 O-RAN.WG11.Cert-Mgmt-Framework-TR.0-R004-v04.00

Technical Report

O-RAN Work Group 11 (Security Work Group)

Study on Certificate Management Framework

Copyright © 2025 by the O-RAN ALLIANCE e.V.

The copying or incorporation into any other work of part or all of the material available in this specification in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material of this specification for your personal use, or copy the material of this specification for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

Register of Associations, Bonn VR 11238, VAT ID DE321720189

Contents

1 Introduction 10

1.1 Scope 10

2 References, Definitions, Terms and Abbreviations 11

2.1 Informative References 11

2.2 Definitions and Abbreviations 13

2.2.1 Definitions 13

2.2.2 Abbreviations and acronyms 14

2.2.3 Terms 15

3 Architecture Requirements and Assumptions 16

3.1 Architecture Requirements 16

3.2 Architecture Assumptions 16

3.2.1 Use Case for Physical Network Functions 16

4 Key Issues 18

4.1 Key Issue #1: Considering RA and CA as separate logical entities 18

4.1.1 General Description 18

4.1.2 Security Threats 18

4.2 Key Issue #2: Usage of PSK/Refnum for Initial Certificate Enrolment of PNFs 18

4.2.1 General Description 18

4.2.2 Security Threats 19

4.3 Key Issue #3: Usage of Vendor Certificates for Initial Certificate Enrolment of PNFs 19

4.3.1 General Description 19

4.3.2 Security Threats 19

4.4 Key Issue #4: Void 19

4.5 Key Issue #5: Void 19

4.6 Key Issue #6: Initial Certificate Enrolment for new NFs 19

4.6.1 General Description 19

4.6.2 Security Threats 19

4.7 Key Issue #7: Void 20

4.8 Key Issue #8: Vendor Root CA Certificate Renewal 20

4.8.1 General Description 20

4.8.2 Security Threats 20

4.9 Key Issue #9: Void 20

4.10 Key Issue #10: Procedure for Certificate Updates when revoked certificates are detected by NFs 20

4.10.1 General Description 20

4.10.2 Security Threats 21

4.11 Key Issue #11: Void 21

4.12 Key Issue #12: Certificate to name mapping 21

4.12.1 General Description 21

4.12.2 Security Threats 21

4.13 Key Issue #13: System overload due to bulk certificate updates 22

4.13.1 General Description 22

4.13.2 Security Threats 22

4.14 Key Issue #14: Void 23

4.15 Key Issue #15: Void 23

4.16 Key Issue #16: Void 23

4.17 Key Issue #17: Void 23

4.18 Key Issue #18: Allow Flexibility in the Number of Operator Certificates Associated with each end entity / Interface 23

