage are included in the certificates as per the certificate profile for SBA entities in clause 6.1.3c.3 of TS 33.310 [3]. Such parameters are assumed to be provisioned in the certificate during the enrolment procedure which is left for solutions addressing key issues 1 and 2.

#### 6.6.2.2 Procedure

Both server and client NFs are expected to check the status of each other's certificates during the TLS handshake using the OCSP protocol based on the parameters included in the certificates (if any). In particular for NF clients, they are expected to always check the status of the server side certificate by contacting the OCSP server unless stapling is used by the NF server. Observe that within the 5G Core, stapling can be used by the "high load" server NFs such as the UDM or NRF to alleviate the burden on the OCSP servers and reduce the signalling traffic. In case the OCSP server reply is other than valid, then the OCSP client, i.e., one of the NFs involved in the handshake, terminates the connection and considers the establishment of TLS not possible with the other end.

When revocation status is unknown (e.g., due to OCSP server unreachable), the OCSP client, i.e., one of the NFs involved in the handshake, continue the TLS connection establishment, and raise alarm for awareness. The alarm details are out of scope from 3GPP specifications. As an implementation example of such a handling, the NF logs the session ID and parameters to identify the NF entities involved in the handshake and the reason for failure and the NF raises an alarm. Further actions can be taken by the operator based on local policy.

NFs are expected to regularly check the status of their own certificates. When to do this regularly could be left to implementation or based on a configuration parameter controlled by the operator. Typically, an NF could check its own certificate status after a failure of TLS tunnel establishment.

### 6.6.3 Evaluation

This solution addresses key issue 5 on "certificates revocation procedures". The solution relies on the OCSP protocol [8] which is a well-established standard protocol for certificate management. The certificate profile for SBA includes the necessary provisions for the usage of OCSP as described in clause 6.1b of TS 33.310 [3]. Therefore this solution has minimal standard impact. Furthermore, most of the existing TLS implementations already include support for OCSP.

## 6.7 Solution #7: A solution addressing the relation between certificate lifecycle management and NF lifecycle management

### 6.7.1 Introduction

This solution addresses the key issue #6 (relation between certificate management lifecycle and NF management lifecycle). As stated in the key issue details, NF lifecycle management (LCM) and certificate LCM have some relations that need to be considered in the certificate management mechanism. Since it is better to keep certificate and registration authorities (CA/RA) as plain as possible for easy deployments, as well as for performance reasons, this solution introduces a new network entity called as Certificate Management Network Entity (CMNE) that is similar to the certificate management function, introduced in [12], being responsible for the synchronization of the VNF LCM with the certificate LCM events.

The CMNE is responsible for the synchronization between certificate related events and NF related events. To achieve this role successfully, the CMNE communicates with the CA/RA and NRF. To have a fine-grained control on both the certificate lifecycle related events and (V)NF lifecycle events, the CMNE also communicates with the orchestration entities at the virtualization layer in NF cloud deployments. For example, the CMNE can be an authorized consumer of the NFV-MANO exposed interfaces [13].

### 6.7.2 Solution details

The CMNE informs the CA/RA about the events so that CA/RA can take further actions related to the NF lifecycle events. For certificate lifecycle related events triggered by CA/RA, the CA/RA informs the CMNE and then CMNE transfers this information to the NRF and the virtualization orchestration entities.

Figure 6.7.2-1 depicts a high-level procedure for synchronization of NF and certificate lifecycle management. Step 1 represents the information flow related to certificate lifecycle events; step 2 shows the high-level flow related to NF lifecycle related events triggered by the virtualization orchestration entities. For example, when the certificate of a NF instance is revoked, the CMNE is informed by the CA/RA and then the CMNE informs to the NRF so that the NRF may take further actions for the affected NF profiles. Another example is when an NF termination related information is received from the orchestration entity, the CNME informs the CA/RA to revoke the certificate of the corresponding NF.



Figure 6.7.3-1: A high-level procedure for synchronization between certificate lifecycle management and NF lifecycle management

1. Certificate management event triggered by CA/RA

1a. NRF subscribes on NF certificate status from CMNE. The subscription can be applied for all NFs registered in the NRF.

1b. CMNE is informed by the CA/RA about NF certificate status change, or the CMNE may periodically query the certificate revocation status of all subscribed NFs from the CRL or the OCSP server and detect the changes.

1c. CMNE notifies NRF about the NF certificate status change, and NRF may take further actions for the affected NF profiles (e.g., NRF sets NF status as SUSPENDED or UNDISCOVERABLE when the certificate status is revoked).

2. Certificate management event triggered by Virtualization orchestration

2a. CMNE subscribes on VNF status from virtualization orchestration entity. The subscription can be applied for all NFs that are subscribed by the NRF(s) in step 1a.

2b. Virtualization orchestration entity notifies CMNE about VNF status change (e.g., VNF termination).

2c. CMNE may take further action about NF certificate change by interacting with CA/RA. For example, CMNE may request CA/RA to revoke the certificate when VNF is terminated.

NOTE 1: The interface between CA/RA and CMNE is proprietary and out of scope of 3GPP.

NOTE 2: The interface between CMNE and virtualization orchestration is out of scope of 3GPP.

### 6.7.3 Evaluation

This solution introduces a new entity called as Certificate Management Network Entity (CMNE) that is responsible for the synchronization between certificate related events and NF related events. For certificate management event triggered by CA/RA, CMNE transfers this information to the NRF for further actions. For VNF lifecycle management event triggered by Virtualization orchestration, CMNE transfers this information to the CA/RA for further actions. To achieve this role successfully, the CMNE need communicate with the CA/RA, NRF and orchestration entities at the virtualization layer in NF cloud deployments.

This solution introduces a new subscription service provided by CMNE and consumed by NRF, so that NRF is aware of NF certificate status change. The NRF needs to maintain the certificate status for each NF.

## 6.8 Solution #8: Enhance the security protection for Certificate parameters

### 6.8.1 Introduction

This solution addresses KI#2 and KI#8.

After an NF is instantiated, it needs to request a certificate from the Certificate Enrolment Function (CeEF)/CA. As highlighted in the security threat, it is important that CeEF/CA can verify the NF's parameters in the NF profile before issuing the certificate.

The solution proposes that the NF is involved and provides the signature of NF profile in order to give the necessary assurance to the CeEF/CA for issuing a certificate.

### 6.8.2 Solution details

#### 6.8.2.1 General

It is assumed that the OAM configures the NF profile during the NF initialization phase. In this case, the OAM can help to evaluate the NF profile for its integrity. When applying for a certificate, the NF may provide some parameters from the NF profile, e.g. NF instance ID, NF type, FQDN/IP address, PLMN ID, etc.

CeEF/CA verifies the integrity of the provided parameters during the certificate enrolment procedure to make sure a correct certificate can be issued. To accomplish the verification. The NF provides the signature of the parameters in NF profile in certificate enrolment request to build trust. The OAM signature can apply to the entire NF profile. Alternatively, if the certificate request only covers some parameters from the NF profile, the OAM signature can be limited to these parameters.

#### 6.8.2.2 Procedure

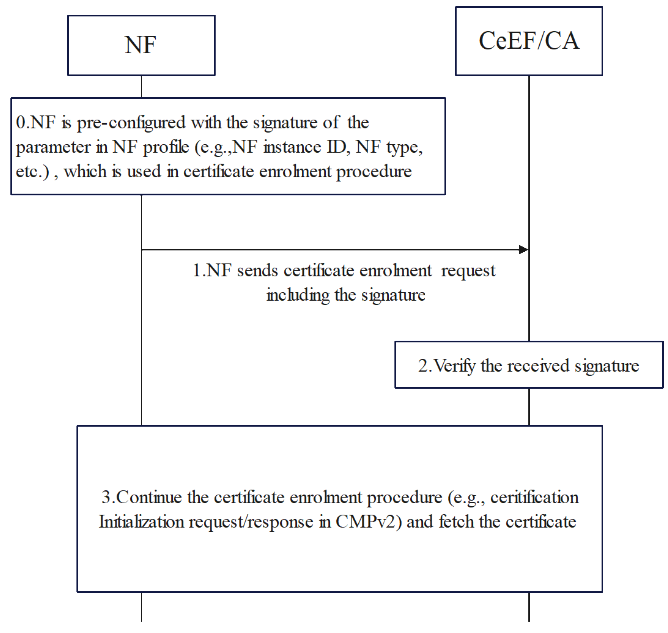


Figure 6.8.2.2-1: The Procedure of CeEF/CA verifying NF profile

0. The NF is pre-configured with the signature of the parameter in NF profile (e.g., NF instance ID, NF type, etc.), which is used in certificate enrolment procedure. The signature can be generated by OAM. For example, OAM can establish a trust relationship with the CeEF/CA in advance by obtain the certificate from CeEF/CA, and then the OAM can configure its signature for the NF.

NOTE 1: the signature can be either sent to NF with its profile or requested by NF after the instantiation phase in case of some parameters are NF self-generated (e,g., NF instance id).

