|  |  |
| --- | --- |
| 3GPP TR 33.876 V0.3.0 (2022-07) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Automated Certificate Management in SBA;  (Release 18) | |
|  | |
| *5G-logo_175px* | 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.  © 2021, 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 4

Introduction 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Architectural and security assumptions 8

5 Key issues 8

5.1 Key Issue #1: Single certificate management protocol and procedures 8

5.1.1 Key issue details 8

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Security protection of NF certificate enrolment 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

5.3 Key Issue #3: NF Certificate Update 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key Issue #4: Trust Chain of Certificate Authority Hierarchy 10

5.4.1 Key issue details 10

5.4.2 Security threats 10

5.4.3 Potential security requirements 10

5.5 Key Issue #5: Certificates revocation procedures 11

5.5.1 Key issue details 11

5.5.2 Security threats 11

5.5.3 Potential security requirements 11

5.6 Key Issue #6: Relation between certificate management lifecycle and NF management lifecycle 11

5.6.1 Key issue details 11

5.6.2 Security threats 12

5.6.3 Potential security requirements 12

5.7 Key Issue #7: Multiples certificates to be associated with a Network Function 12

5.7.1 Key issue details 12

5.7.2 Security threats 12

5.7.3 Potential security requirements 12

5.8 Key Issue #8: Trusted Network Function instances identifiers 13

5.8.1 Key issue details 13

5.8.2 Security threats 13

5.8.3 Potential security requirements 13

5.9 Key Issue #9: Automated Certificate Management for Network Slicing 13

5.9.1 Key issue details 13

5.9.2 Security threats 14

5.9.3 Potential security requirements 14

6 Solutions 15

6.1 Solution #1: Certificate Enrolment and MAnagement Framework (CEMAF) 15

6.1.1 Introduction 15

6.1.2 Solution details 15

6.1.2.1 General 15

6.1.2.2 Architecture 15

6.1.2.3 Procedures 15

6.1.3 Evaluation 16

6.2 Solution #2: Using CMP protocol for certificate enrolment and renewal 16

6.2.1 Introduction 16

6.2.2 Solution details 17

6.2.3 Evaluation 17

6.3 Solution #3: Secure initial enrolment of NF certificates 17

6.3.1 Introduction 17

6.3.2 Solution details 18

6.3.3 Evaluation 20

6.4 Solution #4: Cross-Certification Based Trust Chain in the SBA Architecture 20

6.4.1 Introduction 20

6.4.2 Solution details 21

6.4.2.1 General architecture 21

6.4.2.2 Verify certificate in SBA architecture 22

6.4.3 Evaluation 23

6.5 Solution #5: Interconnection CA Based Trust Chain in the SBA Architecture 23

6.5.1 Introduction 23

6.5.2 Solution details 24

6.5.2.1 General architecture 24

6.5.2.2 Verify certificate in SBA architecture 25

6.5.3 Evaluation 26

6.6 Solution #6: OCSP based revocation procedure 26

6.6.1 Introduction 26

6.6.2 Solution details 26

6.6.2.1 General 26

6.6.2.2 Procedure 26

6.6.3 Evaluation 26

6.7 Solution #7: A solution addressing the relation between certificate lifecycle management and NF lifecycle management 27

6.7.1 Introduction 27

6.7.2 Solution details 27

6.7.3 Evaluation 28

7 Conclusions 28

Annex A (informative): Change history 29

# 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 TS 33.310.

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.

1. Lack of standardisation has resulted into number of bespoke methodologies and varying choices of certificate management protocols resulting into inconsistent model.
2. 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:

1. Principle to be reusable when 5G SBA is for NPN (standalone and PNI)
2. Principles standardised to be able to support NFs doing mutual TLS in Slicing
3. Principles standardised to support both intra and inter PLMN, in the latter referring to SEPP certificates in N32 interfaces and potential cross-certification considerations
4. Principles involving ‘Chain of Trust’ of Certificate Authorities hierarchies
5. 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] 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] RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"

[9] 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".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

# 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:

* The NF cannot communicate with each other.
* If certificate enrolment parameters are tampered, the CA issues an incorrect certificate.
* 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.

### 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:

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

### 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:

*3. Principles involving ‘Chain of Trust’ of Certificate Authorities.*

*4. 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 Rel-17 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:

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

* TLS client EE certificates (for NF consumers)
* TLS server EE certificates (for NF producers)

NOTE 1: Clause 6.1.3c of 3GPP TS 33.310 [3] profiles the TLS entity certificates to be used for 5GC SBA.