4.18.1 General Description 23

4.18.2 Security Threats 23

4.19 Key Issue #19: Certificate Management in Distributed Cluster Processing 24

4.19.1 General Description 24

4.19.2 Security Threats 24

4.20 Key Issue #20: Certificate Management and Secure Storage of Application Private Keys 25

4.20.1 General Description 25

4.20.2 Security Threats 25

4.21 Key Issue #21: Coordinating Certificate Management with VNF/CNF Lifecycle Activities 25

4.21.1 General Description 25

4.21.2 Security Threats 26

4.22 Key Issue #22: Supporting Public and Private Certificate Authorities (CA) 26

4.22.1 General Description 26

4.22.2 Security Threats 26

4.23 Key Issue #23: Distribution of Intermediate and Root Certificates 27

4.23.1 General Description 27

4.23.2 Security Threats 27

4.24 Key Issue #24: CMPv2 Message Minimal Set and Robustness 28

4.24.1 General Description 28

4.24.2 Security Threats 28

4.25 Key Issue #25: RA and CA Capacity Estimation, Renewal Intervals and Credential Strength 28

4.25.1 General Description 28

4.25.2 Security Threats 28

4.26 Key Issue #26: Namespace Conventions 29

4.26.1 General Description 29

4.26.2 Security Threats 29

4.27 Key issue #27: Handling of certificate revocation in O-RAN 29

4.27.1 General Description 29

4.27.2 Security Threats 30

4.28 Key issue #28: Risk of Service un-availability due to root CA Certificate updates for CNFs and VNFs 30

4.28.1 General Description 30

4.28.2 Security Threats 31

4.29 Key issue #29: Certificate requirements for O-Cloud control plane 31

4.29.1 General Description 31

4.29.2 Security Threats 32

4.30 Key issue #30: Certificate management for cloud deployment models 32

4.30.1 General Description 32

4.30.2 Security Threats 32

4.31 Key issue #31: Void 32

4.32 Key issue #32: Void 33

4.33 Key issue #33: Certificate Profiling in O-RAN 33

4.33.1 General Description 33

4.33.2 Security Threats 33

4.34 Key issue #34: Void 33

4.35 Key issue #35: Void 34

4.36 Key issue #36: Certificate sharing or not-sharing in Apps/VNFs/CNFs 34

4.36.1 General Description 34

4.36.2 Security Threats 34

4.37 Key issue #37: Lightweight solution 35

4.37.1 General Description 35

4.37.2 Security Threats 35

4.38 Key issue #38: Interoperability 35

4.38.1 General Description 35

4.38.2 Security Threats 35

4.39 Key issue #39: Crypto agility 36

4.39.1 General Description 36

4.39.2 Security Threats 36

4.40 Key issue #40: Void 36

4.41 Key Issue #41: CMPv2 36

4.41.1 General Description 36

4.41.2 Security Threats 36

4.42 Key Issue #42: Certificate management for Shared O-RU 36

4.42.1 General Description 36

4.42.2 Security Threats 37

4.43 Key Issue #43: NF with an expired certificate 37

4.43.1 General Description 37

4.43.2 Security Threats 37

5 Solutions 38

5.1 Solution #1: Automation of PSK/Refnum based Certificate Enrolment 38

5.1.1 Description 38

5.1.2 Impacts on Existing Interfaces and Functionality 38

5.1.3 Solution Evaluation 38

5.1.4 Potential Security Requirements 38

5.2 Solution #2: Study the use of BRSKI 38

5.2.1 Description 38

5.2.2 Impacts on Existing Interfaces and Functionality 39

5.2.3 Solution Evaluation 39

5.2.4 Potential Security Requirements 40

5.3 Solution #3: Study the use of EST 40

5.3.1 Description 40

5.3.2 Impacts on Existing Interfaces and Functionality 42

5.3.3 Solution Evaluation 42

5.3.4 Potential Security Requirements 42

5.4 Solution #4: Study the use of ACME 42

5.4.1 Description 42

5.4.2 Impacts on Existing Interfaces and Functionality 44

5.4.3 Solution Evaluation 44

5.5 Solution #5: Initial Certificate Enrolment of PNFs using vendor certificates 45

5.5.1 Description 45

5.5.2 Impacts on Existing Interfaces and Functionality 45

5.5.3 Solution Evaluation 46

5.5.4 Potential Security Requirements 46

5.6 Solution #6: Certificate management and secure storage of Application private keys within O-Cloud 46

5.6.1 Description 46

5.6.2 Generation of key pair and modes of operation 46

5.6.3 Secure key and file storage 50

5.6.4 Impacts on Existing Interfaces and Functionality 53

5.6.5 Solution Evaluation 53

5.6.6 Potential Security Requirements 53

5.7 Solution #7: CMPv2 54

5.7.1 Description 54

5.7.2 Impacts on Existing Interfaces and Functionality 54

5.7.3 Solution Evaluation 54

5.7.4 Potential Security Requirements 54

5.8 Solution #8: Vendor Root CA Certificate Renewal notification 55

5.8.1 Description 55

5.8.2 Impacts on Existing Interfaces and Functionality 55

5.8.3 Solution Evaluation 55

5.8.4 Potential Security Requirements 56

5.9 Solution #9: Mitigating the risk of system overload due to bulk certificate updates 56

5.9.1 Description 56

5.9.2 Impacts on Existing Interfaces and Functionality 57

5.9.3 Solution Evaluation 57

5.9.4 Potential Security Requirements 57

5.10 Solution #10: Usage of PSK/Refnum for Initial Certificate Enrolment for PNFs 57

5.10.1 Description 57

5.10.2 Impacts on Existing Interfaces and Functionality 58

5.10.3 Solution Evaluation 58

5.10.4 Potential Security Requirements 58

5.11 Solution #11: Certificate renewal procedure 58

5.11.1 Description 58

5.11.2 Impacts on Existing Interfaces and Functionality 59

5.11.3 Solution Evaluation 59

5.11.4 Potential Security Requirements 60

5.12 Solution #12: Certificate Profile for O-RAN TLS Entity 60

5.12.1 Description 60

5.12.2 Impacts on Existing Interfaces and Functionality 61

5.12.3 Solution Evaluation 61

5.12.4 Potential Security Requirements 63

5.13 Solution #13: Identifying RA and CA as separate logical entities with flexible deployment options 63

5.13.1 General Description 63

5.13.2 Impacts on Existing Interfaces and Functionality 64

5.13.3 Solution Evaluation 64

5.13.4 Potential Security Requirements 64

5.14 Solution #14: Securing Root CA Private Key 65

5.14.1 General Description 65

5.14.2 Impacts on Existing Interfaces and Functionality 65

5.14.3 Solution Evaluation 65

5.14.4 Potential Security Requirements 65

5.15 Solution #15: Certificate enrolment for new NF Deployment using CMPv2 66

5.15.1 General Description 66

5.15.2 Impacts on Existing Interfaces and Functionality 68

5.15.3 Solution Evaluation 68

5.15.4 Potential Security Requirements 68

6 Conclusions 69

6.1 Key Issue #41: CMPv2 69

6.2 ACME as Optional Certificate Management Protocol 69

6.3 Usage of PSK/Refnum for initial certificate enrolmentenrolment for PNFs, CNFs and VNFs 69

6.4 Vendor root CA certificate renewal notification 69

6.5 Initial certificate enrolmentenrolment for PNFs using vendor certificates 70

6.6 Certificate renewal procedure 70

6.7 RA and CA as separate logical entities 70

6.8 EST as Optional Certificate Management Protocol 70

6.9 Use of BRSKI in O-RAN 70

6.10 Mitigating the risk of system overload due to bulk certificate update 70

6.11 Key Issue #20: Certificate Management and Secure Storage of Private Keys 71

6.11.1 Evaluation and Assessment for local security module managed by SSRM within the O-Cloud 71

6.11.2 Evaluation and Assessment for the KMS 71

6.11.3 Conclusion 72

6.12 Cert Profile for O-RAN TLS Entity 72

6.13 Certificate enrollment for new NF Deployment using CMPv2 72

7 Key Issues-Solutions mapping 73

Annex: Change history/Change request (history) 74

**List of Figures**

[Figure 3‑1: Logical Architecture of O-RAN system: Overview of the security architecture 16](#_Toc170122224)