1. The NF sends certificate enrolment request to CeEF/CA including the signature of NF profile to request a new certificate. For example, in case of CMPv2 Initialization Request (ir) [10], the signature can be included in the senderKID or any extended Fields of ir, as long as the CeEF/CA can verify the integrity of the NF profile in the enrolment procedure. How an NF establishes the security connection with CeEF/CA is left to implementation or reference to other solutions.

NOTE 2: Care needs to be taken when verifying the signature in order to avoid verification failures due to misalignment in the arrangement of the parameters.

2. The CeEF/CA verifies the received parameters, including the NF profile signature. If the verification is not successful, the CeEF/CA sends a failure response. How to verify the signature of OAM is left to implementation. e.g., as proposed in step 0, OAM obtains the certificate from CeEF/CA, and then CeEF/CA can verify the OAM signature by verifying the certificate.

3. If the NF profile signature is verified successfully, CeEF/CA continue the certificate enrolment procedure with NF (e.g., NF and CeEF/CA can use CMPv2 as specified in IETF RFC 4210 [10] or specified in other solutions).

### 6.8.3 Evaluation

This solution addresses KI#2 and KI #8 by enhancing the integrity of NF identifier during the certificate enrolment.

For KI#2, this solution mainly addresses the security threat: If certificate enrolment parameters are tampered, the integrity is violated which results into failure of initial trust.

The solution may impact the NF certificate enrolment phase. NF is involved and provides the signature of NF profile in order to give the necessary assurance when requesting the certificate.

The solution may impact existing interfaces.

The solution induces an overhead on the CeEF/CA side for performing the additional checks.

Care needs to be taken in deployments where CeEF is a separate entity (not co-located with the CA) since this would increase the attack surface for the enrolment procedure.

## 6.9 Solution #9: Certificates revocation query procedure based on NRF

### 6.9.1 Introduction

This solution addresses KI#6.

After a certificate expires or is revoked, the NF may still be discovered by the NRF during the NF service discovery procedure, when the certificate of a producer NF instance has been revoked without the knowledge of the NRF, it will lead to inconsistent status in NRF and reduce the service availability. For example, when the NF consumer setups a TLS connection with the NF producer, the connection between the NF consumer and the NF producer may fail because the certificate of the NF producer is no longer valid. This impact network efficiency.

### 6.9.2 Solution details

#### 6.9.2.1 General

Based on an existing service discovery procedure, this solution combines the certificate revocation status query with the service discovery procedure, thereby optimizing the efficiency of certificate revocation status query.

This solution also prevents the NRF from providing an NF producer to an NF consumer after the NF producer's certificate expires or is revoked, that may cause connection setup failures.

#### 6.9.2.2 NF service Registration procedure

An NF carries its own certificate during registration. The NRF stores the certificate information as the NF context. In addition, when the certificate of the NF is renewed, this certificate needs to be updated in the NRF.

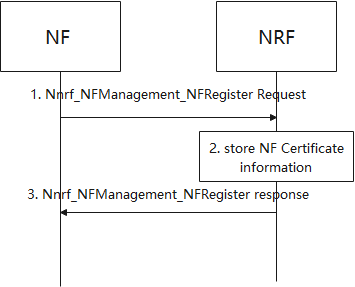


Figure 6.9.2.2-1 NRF store the certificate validity during NF registration

1. NF sends Nnrf\_NFManagement\_NFRegister Request message to NRF with all certificates of NF including the certificates in the certificate chain.

2. NRF stores the certificate information of certificates from NF. The certificate information can be certificate ID, certificate type and certificate validity information.

3. NRF acknowledge NF Registration is accepted via Nnrf\_NFManagement\_NFRegister response.

#### 6.9.2.3 NF/NF service discovery in the same PLMN

In the service discovery procedure, the NRF determines whether to provide the NF producer to the NF consumer based on the certificate status of the NF producer.

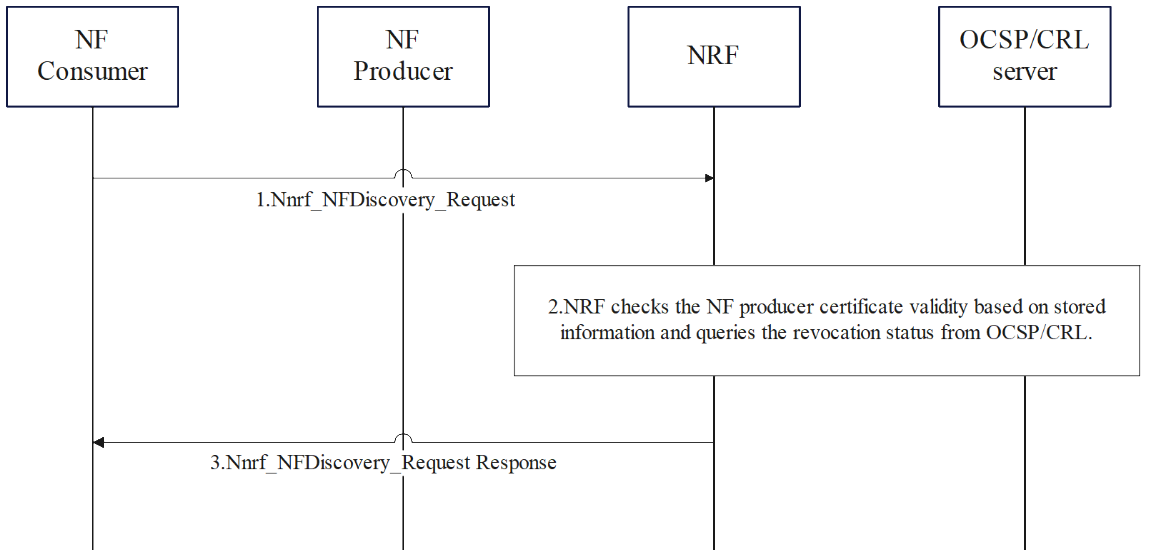


Figure 6.9.2.3-2 NRF queries NF producer certificate when NFDiscovery\_request

1. NF consumer initiates service discover procedure. The NF consumer sends the Nnrf\_NFDiscovery\_Request message to discover an NF producer for the service. NRF determines a required candidate NF producer list as specified in TS 23.501 [5].

2. After determining the candidate NF producer list, the NRF checks the NF producers' certificate validities based on store information in 6.Y.2.2 and queries the certificate revocation status from the CRL or the OCSP server. The NRF can interact with the CRL/OCSP server directly or through a proxy depending on the implantation of the CRL/OCSP server. Certificate validity is the information preconfigured by CA/RA. The revocation status is to indicate whether the certificate is revoked. There are some cases that leads to the revocation (e.g., private key leak, the re-orchestration of NF, etc.)

NOTE: NRF can have a storage mechanism and can be aligned with the update period of the OCSP server (e.g. OCSP server can announce its thisUpdate time and nextUpdate Time as specified in IETF RFC 6960 [8]). it may be done in the implementation level to reduce the signalling.

3. NRF sends Nnrf\_NFDiscovery\_Request Response message to NF consumer.

If multiple NRFs are required to discovery a NF producer, NRF can forward the request to other NRFs as specified in TS 23.502 [14].

### 6.9.3 Evaluation

In this solution, the NRF checks the certificate status from the OCSP/CRL server, so that the NF discovery service can only provide the NF producer with a valid certificate, which improve the service availability.

This solution is expected to add more storage requirement in the NRF, and more signalling and queries during the NF discovery request of NRF. The OCSP/CRL server query can be implemented during the existing NF producer checks specified in clause 6.3 in TS 23.501 [2].

This solution assumes that the NRF can determine the mapping between the certificate and the NFp. This functionality is not defined as part of NRF role in any other 3GPP specifications. The NRF can maintain this mapping locally or indirectly in/through another network entity. Though this can be left to implementation, it does incur additional impact on the NRF.

Care needs to be taken when deploying such solutions in order to avoid unnecessary overhead such as when OCSP/CRL information is provided already in the certificates in which case the checks by the NRF would be also performed by the consumer during the TLS handshake.

Care needs to taken when caching is used by the consumer in which case whatever information is cached in the consumer needs to be kept up-to-date, otherwise the solution will not completely eliminate the risk of "late" failure.

The optimization proposed by this solution works for the communication between the NFc and the NRp, not the communication between the NF and the NRF.

## 6.10 Solution #10: Solution to indicate and validate the purpose of the certificate

### 6.10.1 Introduction

This solution addresses the security requirements exposed in key issue #7 related to the association of multiple certificates which are used for different purposes within a single Network Function (NF) in the 5GC SBA context, namely:

- TLS client EE certificates

- TLS server EE certificates

- Certificates for signing the access tokens for service access authorization (for NRFs acting as OAuth 2.0 authorization servers)

- Certificates for encrypting HTTP application layer protection of messages between SEPPs

- Certificates for signing Client credentials assertion (CCA) tokens (for NF consumers)

NOTE: Other purposes may be added for X.509 certificates in the context of 5GC SBA.

The basic concept is to provide the purpose(s) of the certificate to be used in 5GC SBA in the CSR (Certificate Signing Request) to the Certification Authority (CA). The CA should validate the request and add the purpose(s) in the certificate, specifically in the Extended Key Usage (EKU) field.