* Certificates for signing the access tokens for authorization (JSON Web Signature (JWS) as described in RFC 7515[4]) (for NRFs)
* Certificates for encrypting HTTP messages between SEPPs (clause 13.2.4.4 of TS 33.501 [2])
* 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 3GPP TS 23.501[5] clauses 6.2.6 and 6.3.1, and in 3GPP 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.).

3GPP TS 23.501 [5] defines an NF instance as an identifiable instance of the NF. CSRs must contain a trusted and unique identity of the NF instance requesting the certificate. 3GPP 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 must 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:

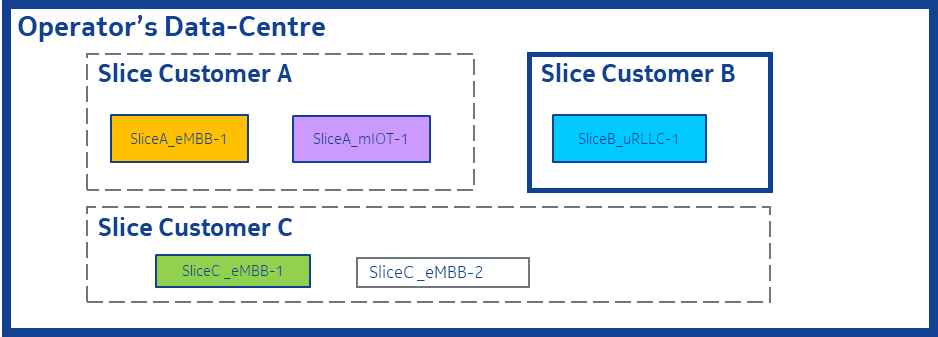


Figure 1 - Different slices logically isolated for different slice customers

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 peform 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

## 6.1 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

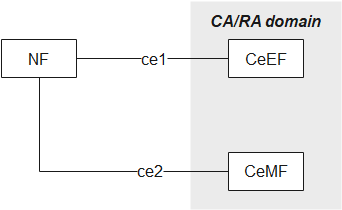
#### 6.1.2.1 General

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 doesn't preclude re-using such protocols.

#### 6.1.2.2 Architecture

Editor's Note: Terminology to be updated according to the following: CeEF 🡪 Enrolment, CeMF 🡪 Management

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.

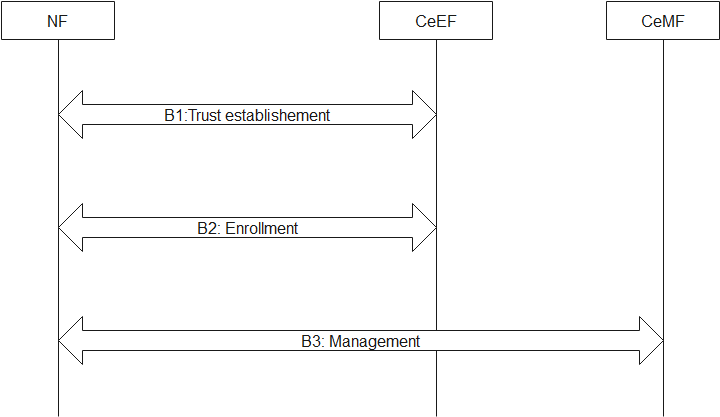


**Figure 6.1.2.2-1 CEMAF reference point architecture**

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 must 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 trsut 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

Editor's note: evaluation is ffs

## 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

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: 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.

Editor's note: CMP profiling for SBA is FFS.

Editor's note: Provision of certain parameters to the NF for CSR generation is FFS.

### 6.2.3 Evaluation

TBD

## 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 shall be 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 intial 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. 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 shall be installed in the operator CA as a trust anchor.

Editor’s note: Details on how the initial trust between NF and Private CA is established is ffs.

1. 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).
2. The private CA signs the public key and issue a certificate for the NF.
3. 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 shall be used by the NF as initial certificate for authentication to the operator CA.
4. The NF, or the Certificate Management NF on behalf of the NF, generates a new private-public key pair, if this is not preprovisioned, to obtain the operator signed end entity certificate on its own public key from RA/CA using for example CMPv2.
5. 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 shall include 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.
6. The NF, or the Certificate Management NF on behalf of the NF, sends the signed certificate enrolment request to the operator CA.
7. 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 proof of possession of the private key for the requested certificate.
8. 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.

### 6.3.3 Evaluation

TBD

## 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. In this solution, we focus on the certificate verification in terms of the chain of trust.