[Figure 4‑1: A possible system comprising different applications with different Root Certificates. 31](#_Toc170122225)

[Figure 5‑1: Certificate-less TLS Authentication 41](#_Toc170122226)

[Figure 5‑2: Certificate-based TLS Authentication. 41](#_Toc170122227)

[Figure 5‑3: A simplified depiction of the workings of ACME 43](#_Toc170122228)

[Figure 5‑4: Secure Storage and Certificate Management Architecture (System Level View) 47](#_Toc170122229)

[Figure 5‑5: Key-generation by the Virtualisation Platform 48](#_Toc170122230)

[Figure 5‑6: Key-generation by the Trusted Application 49](#_Toc170122231)

[Figure 5‑7: Key-generation by the Secure Module (e.g., HSM, TPM) 50](#_Toc170122232)

[Figure 5‑8: Secure Key and File Storage Architecture Framework (overview) 51](#_Toc170122233)

[Figure 5‑9: Scenarios for protecting keys within the secret storage volume based on TPM 52](#_Toc170122234)

[Figure 5‑10: Key protection based on KMS 52](#_Toc170122235)

[Figure 5‑11: Certificate Update Orchestrator 57](#_Toc170122236)

[Figure 5‑12: Certificate renewal procedure 59](#_Toc170122237)

[Figure 5‑13 Certificate enrollment for new NF Deployment 68](#_Toc170122238)

# Introduction

## Scope

This technical report studies a comprehensive framework for certificate management across the O-RAN environment.

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

* Standardize a certificate management framework comprising protocols and procedures for certificate life cycle events (e.g. enrolment, renewal, revocation) within the O-RAN architecture (e.g., O-CU, O-DU, O-RU, Open Fronthaul, Non-RT-RIC, Near-RT-RIC, etc.)
* Address the following objectives:
  + Support reuse of IETF CMPv2 certificate management
  + Explore the IETF ACME, IETF BRSKI, IETF EST, and other industry efforts as potential components for a certificate management framework.
  + Establish lifecycle service models to bring zero touch automation to the certificate management framework.

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

1. version xx.yy.zz
2. where:

xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.

yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.

zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

# References, Definitions, Terms and Abbreviations

## Informative References

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, O-RAN cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

1. 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”
2. 3GPP TR 33.310: "Network Domain Security (NDS); Authentication Framework (AF)"
3. O-RAN ALLIANCE TS: "O-RAN Management Plane Specification"
4. RFC-6187: X.509v3 Certificates for Secure Shell Authentication
5. IETF RFC 4210: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
6. Design and build a privately hosted Public Key Infrastructure

<https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/pki-principles/protect-your-private-keys>

1. NIST SP 1800-16C: Securing Web Transactions: TLS Server Certificate Management

<https://csrc.nist.gov/publications/detail/sp/1800-16/final>

1. 3GPP TS 32.509: "Data formats for multi-vendor plug and play eNode B connection to the network"
2. Void
3. Void
4. ETSI GR NFV-SEC 005, NFV, trust, report on certificate management
5. ETSI GR NFV-IFA 029, Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"
6. IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
7. IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2
8. IETF RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3
9. IETF RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2)
10. IETF RFC 6066: Transport Layer Security (TLS) Extensions: Extension Definitions
11. IETF RFC 6125: Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)
12. IETF RFC 7633: X.509v3 Transport Layer Security (TLS) Feature Extension
13. CA-Browser-Forum-BR-1.8.0: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, August 2021, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.0.pdf>.
14. IETF RFC 6347: Datagram Transport Layer Security Version 1.2
15. IETF RFC 9325: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layert Security (DTLS)
16. Service Identity in TLS <https://datatracker.ietf.org/doc/draft-ietf-uta-rfc6125bis/>
17. IETF RFC 7093:Additional Methods for Generating Key Identifiers Values
18. NIST Special Publication 800-52 Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
19. IETF RFC 6960:X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
20. IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
21. RFC 8995: Bootstrapping Remote Secure Key Infrastructure (BRSKI)
22. RFC 8993: A Reference Model for Autonomic Networking
23. RFC 8994: An Autonomic Control Plane (ACP)
24. RFC 8572: Secure Zero Touch Provisioning (SZTP)
25. IETF RFC 7030: Enrollment over Secure Transport
26. IETF RFC 5054: Using the Secure Remote Password (SRP) Protocol for TLS Authentication
27. IETF RFC 8295: EST (Enrollment over Secure Transport) Extensions
28. IETF RFC 5272: Certificate Management over CMS
29. IETF RFC 8951: Clarification of Enrollment over Secure Transport (EST): Transfer Encodings and ASN.1
30. IETF RFC 8996: Deprecating TLS 1.0 and TLS 1.1
31. IETF RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
32. IETF RFC 3986:Uniform Resource Identifier (URI): Generic Syntax
33. IETF RFC 2119: Key words for use in RFCs to Indicate Requirement Levels
34. O-RAN ALLIANCE TS: “Security Protocols Specifications”
35. IETF RFC 8555: Automatic Certificate Management Environment (ACME)
36. IETF RFC 8738: Automated Certificate Management Environment (ACME) IP Identifier Validation Extension
37. 3GPP TS 28.315: "Management and orchestration; Plug and connect; Procedure flows"
38. 3GPP TS 28.314: "Management and orchestration; Plug and connect; Concepts and requirements"
39. ETSI GR NFV-SEC 009, NFV Security,”Report on use cases and technical approaches for multi-layer host administration”
40. O-RAN ALLIANCE TS: “Security Requirements and Controls Specification”
41. Cryptographic Key Generation: NIST Publishes SP 800-133 Rev. 2, https://csrc.nist.gov/news/2020/nist-publishes-sp-800-133-rev-2
42. SOG-IS Agreed Cryptographic Mechanisms v1.3, <https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>
43. NIST Special Publication 800-57 Part 1 Revision 5: Recommendation for Key Management
44. O-RAN ALLIANCE TS: "O-RAN Architecture Description"
45. O-RAN ALLIANCE TS: "Cloudification and Orchestration Use Cases and Requirements for O-RAN Virtualized RAN"