When the NF consumer (NFc) request a service to a NF producer (NFp), SCP or SEPP, and sends its certificate for authentication (mutual TLS authentication), or when the NFc sends a CCA token (in Nnf service request) that can be checked against the public key certificate (as indicated by NFc in "x5u" or "x5c" parameter in CCA) by the NFp among other situations, the receiver of the certificate should check whether the received purpose in the certificate matches the content of the service request. If it does not match, the receiver of the certificate should reject the request with a corresponding error code.

### 6.10.2 Solution details

The first step of the procedure for the NF is to fetch a certificate that includes the purpose(s) of usage in the context of 5GC SBA (e.g., TLS authentication, CCA signing, etc.). The purpose(s) of the certificate should be added in Extended Key Usage (EKU) field of X.509 public key certificate by the CA server:

- If an automated enrolment protocol is used by the NF to fetch the certificate, the NF should indicate the purpose(s) of the certificate in the certificate request message to the CA. E.g., "ir" or "cr" messages in CMPv2.

- The OAM fetches the certificate from the CA with indicated purpose and install it manually in the NF

Therefore, the solution proposes to use Extended Key Usage (EKU) extension of X.509 certificate to indicate the purpose of the certificate (e.g., TLS, JSON signing, etc.) according to RFC 5280 [19] and draft-ietf-lamps-nf-eku-00 [21].

The receiver of the certificate should validate the purpose indicated in the EKU extension of the certificate, with the actual purpose being used in the service request (e.g., TLS authentication, CCA signing, etc.).

Figure 6.10.2-1 illustrates the procedure with an example that combines a successful validation of the certificate to be used for TLS mutual authentication (NFc à SCP), but it is rejected when used for CCA signing (NFc à NFp).



Figure 6.10.2-1: Validation of the purpose of the certificate

1) The CA is configured with policies intended to validate the purpose of the certificate requests from NFs.

2) The NFc sends a certificate request to the CA with PURPOSE = id-kp-clientAuth, what indicates that the NFc is requesting a certificate in principle intended to be used only for TLS client authentication purposes.

3) The CA validates the purpose of the certificate with predefined policies and adds the purpose in the certificate (EKU extension).

4) The CA sends the certificate with purpose information in EKU extension field to the NFc.

5) The NFc initiates a TLS connection with SCP, which requires mutual authentication.

6) The SCP validates the TLS client authentication, including the purpose of the certificate and allows the TLS connection.

7) The NFc sends a service request to NFp via SCP with CCA token in 3gpp-Sbi-Client-Credentials custom header. Let's assume that NFc misuses the single purpose TLS client certificate by signing the CCA token with the associated private key and including the associated public key certificate (chain) in "x5c" parameter, or, alternatively, adding X.509 URL in "x5u" parameter for this in the signed CCA token.

8) The purpose of the certificate used to verify the signature of the CCA token does not include id-kp-jws, which indicates that the public key encoded in the certificate has not been certified to be used for validating the JWS signature, so the Nnf service request is rejected by the NFp.

9) The NFp sends the service response rejecting the request with 403 Forbidden response where the cause attribute is set to "CCA\_VERIFICATION\_FAILURE", as described in clause 6.7.5 in TS 29.500 [22].

### 6.10.3 Evaluation

The solution addresses the security threats and potential security requirements of KI#7 by proposing a procedure which allows to indicate and verify the purpose of the certificates in SBA.

The solution proposes the use of Extended Key Usage extension of X.509 certificate to indicate the purpose of the certificate being used in SBA, however the actual RFC 5280 (May 2008) [19] only specifies among other purposes the usage of the certificate for TLS client and TLS server authentication. To specify the usage of the certificate for JSON signing and encryption (e.g., CCA) the solution relies upon the IETF draft RFC: draft-ietf-lamps-nf-eku-00 [21].

## 6.11 Solution #11: OCSP Stapling addressing Key Issues #5 and #6

### 6.11.1 Introduction

This solution addresses key issue #5 by introducing, within the context of 5GC SBA, the revocation procedures associated to standard OCSP stapling [15] and [16], whose profile can be found in clause 6.1b of TS 33.310 [3]. The use of the Certificate Status extension, commonly referred to as "OCSP stapling", aims to offload the consumption of client resources and the contact with the OCSP server. OCSP stapling makes the server responsible of performing OCSP requests, thus reducing the latency and increasing the availability of the revocation service, i.e., the server timestamps and caches the most recent OCSP responses, so that those can be attached ("stapled") to the clients TLS handshakes responses together with the certificates, even during short CA and/or OCSP server outages. Every NF should get the OCSP stapling of its end entity (EE) certificate from OCSP periodically.

The solution addresses the relation of the certificate management lifecycle and NF management lifecycle described in key issue #6, specifically the reconciliation of certain NF lifecycle processes such as the discovery procedure performed by the NRF with the validity period of the certificates, by adding the OCSP stapling of the NF EE certificate in the NF profile. Consequently, every NF should register and update its profile with OCSP stapling of its EE certificate in the NRF. The NRF should check the NF producer's (NFp) OCSP stapling from its profile and accordingly responds to the NF consumers discovery, access token or subscription requests by including only the NFps with valid stapling.

### 6.11.2 Solution details

Before the first registration of the NFp in the NRF, the NFp should get the OCSP stapling for its EE certificate from the OCSP server, and then embed this information as part of the NF profile registered in the NRF.

The OCSP stapling contains the validity and revocation status of the EE certificate provided by the OCSP server, despite its initial validity availed from the CA. The OCSP server will always have the latest information about the NF certificate status. The OCSP stapling of the EE certificate can be updated by the periodic requests from the NF to the OCSP server, or by preconfigured OCSP server policies. The OCSP stapling updates should trigger the corresponding update of the information in the NF profile within the NRF.

Figure 6.11.2-1 illustrates the procedure:



Figure 6.11.2-1: OCSP stapling procedure for NFp validation in NRF

1) NFp sends a OCSP stapling request for its EE certificate to OCSP server.

2) OCSP server sends the OCSP stapling response to NFp with the latest status of the EE certificate.

NOTE: Alternatively, OCSP server may push stapling updates to the NFp based on operator security policy.

3) NFp registers or updates its NF profile in the NRF including the latest status of the EE certificate.

4a) NRF register the NFp profile, which contains the OCSP stapling information, i.e., the latest status of the EE certificate.

4b) NRF validates the OCSP stapling message and updates the NF profile.

5) NFc sends a request to NRF for a NFp, e.g., discovery request, access token request, subscription request.

6a) Checks the OCSP stapling information of the candidate NFps (along with other parameters in the profile)

6b) If the status of the EE certificate is OK, the NFp is considered in the response.

7) NRF response to NFc request with a NFp whose EE certificate is valid.

If the NFp instance is removed from the infrastructure by the corresponding management function, the NF profile is deactivated from the NRF, and the management function and/or NRF should inform the operator RA/CA to proceed with the revocation of the certificate. This procedure is left to implementation.

### 6.11.3 Evaluation

The solution addresses the key issue #5 by using one certificate revocation schema known as OCSP stapling. OCSP stapling is one of the revocation schemas profiled in TS 33.310 [3]. In general, OCSP improves the latency and performance of the revocation related procedures by providing an online service, thus the number of revoked certificates is not a concern. Specifically, OCSP stapling enhances the availability of the service in case of CA or OCSP responder outages, since the server caches the most recent OCSP responses.

The solution also proposes a procedure to address the relation between certificate management lifecycle and NF management lifecycle described in key issue #6, by registering and updating the NF profile with OCSP stapling information. The status of the certificate of the NFp will be verified by the NRF before responding the request of the NFc, thus NRF will always respond with a NFp whose EE certificate is valid.

The solution has the following impact in existing architecture and procedures:

- the implementation of an OCSP service as part of the PKI infrastructure of the operator

- the support of OCSP stapling by the NFs

- the update of the NF profile with OCSP stapling information

- the verification of the OCSP stapling information by the NRF

Observations:

- the update of the OCSP stapling information can represent an issue if the certificate is revoked before next OCSP stapling is renewed, since neither NRF nor NF will come to know about the actual OCSP stapling, i.e., status of the certificate.

- the solution addresses NFp-NRF segment, responding to the use case indicated in the KI #6 description. The registration of the NFc is optional (clause 13.4.1.1.1, TS 33.501). If NFc is registered, the same procedure can be applied to NFc-NRF segment, and OCSP stapling could be part of the NFc profile. Nevertheless, for any SBA communication from an NFc to NRF, if done via TLS, the certificate validation of both peers is implicit, hence NFc does not need to store stapling in its profile with NRF.

- NFp could fetch the OCSP stapling of all certificates in the EE certificate chain and update the same in NF profile with NRF.

- the solution introduces additional signalling between the OCSP responder and the NFp corresponding to the updates of OCSP stapling information.

## 6.12 Solution #12: Automated Certificate Management for Network Slices

### 6.12.1 Introduction

The solution addresses key issue #9. The solution presents a proposal to enable the automated certificate management for network slices, taking into consideration that certificates might belong to different domains, e.g., in deployments where different 3rd party slices may co-exist and interoperate.