### 6.4.2 Solution details

#### 6.4.2.1 General architecture

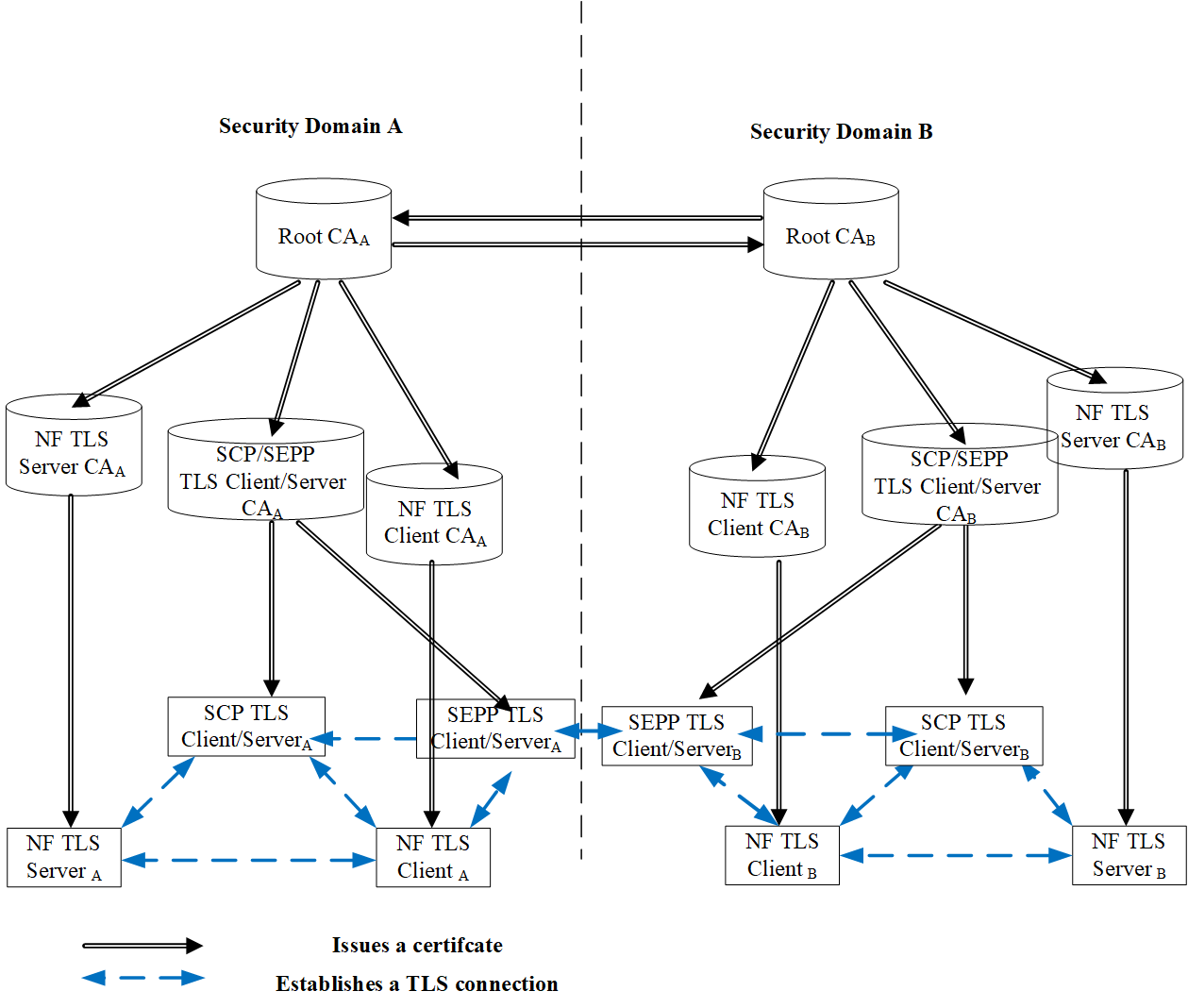


Figure 6.4.2.1-1: General Architecture

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: 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.

Editor's Note: How to manage the cross certification dynamically in SBA is FFS.

Editor’s Note: Whether one PKI domain (i.e., one Root CA) per security domain, or one PKI domain can be per other aspects for SBA certificates is FFS.

Editor’s Note: Whether using one PKI domain for both intra-PLMN and inter-PLMN SBA certificates is FFS.

#### 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

TBD

## 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. In this solution, we focus on the certificate verification in terms of the chain of trust.