## Definitions and Abbreviations

### Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [i.1] and the following apply:

**A1**: Interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.

**A1 policy:** Type of declarative policies expressed using formal statements that enable the Non-RT RIC function in the SMO to guide the Near-RT RIC function, and hence the RAN, towards better fulfilment of the RAN intent.

**A1 Enrichment information:** Information utilized by Near-RT RIC that is collected or derived at SMO/Non-RT RIC either from non-network data sources or from network functions themselves.

**E2**: Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.

**E2 Node**: a logical node terminating E2 interface. In this version of the specification, O-RAN nodes terminating E2 interface are:

- for NR access: O-CU-CP, O-CU-UP, O-DU or any combination.

- for E-UTRA access: O-eNB.

**FCAPS:** Fault, Configuration, Accounting, Performance, Security.

**Intents**: A declarative policy to steer or guide the behavior of RAN functions, allowing the RAN function to calculate the optimal result to achieve stated objective.

**Near-RT RIC:** O-RAN near-real-time RAN Intelligent Controller: a logical function that enables real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface.

**Non-RT RIC:** O-RAN non-real-time RAN Intelligent Controller: a logical function that enables non-real-time control and optimization of RAN elements and resources, AI/ML workflow including model training and updates, and policy-based guidance of applications/features in Near-RT RIC.

**O-CU:** O-RAN Central Unit: a logical node hosting O-CU-CP and O-CU-UP

**O-CU-CP**: O-RAN Central Unit – Control Plane: a logical node hosting the RRC and the control plane part of the PDCP protocol.

**O-CU-UP**: O-RAN Central Unit – User Plane: a logical node hosting the user plane part of the PDCP protocol and the SDAP protocol.

**O-DU**: O-RAN Distributed Unit: a logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split.

**O-RU**: O-RAN Radio Unit: a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split. This is similar to 3GPP’s “TRP” or “RRH” but more specific in including the Low-PHY layer (FFT/iFFT, PRACH extraction).

**O1:** Interface between management entities (NMS/EMS/MANO) and O-RAN managed elements, for operation and management, by which FCAPS management, Software management, File management shall be achieved.

**RAN**: Generally referred as Radio Access Network. In terms of this document, any component below Near-RT RIC per O-RAN architecture, including O-CU/O-DU/O-RU.

**Secure Storage and Retrieval Manager (SSRM):** a component designed to manage the secure storage, retrieval, and lifecycle management of sensitive data, such as cryptographic keys, certificates, and secrets, within the O-Cloud. The SSRM acts as an intermediary layer that abstracts the underlying complexities of secure storage mechanisms and provides standardized interfaces for applications and services to interact with secure resources.

In Kubernetes environments, the combination of the kube-apiserver and cert-manager serves as an embodiment of an SSRM. The kube-apiserver acts as the central entry point for interactions with the Kubernetes control plane, providing authentication, authorization, and a unified API surface. Paired with cert-manager, which automates the management of TLS certificates and abstracts the intricacies of secure storage, this combination streamlines secure communication within Kubernetes clusters. The kube-apiserver offers centralized management, while cert-manager automates the secure storage and retrieval of certificates and private keys, ensuring a seamless and secure experience for applications.

In OpenStack ecosystems, the collaboration between Keystone and Barbican mirrors the SSRM concept. Keystone functions as the identity and access management service, handling authentication, authorization, and policy enforcement. Complementing Keystone, Barbican operates as a secure key management system, safeguarding cryptographic keys and secrets. Together, Keystone and Barbican provide a standardized approach to secure storage, ensuring sensitive data remains protected while abstracting the complexities of secure key management.

### Abbreviations and acronyms

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [i.1] and the following apply:

ACME Automatic Certificate Management Environment

ACP Autonomic Control Plane

AI/ML Artificial Intelligence/Machine Learning

ANI Autonomic Networking Infrastructure

BRSKI Bootstrapping Remote Secure Key Infrastructure

CA Certification Authority

CMPv2 Certificate Management Protocol version 2

CUO Certificate Update Orchestrator

DEK Disk Encryption Key

eNB eNodeB (applies to LTE)

EST Enrollment over Secure Transport

FTP File Transfer Protocol

FTPS File Transfer Protocol Secure

gNB gNodeB (applies to NR)