Different domains may require different configurations with respect to certificate management, moreover when those domains belong to 3rd parties. To allow for 3rd party slice tenants / slice service consumers (e.g., verticals) to configure the usage of their own CA for the network slices they own, interfaces need to be provided in order to manage the required configurations.

This solution proposes a new function referred to as Network Slice Certificate Orchestration Function (NSCOF) for providing those interfaces between different domains, including authorized 3rd parties, who can own one or more network slices. NSCOF function may enable automated certificate management procedures by orchestrating the communication in the interfaces between the different CAs and sub-CAs of the referred slicing domains, as well as between network slice orchestrator and CAs, in the following scenarios (among others):

- Slice service consumer specific root CA for all network slices owned and administrated by that slice service consumer. This specific root CA will be used in the certificate management procedures for all network functions of all network slices owned by the slice service consumer. Interactions with operator 5G Core shared functions may require cross certification schemas between operator CA and slice service consumer CA, or alternatively an initial (manual) out-of-band exchange of public root CA certificates.

- Network slice specific root CA, used by all network functions for that specific network slice, owned and administrated by the slice service consumer. The slice service consumer may have other network slices using the operator CA.

- Slice service consumer specific sub-CA, signed by the operator root CA (or intermediate CA), used for all network slices owned by that slice service consumer. The administration of the slice service consumer specific sub-CA can be done by the operator, the slice service consumer (3rd party) or shared among both entities.

- Network slice specific sub-CA, signed by the operator root CA, used for all network functions of that particular slice. The administration of the slice service consumer specific sub-CA can be done by the operator, the slice service consumer (3rd party) or shared among both entities.

- Network Functions (e.g., AMF) can be shared from the operator host network to serve multiple slices, which can be managed by 3rd party CAs owned by the slice service consumers. Thus, trust needs to be pre-established between operator CA and eventually involved 3rd party CAs.

### 6.12.2 Solution details

The figure 6.12.2-1 illustrates an example of orchestration tasks provided by the NSCOF function to enable automated certificate management for Slices, when 3rd parties (administrators and CAs) are involved.

The pre-requisites for this solution proposal are:

- Secure mutual TLS connection is established between the 3rd party certificate administrator and NSCOF function.

- NSCOF has a pre-established trust relationship with Operator's RA/CA

- Operator's RA/CA has a pre-established trust relationship with 3rd Party CA

NOTE 1: How the NSCOF has built a trust relationship with Operator's RA/CA, and how the operator's RA/CA has built a trust relationship with 3rd Party CA, are aspects left to implementation (e.g., cross certification, exchanging of public root CA certs as trust anchors, etc.). The latter assumption enables the certificates of NFs to be used in both environments, host operator network and slice service consumer network, since the trust has been pre-established.



Figure 6.12.2-1: Example of certificate management procedure orchestrated by NSCOF

1) 3rd Party Certificate Admin provides slice-specific root-CA OR sub-CA configurations to NSCOF.

For each NF allocated to applicable slice:

2a) (Optional) In some implementations, after having verified a successful deployment of NFs associated with specific NSSAIs, the Network Slice Orchestrator may request NSCOF for certificates for every of those NFs belonging to specific slices.

2b) (Optional) In some implementations, if NSCOF can identify the NFs associated with the NSSAIs from the information provided by 3rd party certificate administrator, NSCOF may send the Certificate Signing Request to Operator's CA on behalf of the NFs.

3) NSCOF provides the operator RA/CA with the information related to the (sub-) CA, and if applicable 3rd party CA, configurations according to the NSSAI to which each NF is associated.

4) Operator's RA/CA executes the certificate signing procedures with the corresponding (sub-) CAs (in the diagram a 3rd party CA is represented as example) as per received configurations.

5) Operator's RA/CA provides the signed NF certificate to NSCOF

6a) (Optional) In implementations where Step 2a) is used as trigger for NF certificate signing, a response is sent to Network Slice Orchestrator, which takes care of provisioning the signed certificate to the respective NF.

6b) (Optional) In some implementations, NSCOF may provision the signed certificate to the respective NFs.

NOTE 2: In some implementations, NSCOF can be an integral part of Network Slice Orchestrator.

### 6.12.3 Evaluation

The solution introduces a new logical function referred to as Network Slice Certificate Orchestration Function (NSCOF) to enable automated certificate management for Slices, especially when 3rd parties (administrators and CAs) are involved.

The solution addresses the requirement for the automated certificate management framework to manage certificates belonging to different domains (including authorized 3rd parties) by orchestrating the communication in the interfaces between the different entities (e.g., Management functions, operator RA/CA, slice service consumer CA) involved in Network Slicing certificate management.

When a network slice is created, the slice owner (operator or 3rd party), based on the specific slice security requirements, decides whether the slice requires a specific CA (root or sub-CA), and if so, proceeds to provision the information of that CA in the NSCOF. The NSCOF sends that information to the operator RA, which at the reception of the CSR for the NF, redirects the request to the corresponding CA or sub-CA allocated to the slice of which the NF takes part.

The impact of the solution is:

- The introduction of a new functionality part of the Slicing orchestration framework named as Network Slice Certificate Orchestration Function (NSCOF)

Observations:

- If step 2) (Optional) is performed, the generation of the CSR in NSCOF on behalf of the NF may represent a security risk, as the key pair (private/public) is generated in the NSCOF.

NOTE 1: In general, the solution assumes that NSCOF is trusted by the slice owner. If the NSCOF was not fully trusted by the slice owner, the key pair would be generated in the NF and only the public key would be sent to NSCOF for the certificate generation in the corresponding CA.

- When the administration of the sub-CA and/or root CAs need to be shared, security aspects related to multi-tenancy need to be considered.

- In network slices specific sub-CAs share a common root CA, there is a potential security issue of "over trust", since any certificate issued by those sub-CAs can chain back to the root CA and pass the authentication.

NOTE 2: Specific security requirements on network slices may require to configure a dedicated root CA per slice, thus avoiding a potential security issue of 'over trust'.

## 6.13 Solution #13: Build initial trust for NF certificate enrolment

### 6.13.1 Introduction

This solution addresses Key Issue 2: Security protection of NF certificate enrolment.

As stated in the key issue details, before issuing a certificate, operator CA/RA needs to establish an initial trust with the requestor NF instance, ensuring that the requestor NF instance is the correct one and is entitled to request a certificate. This solution introduces certificate management (CM) proxy functionality to verify the NF identities, and facilitates the initial trust establishment between NF and CA/RA. Considering that the new functionality also acts as a bridge between CA domain and SBA domain, it can be implemented in the same entity called as Certificate Management Network Entity (CMNE) that is introduced in the Solution #7: A solution addressing the relation between certificate lifecycle management and NF lifecycle management.

To enhance the trustworthiness of the virtualized 3GPP NF, it is proposed to have optional procedures where CM proxy acting as Relying Party can verify VNF based on attestation result when attestation is in use. The details of attestation solution and procedure is further investigated in the FS\_SIV study [17] and out of scope of this solution.

It is also assumed that the CM proxy trusts the OAM and CA/RA, and there are many ways to establish the trust between them (for example SSH or TLS), which is out of scope of this solution.

### 6.13.2 Solution Details

The following description provides a high-level overview about a possible solution by introducing the certificate management (CM) proxy as a bridge and facilitate the initial trust establishment between NF and CA/RA without having impact on CA/RA. The description shows the steps by which an entity in the NF receives an end-entity certificate. The individual steps are only indicative.

NOTE 0: How to perform and use attestation and as well as trusted execution is out of scope of this solution.



Figure 6.13.2-1: High-level procedure to build initial trust for NF certificate enrolment

1. NF has been successfully instantiated (with day-0 configuration).

The day-0 configuration can include the initial credential and trust anchors (e.g., root certificate) to be used by NF to establish a secure communication channel initiated from CM proxy.

For example, if TLS is used as a secure communication channel between NF and CM proxy, the NF can be pre-provisioned with a TLS server certificate which is signed by a root certificate that is stored in the CM proxy.

The initial credential, such as one time secret can be pre-provisioned for authentication between CM Proxy and NF through day-0 configuration of NF and CM Proxy.

The initial credential, such as one time secret can be pre-provisioned for authentication between CA/RA and NF through day-0 configuration of CM Proxy or CA/RA. In this solution, it is used by CA/RA to authenticate the NF.

2. (Optional when attestation is in use) To enhance the trustworthiness of the virtualized 3GPP NF, the virtualised NF instance is attested. It is assumed that the attestation results are maintained by the Attestation Verifier for subsequent access [17].

3. CM proxy is provisioned through OAM procedure with necessary information.

The necessary information includes initial credential to be used by CM proxy to setup secure communication channel with NF. For example, if TLS is used as a secure communication channel between NF and CM proxy, the CM proxy can verify the TLS server certificate of the NF using a preconfigured root certificate in the CM proxy.

The necessary information also includes NF identities (e.g., FQDNs to be presented in the certificate).

4. (Optional when attestation is in use) CM proxy acting as Relying Party can verify VNF based on attestation result and decide whether the NF is eligible for certification or not.

5. CM proxy registers NF end-entity to CA/RA.

The identities of NF end-entity (got from previous steps) are registered to CA/RA.