### 6.5.2 Solution details

#### 6.5.2.1 General architecture

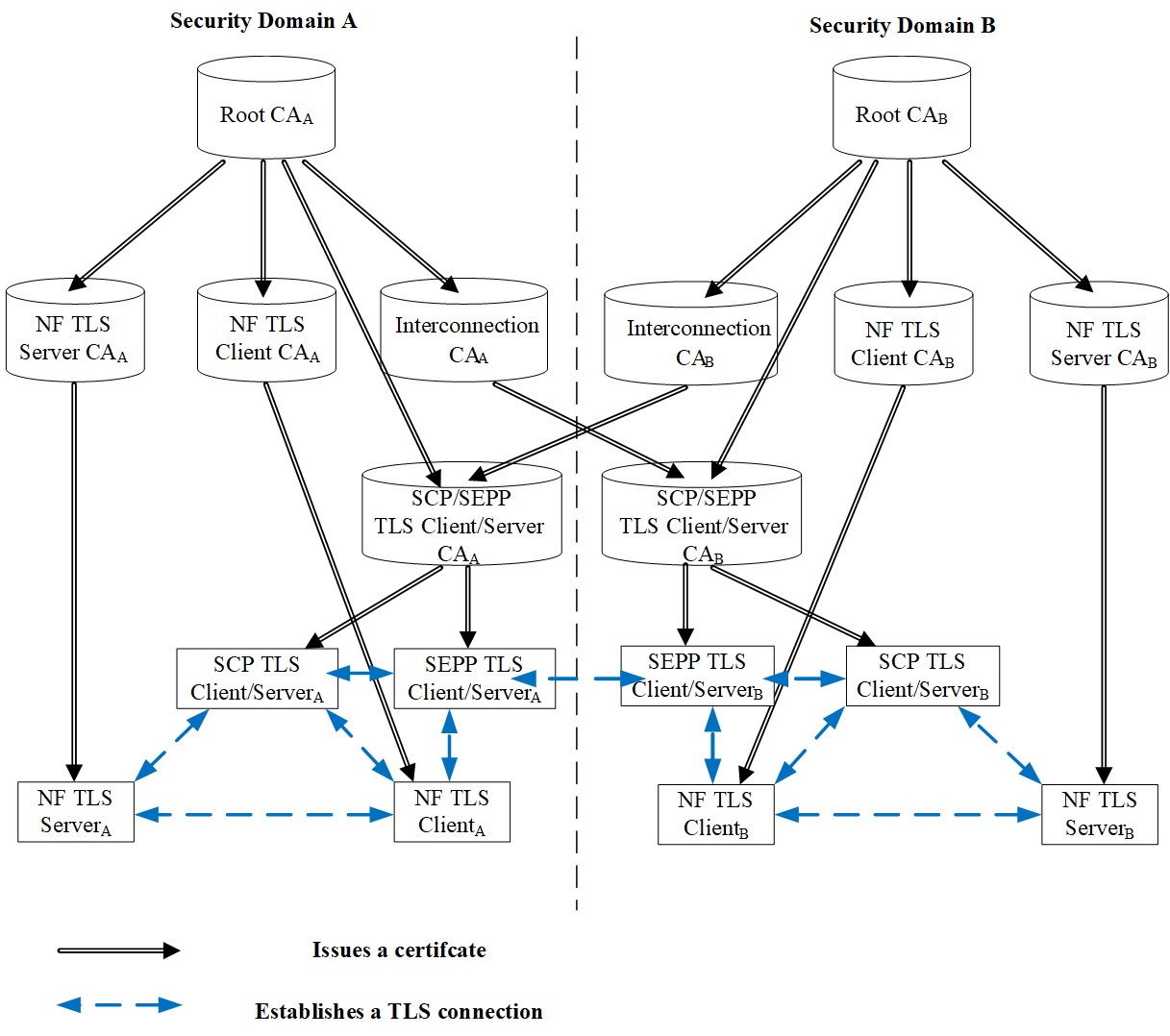


Figure 6.5.2.1-1: General Architecture

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: 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.

Editor’s Note: Whether one PKI domain (i.e., one Root CA) per security domain, or one PKI domain can be per other aspects for SBA certificates is FFS.

Editor’s Note: Whether using one PKI domain for both intra-PLMN and inter-PLMN SBA certificates is FFS.

#### 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

TBD

## 6.6 Solution #6: OCSP based revocation procedure

### 6.6.1 Introduction

The solution addresses the requirement of key issue 3 and 5 focusing mainly on the trigger aspects. 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.

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.

Editor's Note: When revocation status is unknown, whether hard-fail or soft-fail the TLS connection is FFS

### 6.6.3 Evaluation

Editor's note: evaluation is ffs

## 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

Editor's note: Involvement of the NRF requires further study.

Editor's note: Interaction with OAM is FFS.

### 6.7.3 Evaluation

TBD

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):  
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 |