IPsec Internet Protocol Security

KEK Key Encryption Key

KMS Key Management System

KPI Key Performance Indicator

KQI Key Quality Indicator

LBT Listen Before Talk

LLS Lower Layer Split

MIMO Multiple Input, Multiple Output

MNO Mobile Network Operator

NETCONF Network Configuration Protocol

NF Network Function

NFV Network Function Virtualisation

O-RAN Open Radio Access Network

PDCP Packet Data Convergence Protocol

PNF Physical Network Function

PRB Physical Resource Block

PTP Precision Timing Protocol

QoE Quality of Experience

RA Registration Authority

RBAC Role-based Access Control

RIC O-RAN RAN Intelligent Controller

SDN Software Defined Network

SEK Secret Encryption Key

SINR Signal-to-Interference-plus-Noise Ratio

SMO Service Management and Orchestration

SSH Secure Shell

SSRM Secure Storage Resource Manager

SZTP Secure Zero Touch Provisioning

TLS Transport Layer Security

UAV Unmanned Aerial Vehicle

V2X Vehicle to Everything

VM Virtual machine

VNF Virtualised Network Function

### Terms

In this document, the significance of the following words are as defined in the RFC 2119 [i.40] publication by IETF. These words are:

* "SHALL" This word, or the words "REQUIRED" and "MUST" mean that the process is an absolute requirement of the specification.
* "SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood, and the case carefully weighed before choosing a different course.
* "MAY" This word or the adjective "optional" means that this item is truly optional. One vendor may choose to include the process because a particular marketplace requires it or because it enhances the product, for example, another vendor may omit the same item.

# Architecture Requirements and Assumptions

## Architecture Requirements

The Certificate Management Framework Architecture should be compatible with the M-Plane Certificate Management Framework specified in O-RAN Management Plane Specification [i.3]. These certificates conform to the X.509v3 certificate profile in RFC 5280 [i.30].

The M-Plane Certificate Management Framework in O-RAN Management Plane Specification [i.3] references Clause 9 of 3GPP TS 33.310 [i.2] where CMPv2 is used by “base stations to obtain an operator-signed certificate using a secured communication based on the vendor-signed certificate in the base station and a vendor root certificate pre-installed in the CA/RA server.”

The M-Plane Certificate Management Framework in O-RAN Management Plane Specification [i.3] also states that “while the approach in [i.2] has been defined for provisioning certificates for use in either IPsec or TLS, the same techniques defined for provisioning TLS certificates are specified to be re-used to provision certificates for use in securing the SSHv2 based M-Plane connection as specified in RFC 6187 [i.4]. Hence, the TLS client CA is responsible for issuing certificates to NETCONF clients, irrespective of whether NETCONF is secured using TLS or SSHv2. Similarly, the TLS server CA is responsible for issuing certificates to NETCONF servers, irrespective of whether NETCONF is secured using TLS or SSHv2.”

## Architecture Assumptions

### Use Case for Physical Network Functions

Figure 3‑1 shows a general deployment architecture for certificate enrolment of a physical NF by an operator PKI. This general deployment architecture is generalized from clause 9 of 3GPP 33.310 [i.2].

The NF obtains the operator-signed certificate on its own public key from RA/CA using CMPv2.

Secure  
protocol

Enrolled NF certificate is used in the security association.

NF B

Vendor root certificate is pre-installed.

Vendor-signed certificate of NF public key is pre-installed.

CMPv2

NF

RA/CA

Figure 3‑1: Logical Architecture of O-RAN system: Overview of the security architecture

The NF is pre-provisioned with a public-private key pair by the vendor, and has the vendor-signed certificate of its public key pre-installed.

An operator may deploy an RA/CA to replace the vendor-provisioned certificates with operator provided certificates. The operator CA may be deployed using one of the following:

- either a stand-alone CA implementing a CMPv2 server, or

- a CA having delegated certain tasks to an RA, which is operating the CMPv2 server.

On initial contact to the operator network the NF establishes a communication channel to the RA/CA of the operator. Using CMPv2 [i.5] a request for a certificate is sent to the RA/CA. The network authenticates the messages from the NF based on the vendor-signed certificate of the NF and the vendor root certificate pre-installed in the network. The NF shall check the integrity protection on the messages from the RA/CA based on the operator root certificate provisioned in the NF. In a response message the NF receives the operator-signed certificate. During the execution of the CMPv2 protocol the NF has to successfully provide a Proof of Possession of the private key associated to the public key to be certified.

The operator root certificate may be provisioned in the NF prior to or during the CMPv2 protocol run. The protection of the operator root certificate during provisioning may be decided by operator security policy. If an operator root certificate provisioned prior to the CMPv2 protocol run is available, the NF shall use it. Otherwise, the NF shall use the operator root certificate provisioned during the CMPv2 run. If no operator root certificate is provisioned at all then the NF shall abort the procedure.

After enrolment has been performed, the NF can use the operator-signed certificate to authenticate itself to the NF B of the operator, which is pre-installed with the operator root certificate. The NF then authenticates the NF B using the operator root certificate.

If at later stage of NF deployment the operator wants to renew the NF certificate, the same procedure will be executed with the old operator-signed certificate of the NF taking the place of the vendor-signed certificate in the initial enrolment.

# Key Issues

## Key Issue #1: Considering RA and CA as separate logical entities

### General Description

Given the system requirements for O-RAN, it’s essential to recognize the Registration Authority (RA) and Certificate Authority (CA) as individual logical units. Some implementations might integrate both within the same network, while others could opt for separate networks, possibly utilizing third-party CAs. As highlighted in RFC4210 [i.5] Appendix A, the justification for an RA's presence can be categorized into technical and organizational reasons. Technically, not all end entities have the necessary hardware for token initialization, making it beneficial for the RA to have this capability, which could also be driven by policy considerations. Moreover, certain entities might not be equipped to issue certificates, underscoring the RA's potential role in this aspect. Organizationally, centralizing tasks within the RA might be more cost-effective, especially when there's a need for specialized token initialization equipment. By incorporating RAs, organizations might also reduce the number of CAs they require. RAs are often better positioned to link individuals with their digital identifiers, especially when the CA is located at a considerable distance from the end entity. It's also worth noting that many setups already possess an administrative structure, simplifying the process of identifying suitable RA candidates, a convenience that might not always extend to CAs.