6. CA/RA provides authentication credentials to the CM proxy.

Depends on the agreement with the CA/RA, for example an initial authentication key (IAK) is agreed to be used in the enrolment protocol to get a certificate for the NF end-entity, the CA/RA sends IAK as the authentication credentials to the CM proxy.

NOTE: The Initial Authentication Key (IAK) is described in the RFC 4210 without details. As an example, theauthentication credentials can be a one-time secret used by CA to authenticate the received certificate signing request (CSR) associated with the registered NF identity in step 5.

7. CM proxy provides the NF about enrolment information and authentication materials.

The enrolment information includes enrolment protocol, CA/RA details and registered NF identities in step 5.

The authentication materials sending from CM proxy need be protected. For example, if TLS is used as a transport layer protection between NF and CM proxy.

8. NF generates key pair and prepares the CSR (Certificate Signing Request) message.

9. NF sends the certificate enrolment request to the CA/RA. Authentication credential received in step 7 is used to authenticate the origin of CSR from the end entity to the CA/RA.

The NF can authenticate the CA/RA based on out-of-band means. For example, CA/RA's root certificate is pre-configured as trust anchor in the NF, or it is installed during step 7.

10. CA/RA returns the issued certificate to the NF.

CA/RA validates the certificate enrolment request based on local policies using the identities received in step 5.

### 6.13.3 Evaluation

This solution introduces a new certificate management (CM) proxy functionality which acts as a bridge between SBA domain and PKI domain, and facilitates the initial trust establishment between NF and CA/RA without having impact on CA/RA.

The NF end-entity identities (e.g., FQDNs to be presented in the certificate) are registered by CM Proxy to CA/RA without having impact on CA/RA. The CA/RA can validate the certificate enrolment request based on local policies and registered identities.

The presence of CM Proxy provides a possibility to integrate with an attestation solution if needed, i.e., CM Proxy acts as Relying Party role and verifies VNF based on attestation result when attestation is in use. The details of attestation solution and procedure is further investigated in the FS\_SIV study [17] and out of scope of this solution.

The solution does not cover the initial trust for the CM Proxy.

The solution assumes the NF is pre-provisioned with TLS server certificate and one time secret (e.g., Initial Authentication Key). The CM Proxy authenticates the NF using NF's TLS server certificate, and NF authenticates CM Proxy using one time secret.

It is up to implementation policy to determine the (re) usage and type of Initial Authentication Key (s).

## 6.14 Solution #14: Ensuring the management of bulk certificate updates

### 6.14.1 Introduction

The solution addresses the security threat of KI#3 related to the potential partial or complete disruption of the automated certificate management framework due to a simultaneous update / renewal of a vast number of certificates.

The following scenarios are examples where bulk certificate updates may be required:

- Operator or an automation function determines a need to update many certificates due to a compromised algorithm, or compromised key, or revoked certificate.

- Many simultaneous alarms indicating the need to renew a huge number of certificates that are about to expire.

- CA may announce revocation of some CA certificates. If some of the root certificates, being used to sign several certificates for various NFs, are revoked, this action can lead to simultaneous updates of certificates for many network functions.

- Certificate Revocation List (CRL) may be updated with new certificate revocations, which can affect a large number of NFs.

In order to cater to various possible triggers of bulk certificate updates, the solution proposes a new network management functionality named in this solution as Certificate Update Orchestrator (CUO). Such a functionality can be implemented as part of the MANagement and Orchestration (MANO).

### 6.14.2 Solution details

CUO performs the following actions in order to mitigate the risks of automated certificate management leading to service un-availability.

- Monitoring of certificate expiry related alarms reported by network management systems

- Monitors CA announcements for certificate revocations

- CUO may subscribe to CA announcement notifications

- Monitors CRL/OCSP data stores for certificate revocations

- CUO may subscribe to notifications from applications that monitor changes / updates in CRL/OCSP data stores

- Accept certificate update triggers from the operator or an automation related function.

To ensure the proper management of the certificate updates for a large number of NFs, CUO may perform the following actions:

- Stagger the certificate updates in time such that only a small amount of certificate updates is ongoing simultaneously, while ensuring the updates are done within the stipulated time, especially for those that are close to expiry.

- Prioritize the certificate updates for those certificates having lesser time remaining for expiry.

### 6.14.3 Evaluation

This solution has no impacts on NFs, CAs or on any existing signalling procedures. The CUO described in this solution can be implemented independently as part of operator's management and orchestration framework.

## 6.15 Solution #15: Policy based certificate update/renewal

### 6.15.1 Introduction

This contribution addresses this key issue #3, and in particular the risk that may occur during the simultaneous update/renewal of a vast number of certificates.

### 6.15.2 Solution details

Normally, certificate update for CA/ PKI subscribers can be initiated in advance (e.g., one/two months) before the certificate expires due to the policy of the CA or the PKI subscribers, so that the new certificate can be tested while the current certificate is still available. Therefore, the CA has an enough period of time to process the simultaneous certificate update before the expiration date. The detailed description is as follows:

1. The time for updating the certificate before the certificate expires can be preconfigured in the NF and monitored by the CA.

2. When the NF discovers that the certificate is about to expire according to the preconfigured update time, it will trigger the certificate update process.

3. Even if the NF does not trigger the certificate update process, the CA can also monitor that the certificate for NF is about to expire, and trigger the certificate update for NF.

4. Besides, the CA does not have to update the certificates with the same expiration date at the same time. The certificates can be divided into different groups and been updated separately due to the policy of the CA. The CA can even set different update times for NFs with the same expiration time. This can also address the scenario of CA's certification update and revocation, which results in the simultaneous certificate update for CA and the involved entity certificates.

The compromise of a crypto algorithm in use is a corner case, and can also be addressed by the CA policy as described in step 4.

All the aspects above depend on CA/ PKI subscribers' policies and NF/CA internal implementations. So, how to deal with the simultaneous update/renewal of a vast number of certificates could be left to implementation based on the policy of CA controlled by the operator. If needed some guidance can be added in the normative phase to clarify this.

### 6.15.3 Evaluation

This solution specifically addresses the risk of service outage during simultaneous update/renewal of vast number of certificates. This is a threat identified in Key Issue #3.

The solution depends on the preconfigured policy and internal implementation of the NF/CA, and does not have standards impact.

## 6.16 Solution #16: Using ACME protocol for certificate enrolment and renewal

### 6.16.1 Introduction

This solution addresses Key Issue 1: Single certificate management protocol and procedures.

As stated in Key Issue 1, considering virtualization in 5G SBA, it is impractical to manage certificates manually. If there is no standardized use of an automated certificate management protocol, the certificate management needs to be done manually which may lead to missing refreshment of certificates and usage of expired certificates.

The solution proposes to use the ACME protocol to solve for the requirements in Key Issue 1.

It is beneficial to have standardised certificate management protocols and procedures for certificate enrolment and renewal to ensure that trusted and valid certificates are in use at all times.

The ACME protocol provides full certificate lifecycle support including enrolment, renewal and revocation. ACME is focused purely on the certificate lifecycle which provides simpler implementation and support. Machine to machine support is readily available with open-source client implementations in many languages.

ACME offers a solution to fully address the challenges of Key Issue 1 and provide the following benefits:

- Enables automatic acquisition and management of certificates

- Simplifies deployment of TLS across devices

- Cryptographic key material can be changed automatically, replacement keys can be rolled out automatically

- Reduces chance of global outages

- It reduces the chance of the environment becoming calcified on a single certificate on accident because they change regularly.

- It makes monitoring certificate lifecycles easier because changes happen on a predictable basis, which enables monitoring and proactive issue resolution.

- Enables quicker responses to global outages when they happen

- Reduces the chance that a vendor will divest itself the obligation for the CNF's implementation's requirement to manage its own certificates in favour of an "optional" certificate life cycle management operational support system.

- Reduces the need for third party vendor 'plugins' to actively manage the configuration files on a running CNF.

- Reduces the chance that third party management of certificates violates a containers' immutability property, which in an increasingly cloud native and containerized environment is a pillar of integrity.

- Removes vendor lock in on certificate issuance enabling migrating from one solution/vendor without code changes.

- Using certificates uniformly across this ecosystem could help secure the network from tampering and other malicious acts.

- Can be used with public trust anchors or in a private PKI

### 6.16.2 Solution details

#### 6.16.2.1 Solution overview

ACME can be implemented in multiple ways depending on the trust model network participants wish to use and which aspects of the 5G infrastructure will use ACME based certificates. IETF RFC 8555 [23] is extensible to many use cases, such as the TNAuthList profile [27].

ACME architectural elements, as depicted in Figure 6.16.2.1-1, include an ACME client (Client) and an ACME server (Server). These map directly to the CEMAF reference point architecture illustrated in Figure 6.1.2.2-1. The ACME client maps to the NF, and the ACME server maps to the CeEF and to the CeMF. The same ACME server can be used for both the CeEF and CeMF, or different ACME servers could be used.