NOTE: For example, in WG11, the work-item for Near-RT RIC discusses the security procedure for xApp registration, where Near-RT RIC can also act as RA for xApps.

### Security Threats

**Single Point of Compromise:** Combining RA and CA functions into one entity creates a single point of compromise. If an attacker gains access to this combined entity, they can both verify (as the RA) and issue (as the CA) certificates, leading to a complete breakdown of the trust model.

**Operational Complexity:** Merging or intertwining the roles of RA and CA can lead to operational challenges, increasing the risk of human errors or misconfigurations.

**Lack of Role Segregation:** Combining roles goes against the principle of least privilege, where entities should only have the minimum access required to perform their tasks. Misuse or abuse of privileges becomes a significant concern, especially if internal actors become malicious.

**Backup and Recovery Risks:** A combined system means there's more data to backup and recover, complicating these processes. This may cause data loss or prolonged downtimes can occur if backup or recovery fails.

**Policy Overlaps:** There might be policy overlaps or contradictions when RA and CA are combined. For instance, the policy for verifying an entity's identity (RA function) might conflict with the policy for issuing a certificate (CA function).

## Key Issue #2: Usage of PSK/Refnum for Initial Certificate Enrolment of PNFs

### General Description

Using PSK/Refnum as a method for the Initial Certificate Enrolment of PNFs is an approach that might be essential for ensuring backward compatibility. However, this method of Certificate Management could necessitate manual interventions, thereby introducing potential vulnerabilities. To mitigate these risks, there's a need for supporting solutions that can seamlessly automate the PSK/Refnum based Certificate Enrolment process.

### Security Threats

**Manual Intervention Risks:** Relying on manual steps for certificate enrolment can lead to human errors, misconfigurations, or oversights, which can compromise the security of the system. Incorrect certificate enrolments, unauthorized access, or even system downtimes can result from these errors, compromising the security and reliability of the O-RAN system.

## Key Issue #3: Usage of Vendor Certificates for Initial Certificate Enrolment of PNFs

### General Description

The use of Vendor Certificates for the initial registration and certificate enrolment is outlined in 3GPP TS 33.310 [i.2]clause 9 “Certificate Enrolment for base stations”.

This approach facilitates automated Certificate Enrolment, streamlining the integration of new PNFs with a plug-and-play model.

### Security Threats

**Vendor Trustworthiness**: Relying on vendor certificates necessitates a high level of trust in the vendor's security practices and certificate management. If a vendor's security practices are lax, it could lead to the issuance of compromised or weak certificates.

**Single Point of Failure:** If many PNFs rely on a single vendor's certificate for enrolment, it becomes a single point of failure.Compromise of the vendor certificate can jeopardize the security of all associated PNFs.

## Key Issue #4: Void

Void

## Key Issue #5: Void

Void

## Key Issue #6: Initial Certificate Enrolment for new NFs

### General Description

For the seamless integration of new NFs into the network, there's a need for an automated procedure to obtain CA-signed certificates. This process should ensure a pre-established trust relationship with the Registration Authority (RA).

### Security Threats

**Certificate Mismanagement:** If the procedure for obtaining CA-signed certificates isn't robust or secure, there's a risk of certificate mismanagement, misuse, or fraud. This may cause impersonation of legitimate NFs and/or network breaches.

**Lack of Automation**: Manual processes for NF certificate enrolment can introduce human errors, inconsistencies, or delays. This may cause misconfigurations and/or operational inefficiencies.

**Interception of Initial Communication**: The initial communication between the NF and the network during the enrolment phase could be intercepted if not securely encrypted. This may cause eavesdropping, data interception, or man-in-the-middle attacks.

**Inadequate Revocation Mechanisms**: If a NF is compromised or needs replacement, there should be a swift mechanism to revoke its certificate. Ongoing risks arise from breached NFs if certificate revocation is either delayed or not executed properly.

## Key Issue #7: Void

Void

## Key Issue #8: Vendor Root CA Certificate Renewal

### General Description

When a Vendor’s Root CA certificate approaches its expiration date, it's imperative for the Registration Authority (RA) to automatically renew the trust through the certificate management protocol. This proactive approach is essential to guarantee uninterrupted system availability.

### Security Threats

**Expired Certificate Usage**: If the Vendor's Root CA certificate expires without renewal, any NF relying on it could face authentication failures. This may cause system disruptions and/or declined connections.

**Dependency on Vendor:** The renewal process might depend on the vendor's responsiveness and their certificate issuance protocols. This may cause delays in certificate issuance and vulnerabilities in vendor-provided certificates.

**Manual Renewal Process:** Relying on a manual process for the renewal of the Vendor Root CA Certificate introduces several challenges. Manual processes inherently increase the risk of oversight, delays, and human error. Without automation, there's a higher likelihood that the certificate might expire before renewal, especially if the impending expiration goes unnoticed or if there are delays in the manual renewal procedure.