Client

Server

[Order]

Signature

Required Authorizations

[Responses]

Signature

Validation

[CSR]

Signature

Acknowledgement

Await issuance

[POST-as-GET Request]

Signature

Certificate

Figure 6.16.2.1-1 Information covered by request signatures Certificate Issuance

#### 6.16.2.2 ACME Profiling for SBA

##### 6.16.2.2.0 General

The following ACME procedures are in the scope of certificate management for SBA:

- Certificate Enrolment: Register an ACME account using an ACME client, request a certificate and solve the validation challenge to confirm control of the target(s) and the certificates will be issued. Robust solutions would include automated challenge solving.

- Certificate Renewal: At 2/3rds of the certificate lifetime, the certificate will be renewed. If automation is used, no manual work is required. Where appropriate, support for RFC 8739 [28] - Short-Term, Automatically Renewed (STAR) Certificates is desirable.

- Certificate Revocation: Self-service revocation is possible using the registered client. Manual revocation by the CA operator is also possible in cases where self-service is not viable or desirable.

NOTE: The support of SBA certificate profile as specified in TS 33.310 [3] by ACME has not been addressed in the present document.

##### 6.16.2.2.1 General Requirements

The following requirements apply to ACME usage in Service Based Architecture:

- ACME provides full certificate lifecycle functionality, but it needs established trust anchors and appropriate validation challenge solving architecture.

- The usage of the senderNonce and the recipNonce fields is mandatory. The length of the fields as recommended in [23] is used. The recipNonce in the very first message in the transaction is set to 0 by the sender and is disregarded by the recipient of the message.

##### 6.16.2.2.2 Profile for PKI Fields

6.16.2.2.2.1 General

The NF Instance certificate enrolment supports the following ACME 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 [23] apply.

6.16.2.2.2.2 Account Initialization and Response

The normal ACME flow for ACME account setup below would be adapted to streamline contact information exchange because participants will already be known within the ecosystem. TOS acceptance will be dropped, but otherwise remain a standard ACME flow.

Client

Server

[Contact Information]

[ToS Agreement]

[Additional Data

Signature]

Account URL

Account Object

Figure 6.16.2.2.2.2-1:Account Initiation and Response

6.16.2.2.2.3 Certificate Validation

RFC 8555 [23] section 8 covers the 3 TLS validation methods (DNS, HTTP, TLS-ALPN) in detail. Additional validation methods using reliable RAN and SBA information. While DNS or HTTP challenges are the most common way in ACME to check the validity of a signing request, the request can also be validated independently of any DNS infrastructure through other methods (e.g., external account bindings).

External account binding is an alternative method of validating a signing request in 5G SBA CNF that does not depend on any DNS infrastructure. It involves linking the request to an existing validated account at the certificate authority (CA) by providing the account key and a digital signature of the signing request to the CA. This method requires the requesting entity to have a previously validated account at the CA, and the security of the validation process depends heavily on the security of the account key and the digital signature.

While external account binding can provide an alternative to DNS or HTTP challenges for validating signing requests in 5G SBA CNF, it is crucial to maintain the security and integrity of the process to prevent unauthorized certificate issuance. This involves ensuring the account key is kept secure and not shared, and the digital signature is created using a secure algorithm and trusted implementation.

When DNS is used as a challenge mechanism to validate the domain ownership by a client in 5G SBA CNF, there are several security threats that could compromise the integrity of the validation process. These threats include:

1. DNS Spoofing: An attacker may attempt to impersonate the DNS server and provide fake DNS responses to the ACME client, leading to a successful domain validation. This can be mitigated by using DNSSEC (DNS Security Extensions) to ensure the authenticity of DNS responses.

2. DNS Cache Poisoning: An attacker may attempt to poison the DNS cache of the ACME client with incorrect information, leading to a successful domain validation. This can be mitigated by implementing DNS cache poisoning prevention mechanisms such as Response Rate Limiting (RRL) and DNS Cookies.

3. Man-in-the-Middle (MitM) Attacks: An attacker may intercept the communication between the ACME client and the DNS server, modify the DNS responses, and provide fake domain validation results to the ACME client. This can be mitigated by using secure communication protocols such as HTTPS/TLS to encrypt the communication and prevent interception.

4. DNS Server Compromise: A DNS server may be compromised by an attacker, leading to the issuance of fake DNS responses to the ACME client and successful domain validation. This can be mitigated by ensuring that the DNS server is properly secured, regularly updated, and audited for vulnerabilities.

To mitigate these threats and ensure the protection of DNS when used as a challenge mechanism to validate the domain ownership by a client in 5G SBA CNF, the following security measures should be implemented: DNSSEC, RRL or DNS Cookies, HTTPS/TLS, proper security and regular updates of DNS server.

6.16.2.2.2.4 Key Update Request and Key Update Response

RFC 8555 section 7.3.5 covers key updates in detail and is appropriate within the 3gpp ecosystem.

6.16.2.2.2.5 Certificate acquisition and renewal

RFC 8555 section 7.4 covers certificate acquisition. Renewals are simply another acquisition request. Typically, renewals happen at 2/3rds the lifetime of the certificates. Where appropriate, support for RFC 8739 [28] can be advantageous to support short lived certificates.

NOTE: Life spans for certificates are not defined by ACME and while typical use is short-lived, the life span of the certificates would be up to implementation.

#### 6.16.2.3 ACME Transport

Transport of ACME messages between end entities (network elements) and RA/CA is done over HTTPS as specified in IETF RFC 2818 using JSON Web Signature RFC 7515 [4] for additional protections. Transport between CA elements is up to the CA operator, but should use a secure channel.

NOTE: Further details on the ACME profiling will be addressed during normative work.

### 6.16.3 Evaluation

This solution addresses Key Issue #1: Single certificate management protocol and procedures.

NOTE: ACME has not been profiled for use cases of 5G SBA architecture. Details of initial trust framework for ACME, ACME signalling handshake message content for 5G SBA use cases, and ACME architecture for request/response for all five certificate types used in 5G SBA have not been addressed in the present document.

It is beneficial to have an automated certificate management protocol and procedures to avoid missing refreshment of certificates and use of expired certificates. It is also important that the protocol and procedures be well established standards as the environments in which they are to be used are multi-vendor and may cross multiple administrative domains. The ACME protocol [23] is a good candidate to support automatic certificate enrolment and renewal procedures. ACME also provides facilities for other certificate management functions, such as certificate revocation.

ACME is focused purely on the certificate lifecycle, which makes it lightweight and easy to support. It allows a client to request certificate management actions using a set of JavaScript Object Notation (JSON) messages [24] carried over HTTPS [25]. As such, it aligns well with the Certificate Enrolment and MAnagement Framework (CEMAF) outlined in the present document. Certificate Enrolment using ACME resembles the certificate issuance process of a traditional Certificate Authority (CA) in which a client creates an account, requests a certificate, and proves control of the identifier(s) in that certificate in order for the CA to issue the requested certificate. CeEF and CeMF map to ACME servers. NF entities map to ACME clients.

5G SBA in general, and more specifically the increase in modularity of NFs, has resulted in multi-vendor environments becoming more prevalent. It is now common for NFs to come from different vendors, and for the cloud native environment in which they run to come from yet another vendor, and for all of these to be independent of the CA that is authoritative for the certificates that are used to secure their communications. A key benefit of ACME over prior art is its automated validation of authority to represent an identifier. ACME uses an extensible challenge/response framework for identifier validation. Although the original focus of ACME was validating domain names for issuing certificates for Web PKI, ACME supports extensions for other identifiers in other PKI contexts, including certificates attesting to IP addresses [26]. 3GPP specific identifier validation challenges can be defined if necessary.

## 6.17 Solution #17: Assurance of unique NF identifiers in certificates

### 6.17.1 Introduction

This solution addresses the security threat exposed in key issue #8 related to the misuse of NF instance identities to fetch a valid operator certificate.

The solution proposes a procedure that allows the operator CA/RA to verify that the CSR message comes from a genuine NF instance. The procedure, performed by the operator CA/RA, consists of validating the NF Instance Id in the CSR (included in Subject Alt Name (SAN) field as per certificate profile in 6.3.1c of TS 33.310 [3]) with the NF Instance Id pre-provisioned in NF (i.e., initial credentials, e.g., initial certificate) during the building of initial trust between NF and operator CA/RA (please refer to solutions addressing KI#2 in the present document).

### 6.17.2 Solution details

The following diagram represents the security procedure to ensure that the CSR message comes from a genuine NF instance and NF Instance Id has not been misused.



Figure 6.17.2-1: Assurance of unique NF identifiers in certificates

1. During the process of building initial trust between NF and Operator CA/RA the NF Instance Id and NF credentials get known by Operator CA/RA.

NOTE: The selected mechanism to establish the initial trust between NF and Operator CA/RA, e.g., PSK/Refnum, initial certificate, etc., requires conveying the NF Instance Id of the NF along with the credentials of the NF.

2. NF creates a Certificate Signing Request (CSR) including the NF Instance Id in SAN field.

3. NF sends the CSR to Operator CA/RA

4. The operator CA/RA verifies the message protection according to the selected initial trust security mechanism (e.g., pre-shared key, certificate, etc.).

5. The operator CA/RA verifies that the NF Instance Id in the SAN field of the CSR corresponds to the NF Instance Id conveyed during the initial trust building procedure.