## Key Issue #9: Void

Void

## Key Issue #10: Procedure for Certificate Updates when revoked certificates are detected by NFs

### General Description

During the establishment of TLS or IPsec, an NF might detect revoked certificates. A clear and efficient procedure is essential to update such certificates to ensure the confidentiality and integrity of communications.

### Security Threats

**Continued Use of Revoked Certificates:** Without a prompt update procedure, NFs might continue using revoked certificates, leading to insecure communications.

**Delay in Certificate Replacement**: If the procedure for updating revoked certificates isn't efficient, there could be significant delays in replacing them. This may cause extended periods of vulnerability, potential NF disruptions, and declined connections.

**Lack of Automation:** Manual processes for updating revoked certificates can introduce human errors, inconsistencies, or delays. This may cause misconfigurations and/or operational inefficiencies.

**Inadequate Monitoring:** Without continuous monitoring, revoked certificates might go undetected or unaddressed for extended periods.

**Ineffective Revocation Lists**: If Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) servers are not updated promptly or are inaccessible, NFs might not detect revoked certificates in time. This may cause continued use of compromised certificates and unauthorized access.

## Key Issue #11: Void

Void

## Key Issue #12: Certificate to name mapping

### General Description

The Certificate-to-name mapping system is a critical component in the authorisation process. It can lead to a breakdown in the trust model of the O-RAN system. Unauthorized access, especially if mapped to high-privilege names, can compromise the integrity and availability of the O-RAN system.

### Security Threats

**Mapping Database Compromise**: If an attacker gains access to the system or database where the Certificate-to-name mappings are stored, they can alter these mappings. For instance, they might map their own certificate to a high-privilege username.

**Certificate Manipulation and spoofed authentication**:

The integrity and authenticity of certificates, pivotal in secure communications and authorisation within the O-RAN network, can be jeopardized through certificate manipulation and spoofed authentication. These threats can be notably exploited when the cipher used for signing the certificate lacks integrity assurance or when the TLS server is misconfigured, leading to inadequate validation of certificate signatures. This threat can be exploited under the following two cases:

* Exploitation through cipher integrity:
  + Attackers may alter or create certificates, manipulating identity information, and if the cipher lacks integrity, the system might accept these as valid, granting unauthorized access or privileges.
* Exploitation through TLS misconfiguration:
  + A TLS server that doesn’t validate certificate signatures accurately may accept manipulated or spoofed certificates, providing attackers unauthorized access based on misrepresented identity information.

The system, whether due to cipher integrity issues or TLS misconfigurations, may erroneously trust the manipulated or spoofed certificate, mapping it to a high-privilege username or granting unauthorized access and privileges.

Attackers, once authenticated, can perform unauthorized activities, such as data theft, network misconfigurations, or other malicious actions, under the guise of a legitimate entity.

## Key Issue #13: System overload due to bulk certificate updates

### General Description

When huge number of PNFs / VNFs need to update certificates, the system and communication networks may be overloaded.

If a huge number of network functions and/or services simultaneously require certificate updates (due to same expiry date, or, due to a common CA certificate revocation, or any other reason), it is possible that all of them trigger the certificate management procedures at the same time.

* Operators may want to frequently renew the certificates in order to mitigate any security risks involved with using the certificates for longer durations.
  + If, for example, a certain crypto algorithm is declared as compromised, it is likely that a huge number of network functions (physical and virtual) need to update their certificates.
* In scenarios when certificates are revoked, in order to avoid any security threats, it is desirable to update and use new certificates as soon as possible.
  + According to RFC 4210 [i.5](sections 5.3.13 and 5.3.15), CA may announce revocation of certificates. It is likely that such revoked certificates affect many NFs simultaneously.
  + When a new certificate needs to be used, existing secure connections (IPsec/TLS) need to be terminated. This may lead to intermittent unavailability of networks.
* For systems using certificates as authentication mechanisms for man-to-machine communications, the number of certificates will be directly proportional to the number of users. This could mean a large number of certificates, and maybe a need to update all of them together.

Automated certificate management facilitates the need for minimum manual intervention; however, this can lead to a congestion or overload in the system in scenarios when bulk certificate updates happening simultaneously. Such system overload may lead to un-intentional Denial-of-Services. In scenarios when multiple NF instances catering to specific network slices, the affected network slices may not be dimensioned to accommodate such overload due to bulk certificate updates.

### Security Threats

**System Overload:** When a large number of PNFs/VNFs simultaneously trigger certificate management procedures, it can cause significant strain on the system, potentially leading to slowdowns or outages.

**Communication Network Congestion:** The simultaneous update of certificates can lead to a surge in network traffic, causing congestion in communication networks.

**Potential Denial of Service (DoS):** Automated bulk certificate updates, especially if not properly managed or throttled, can unintentionally result in a DoS condition, making services unavailable to legitimate O-RAN NFs.

**Intermittent Network Unavailability:** When secure connections (like IPsec/TLS) need to be terminated to update certificates, it can lead to temporary network disruptions.

**Crypto Algorithm Compromise:** If a cryptographic algorithm is declared compromised, a vast number of network functions might need immediate certificate updates, exacerbating the overload issue.

**Certificate Revocation Risks:** The revocation of certificates, especially if affecting many network functions simultaneously, can lead to widespread disruptions if not managed properly.

**Delay in Addressing Security Threats:** While operators might want to renew certificates frequently to mitigate risks, the potential system overload can delay these updates, leaving the system vulnerable for longer durations.

**Man-to-Machine Authentication Risks:** For O-RAN systems with a large number of users using certificates for authentication, simultaneous updates can lead to widespread authentication failures or delays.