6. NF fetches the certificate from Operator CA/RA

### 6.17.2 Evaluation

The solution addresses the security threats and potential security requirements of KI#8 by proposing a procedure which allows the operator CA/RA to verify that the NF identifier (NF Instance Id) has not been misused to fetch a valid certificate. Thus, a rogue NF won't be able to fetch an operator certificate by only knowing the NF Instance Id.

The solution binds the NF identifier (NF Instance Id) provided during the initial trust procedure with operator RA/CA, with the NF identifier provided in the SAN field of the certificate request to fetch the operator certificate from the RA/CA.

The specific implementation of the solution depends on the selected mechanism to build initial trust between NF and operator CA/RA. The mechanisms to build initial trust between NF and operator CA/RA are not part of this solution.

## 6.18 Solution #18: Slice specific initial enrolment procedure

### 6.18.1 Introduction

This contribution proposes a solution for key issue #9. In particular, the solution is based on solution #3 which provides initial trust between NF and operator CA. For the scenario of the automated certificate management for network slices where different 3rd party slices may co-exist and interoperate, the initial trust between NF and the 3rd party CA can be established using the mechanism in solution #3, where the initial certificate is issued by the operator CA and the entity certificate can be issued by the 3rd party CA. During the process, the certificate management NF can take the role of interacting with the 3rd party CA.

The solution concept is represented in the figure 6.18.1-1.

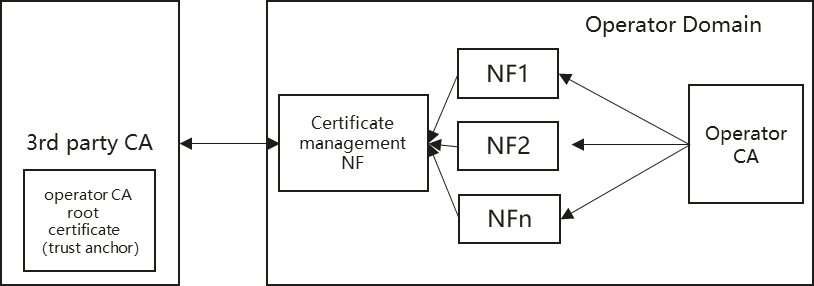


Figure 6.18.1-1: Secure initial enrolment through Operator CA and Certificate Management NF

### 6.18.2 Solution details

For NFs in 5GC SBA to fetch end entity X.509 certificates signed by a 3rd party CA, the NFs are expected to have an identity that is trusted and accepted by the operator CA and can obtain a certificate from the operator CA. This certificate issued by the operator CA can be used to protect the process of requesting the certificate signed by the 3rd party CA. The solution details are similar with the process of certificate enrolment in solution #3 with the following differences:

- The private CA is replaced with the operator CA.

- The operator CA is replaced with the 3rd party CA.

### 6.18.3 Evaluation

The solution addresses the security requirement of KI#9 related to the scenario of the automated certificate management for network slices by proposing a procedure for the NF to fetch a certificate from a 3rd party CA, owned/managed by the slicing customer. The procedure proposes to use an initial certificate for authentication to the 3rd party CA, signed by an operator CA. The normal certificate management like certificate update, revocation can follow the normal process addressed by KI #3 and KI#5. Other aspects like the alignment between NF lifecycle and certificate lifecycle in the certificate management for network slicing are not covered.

The prerequisite of this solution is that the NFs have obtained certificates issued by the operator CA using mechanisms addressing KI#2.

The solution requires the implementation of an operator CA, the root certificate of that operator CA is pre-configured as trust anchor in the 3rd party CA to enable the authentication of the NF during the initial certificate enrolment in 3rd party CA.

# 7 Conclusions

## 7.1 KI#1: Single certificate management protocol and procedures

### 7.1.1 Analysis

The key issue addresses the need to use an automated certificate management protocol and procedures in 5G SBA with capabilities (e.g., enrolment, renewal) to manage the lifecycle of the certificates. It is also desirable to have one single solution for the entire lifecycle of the certificates to facilitate interoperability and reduce the implementation complexity.

Two solutions are presented to cover this key issue.

- Solution #1 introduces an overall framework named as CEMAF (Certificate Enrolment and MAnagement Framework). CEMAF proposes to group the certificate management procedures in three blocks, corresponding to the initial trust establishment, the enrolment of the certificate, and the management procedures during the lifecycle of the certificate (updates, revocation, status notification, etc.).

- Solution #2 proposes CMP as a protocol for certificate enrolment and renewal procedures, and a CMPv2 profiling for SBA has been provided accordingly.

CMP complies with the requirements to be a single certificate management protocol in 5G SBA for the procedures of enrolment and renewal.

The certificate management framework requires to be completed with the procedures related to initial trust establishment, and management procedures not covered in the CMP profiling for 5G SBA (e.g., revocation).

### 7.1.1 Conclusion

It is proposed to pursue CMP protocol in normative specification for the procedures of certificate enrolment and certificate renewal in 5G SBA.

## 7.2 KI#2: Security protection of NF certificate enrolment

### 7.2.1 Analysis

The protection of the NF certificate enrolment procedure requires to build initial trust with the CA/RA to fetch the operator certificate, as well as security mechanisms during the whole procedure that includes integrity protection, anti-replay protection and mutual authentication.

The conclusion for KI#1 proposes to pursue CMP as selected protocol for the enrolment procedure. In addition to the intrinsic security features of CMP, the following solutions have addressed the following security aspects:

- Solution #3 proposes a procedure to secure the initial enrolment of the NF certificates, by the introduction of a local CA used for NFs within the same security domain (e.g., part of the same cloud infrastructure), which delivers a first initial certificate.

- Solution #8 proposes a procedure to enhance the protection of the certificate enrolment by providing a pre-configured signature of the NF profile in the certificate request, that can be verified in the operator CA.

- Solution #13 proposes a procedure to build the initial trust for NF certificate enrolment by the introduction of a new functionality that acts as a proxy between the NF and the operator CA/RA.

The common ground for all solutions is the involvement of the OAM system, which instantiates the NF and provides the initial trust (e.g., signature, certificate, credentials, etc.), which can be verified by the operator CA/RA. The OAM system is trusted for the operator CA/RA.

### 7.2.2 Conclusion

It is proposed to pursue an approach where the OAM system of the NF provides the initial trust to be used during NF operator certificate enrolment procedure. The initial trust can be implemented by an initial (OAM) certificate (although other implementation options are also valid, e.g., signature of certain NF parameters), which can be verified by the operator CA/RA, since the trust between the OAM system and the operator CA/RA has been pre-established.

It is agreed to propose the Solution #3 as the basis for the normative work.

## 7.3 KI#3: NF Certificate Update

### 7.3.1 Analysis

The key issue addresses the need to support a certificate update procedure for NFs for example due to expiry or change in the validity status as well as scenarios where such an update under certain circumstances is required for a vast number of NFs.

Now since it is agreed to pursue CMPv2 protocol in the normative phase, updates or renewal of certificates could as well be handled by the same protocol without the need to support any new procedure.

Two solutions have been proposed to cover a possible service outage issue when automated certificate management may lead to simultaneous updates of certificates for several, even multiple NFs.

Solution #14 proposes a new network management functionality named Certificate Update Orchestrator (CUO) which can be implemented as part of the management and orchestration to address the issue. This can be implemented without any impacts to NFs, CAs, or on any existing signalling procedures.

Solution #15 proposes a policy-based solution which mainly depends on the CA/NF policies and internal implementations.

### 7.3.2 Conclusion

It is concluded that the update/renewal of certificates could be handled by the CMPv2 protocol as concluded in clause 7.1.2. The update/renewal trigger, for example due to expiry, change in validity "status" or other events such as the sudden disclosure of broken cryptographic primitives, could be based on internal configuration, operator policies, etc. Therefore, no normative work is needed, and this aspect of the overall framework could be left to implementation. Whether there is a need for informative guidance for the security threat related to simultaneous update / renewal of a vast number of certificates leading to partial or complete service disruption will be decided in the normative phase.

## 7.4 KI#4: Trust Chain of Certificate Authority Hierarchy

### 7.4.1 Analysis

This key issue addresses the establishment of trust chain of Certificate Authority Hierarchy, which ensures the legitimacy and credibility of the certificate authority. Based on the trust chain, each TLS entity in 5G SBA is able to obtain its certificates and verify the certificates of other TLS entities.

Two solutions have been proposed to establish the trust chain of Certificate Authority Hierarchy.

Solution #4 describes the cross-certification based trust chain in the SBA Architecture, which supports the intra-domain SBA connection and the inter-domain SBA connection. Cross-certification enables the users under each of the authorities to trust the other authority's certificates, which could benefit the certificate verification between SEPPs.

Solution #5 describes the interconnection CA based trust chain in the SBA Architecture, which supports the intra-domain SBA connection and the inter-domain SBA connection. The interconnection CA can be used to issue certificates to the SEG CAs, TLS client CA or TLS server CA of other domains, with which the operator's SEGs and TLS entities have interconnection.

### 7.4.2 Conclusion

The validation of the trust chain of CA hierarchy is required in the automated certificate management framework, and that the solutions presented in the study are implementation options.

Further details are to be discussed during normative phase.

## 7.5 KI#5: Certificates revocation procedures

### 7.5.1 Analysis

The KI#5 requires for 5G Core SBA a certificate revocation schema, part of the overall certificate lifecycle management framework, that should be scalable, fast due to the highly dynamic environment of the infrastructure, and resilient in case of outages. Certification Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) and OCSP stapling are listed as possible schemas, and even they have been profiled in TS 33.310 [3].

Two solutions have been presented in the study:

- Solution #6 proposes a OCSP based revocation procedure, with the option of using stapling for 'high load' server NFs to alleviate the burden of OCSP servers and reduce the signalling.

- Solution #11 proposes a OCSP stapling based revocation procedure.

OCSP and OCSP stapling are well-established standard protocols for certificate management. OCSP improves the latency and performance of the revocation related procedures by providing an online service, and OCSP stapling enhances it by caching the OCSP responses, thus ensuring the availability of the service as well in case of CA or OCSP responder outages.

A profile of OCSP and OCSP stapling can be found in clause 6.1b of TS 33.310 [3].

### 7.5.2 Conclusion

For certificate revocation, it is agreed to pursue CRL in the normative phase. CRL support for TLS is already specified in TS 33.310 (Table 6.1.3c.3-1: cRLDistributionPoint as mandatory extension).

OCSP [8] and OCSP stapling [15] and [16] are possible additional certificate revocation schemas for SBA. The support of those mechanisms will be decided during normative phase.

## 7.6 KI#6: Relation between certificate management lifecycle and NF management lifecycle

### 7.6.1 Analysis

The KI#6 requires to consider the NF lifecycle in the certificate lifecycle management for SBA, thus the solutions need to address the relations between both lifecycles.

Three solutions have been evaluated in the study:

- Solution #7 introduces a new network entity named as 'Certificate Management Network Entity' (CMNE), responsible for the synchronization between certificate related events and NR related events, by communicating with CA/RA, NRF and Virtualization Orchestration platforms.

- Solution #9 proposes that the NRF checks during the discovery procedure of the NFc the certificate validity of the NFp from the OCSP/CRL server, so that the NF discovery service can only provide the response including a NFp with a valid certificate.

- Solution #11 proposes to register and update the NF profile in NRF with OCSP stapling information, so that the status of the certificate of the NFp will be verified by the NRF before responding the request of the NFc. Thus, the NRF will always respond with a NFp whose EE certificate is valid.

The common ground among solution #9 and solution #11 is that both solutions propose to use revocation information provided by OCSP service to coordinate the relation among the NF lifecycle and the certificate lifecycle. In general, OCSP stapling offers better efficiency and reliability than OCSP when providing revocation services by reducing the required signalling and by ensuring the revocation service in case of eventual outage or non-reachability of OCSP server.

### 7.6.2 Conclusion

In relation to NF and certificate lifecycle management, it is agreed to further discuss and decide on the following option during the normative phase:

- During the NF discovery procedure, the NRF can perform certain checks in order to determine that the potential producers have valid certificates. Such checks can be based on locally stored information or by querying other network entities such as OCSP/CRL servers.

## 7.7 KI#7: Multiples certificates to be associated with a Network Function

### 7.7.1 Analysis

The NFs in SBA may need to support multiple operator certificates for different purposes (e.g., TLS authentication, JSON signing and encryption). The key issue addresses the need of certificate management framework in SBA to provide the means to manage the usage of the issued certificates.

The solution presented to cover this key issue is the following:

- Solution #10 introduces a procedure to indicate and validate the purpose of the X.509 certificates used in SBA by using the Extended Key Usage extension of the certificate as defined in IETF RFC 5280 [19] and IETF draft-ietf-lamps-nf-eku-00 [21].

### 7.7.2 Conclusion

It is proposed to pursue the proposed procedure in solution #10 to indicate and validate the purpose of the X.509 certificates in the normative specification as part of the desired certificate management framework in SBA.

The SBA certificate profile is to be expanded in the possible values for extendedKeyUsage to cover the usage of JSON signing and encryption.

The usage of the Extended Key Usage extension of the certificated in the solution has dependency on the final status of IETF draft-ietf-lamps-nf-eku-00 [21], which is work in progress in IETF at the time of writing.

## 7.8 KI#8: Trusted Network Function instances identifiers

### 7.8.1 Analysis

The KI#8 requires that the certificate management framework should be able to manage and track the NF instance identifiers per end entity, in order to avoid that a malicious of compromised NF instance could fetch a valid certificate using a compromised NF instance ID.

Two solutions have been evaluated in the study:

- Solution #8 introduces a procedure consisting in the pre-configuration of signature of certain parameter(s) such as NF instance ID or NF type in the NF profile, that can be verified in the operator CA as part of the certificate enrolment procedure. OAM system, as trusted entity for the operator CA and NF, can configure the signature intended to protect the integrity of the NF identifier.

- Solution #17 introduces a procedure that allows the operator CA to verify that NF identifier has not misused. It binds that identifier (NF Instance Id) provided during the initial trust procedure between NF and operator CA with the NF identifier provided in the SAN field of the certificate request to fetch the operator certificate from the operator CA.

The common ground of both solutions is that they require to build an initial trust between NF and operator CA to later on verify the NF identity at the certificate enrolment phase.

### 7.8.2 Conclusion

For the normative work, it is agreed to further discuss and decide on the following principle addressing KI#8:

- Operator RA/CA should be able to verify that the NF instance ID in the CSR belongs to the NF instance requesting the certificate.

## 7.9 KI#9: Automated Certificate Management for Network Slicing

### 7.9.1 Analysis

The automated certificate management framework in SBA may need to work with certificates that belong to different domains, such as customer 3rd party slices, with different requirements in terms for example of certificate lifecycles and CA(s) security policies, managed by multiple administrators (tenants).

Two solutions are presented to cover this key issue: solution #12 and solution #18.

The proposed solution #12 introduces a new functionality, that can be part of the slicing orchestration framework, intended to orchestrate the procedures/processes between the different entities involved in the Network Slicing certificate management, such as management functions, operator CA/RA and (sub-)CA for slice(s).

In general, the solution #12 assumes that NSCOF is trusted by the slice owner.

The administration of the sub-CAs and/or root CAs may need to be shared, so security aspects related to multi-tenancy need to be consider in those implementations.

Due to specific security requirements of the slice dedicated sub-CAs and/or root CAs may be needed. It is assumed that those CAs are created together with the slice, and the information is conveyed by the NSCOF to the corresponding operator RA, receptor of the CSRs from the NFs.

The proposed solution #18 relies on using an initial certificate for authentication to the 3rd party CA, signed by an operator CA. The root certificate of the operator CA is pre-configured as trust anchor in the 3rd party CA to enable the authentication of the NF during the initial certificate enrolment in 3rd party CA.

### 7.9.2 Conclusion

It is proposed that the automated certificate management framework supports management of certificates in Network Slicing. The details are left to normative phase.

Including the description of some relevant use cases/scenarios in Network Slicing as informative guidelines for deployments is to be decided during normative phase.

Annex A:   
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA3#106-e |  |  |  |  | TR Skeleton | 0.0.0 |
| 2022-02 | SA3#106e | S3-220504 |  |  |  | Adding Introduction and Scope sections | 0.1.0 |
| 2022-05 | SA3#107e | S3-221270 |  |  |  | Update of introduction and scope  Adding Key issues #1, #2, #3, #4, #5, #6, #7, #8, #9. | 0.2.0 |
| 2022-07 | SA3#107e AdHoc | S3-221619 |  |  |  | Update of Key issue #6  Adding Solutions #1, #2, #3, #4, #5, #6, #7 | 0.3.0 |
| 2022-10 | SA3#108e AdHoc | S3-223033 |  |  |  | Update of Key issue #3  Adding Solutions #8, #9, #10, #11, #12, #13 | 0.4.0 |
| 2022-11 | SA3#109 Toulouse | S3-224165 |  |  |  | Evaluations for Solutions #3, #8, #9, #11, #12  Update to solution #3  Adding Solutions #14, #15  Adding Security Assumptions in chapter 4  Preliminary conclusion for KI#1 | 0.5.0 |
| 2023-02 | SA3#110 Athens | S3-231499 |  |  |  | Evaluation for Solutions #1, #2, #3, #4, #5, #6, #8, #10, #12, #13, #14, #15,  Update to solution #10  Conclusion of Key Issues #2, #3, #5, #7, #9  New solutions #16, #17, #18 | 0.6.0 |
| 2023-04 | SA3#110Adhoc-e | S3-232225 |  |  |  | Updates of evaluations for solutions #3, #7, #18  Updates of conclusions of key issues #5, #9  New conclusions of key issues #4, #6, #8 | 0.7.0 |
| 2023-05 | SA3#111 Berlin | S3-233189 |  |  |  | Updates of solutions #7, #16  Updates of conclusion of key issue #6  Clean up and editorials | 0.8.0 |
| 2023-05 | SA#100 | SP-230572 |  |  |  | Presented for information and approval | 1.0.0 |
| 2023-06 |  |  |  |  |  | Upgrade to change control version | 18.0.0 |
| 2023-07 |  |  |  |  |  | EditHelp review | 18.0.1 |