**Operational Complexity:** Managing and coordinating certificate updates for a vast number of PNFs/VNFs can be operationally complex, increasing the risk of errors or misconfigurations.

## Key Issue #14: Void

Void

## Key Issue #15: Void

Void

## Key Issue #16: Void

Void

## Key Issue #17: Void

Void

## Key Issue #18: Allow Flexibility in the Number of Operator Certificates Associated with each end entity / Interface

### General Description

This key issue addresses the procedure for certificate management when one network function in O-RAN (PNF/VNF/CNF) has several functionalities and several logical interfaces, thus one network function may have several identities for different functionalities and different communication interfaces [ETSI GR NFV-SEC005 V1.2.1 [i.11]].

### Security Threats

**Multiple Certificate Tracking:** With multiple certificates per network function, tracking, renewing, and revoking certificates becomes more complex. This complexity can lead to mismanagement or oversight, potentially leaving expired or compromised certificates in use.

**Multiple Points of Compromise:** Each certificate represents a potential point of compromise. With multiple certificates per network function, the attack surface increases, offering more opportunities for attackers to target or exploit a specific certificate.

**Ambiguous Authorization**: With multiple identities for a single network function, there's a risk of confusion in determining which certificate grants what level of access or functionality. This can lead to unintentional over-privilege or under-privilege in access controls.

**Granular Revocation:** If one certificate associated with a network function is compromised, determining whether to revoke only that certificate or all associated certificates can be challenging. Incorrect decisions can either leave vulnerabilities open or disrupt legitimate functionalities.

**Authentication overhead due to multiple certificates**: Engaging in multiple authentications across various interactions due to the management of numerous certificates for a network function interacting with different interfaces or systems, which could inadvertently introduce cumulative latency and operational delays in the network communication and data transmission processes.

**Varied Certificate Handling:** Different vendors might handle multiple certificates differently, leading to potential integration or interoperability challenges in a multi-vendor O-RAN environment.

**Bulk Operations Vulnerabilities:** Automated systems managing multiple certificates might inadvertently expose them to risks during bulk operations, like simultaneous renewals or updates, potentially leading to system overloads or misconfigurations.

## Key Issue #19: Certificate Management in Distributed Cluster Processing

### General Description

VNF and CNF components terminating interfaces that use X.509 certificates for authentication can be scaled across multiple instances on a single host and across multiple hosts. This distributed nature poses unique challenges for certificate management.

The certificate management framework must support these architectural patterns. It's imperative to ensure that as VNFs and CNFs scale, the associated certificates are managed securely and efficiently.

Adherence to best practices is crucial:

* Each VNF or CNF instance should ideally have its unique certificate. This not only ensures individualized authentication but also limits the potential security impact should any single instance be compromised.
* In environments like Kubernetes, controlling the traffic flow into and out of the cluster is vital. Assigning certificates to the ingress or egress points provides a layer of authenticated security.

Furthermore, as deployments expand to support geographic redundancy, the certificate management system should be capable of maintaining consistent security protocols across all NF instances, irrespective of their location.

### Security Threats

**Certificate Management Mistakes:** As VNF and CNF components scale across multiple instances and hosts, the sheer number of certificates to manage can become overwhelming, leading to potential mismanagement or oversight.

**Varying Certificate Assignments:** Different architectural patterns might lead to inconsistencies in how certificates are assigned, renewed, or revoked, potentially leaving vulnerabilities open or causing operational disruptions.

**Single Point of Failure:** If one instance of a VNF or CNF is compromised, and best practices like unique certificates for unique instances aren't followed, attackers might gain unauthorized access to other instances or components.

**Cluster Entry and Exit Points (Ingress/Egress Vulnerabilities):** Assigning a certificate to the ingress or egress point in a Kubernetes cluster can create a choke point. If this certificate is compromised, it can jeopardize the security of the entire cluster.

**Geographic Redundancy Concerns (Synchronization Issues):** Deployments that support geographic redundancy might face challenges in synchronizing certificate updates, renewals, or revocations across geographically distributed instances, leading to potential inconsistencies or vulnerabilities.

**Automated Scaling Risks:** In environments where instances are dynamically created or destroyed based on demand, ensuring that each instance has a valid, uncompromised certificate becomes challenging. There's a risk of instances being spun up with outdated or vulnerable certificates.

**Interoperability and Integration Issues:** Different VNF and CNF components, especially from different vendors or in different architectural patterns, might handle certificates differently, leading to potential integration challenges or security gaps.

**Revocation and Renewal Challenges:** With distributed clusters, determining which certificate to renew or revoke, especially in the event of a compromise, becomes complex. Incorrect decisions can disrupt legitimate services or leave vulnerabilities open.

## Key Issue #20: Certificate Management and Secure Storage of Application Private Keys

### General Description

Secure distribution and storage of Application certificates and private keys is critical to the effective use of certificates for authentication and confidentiality. The certificate management framework should include recommendations for secure storage of Applications private keys.

### Security Threats

**Storage compromise:** Without secure storage solutions like vaults where keys are stored can be breached, leading to the exposure of sensitive cryptographic material and the compromising the entire authentication mechanism.

**Man-in-the-Middle attacks:** Transmitting private keys over networks, if not done securely, can expose them to interception, leading to potential man-in-the-middle attacks.

**Physical access to storage:** If the environment isn't resistant to physical breaches, adversaries could gain physical access to the storage medium, leading to potential data theft or tampering.

**Lack of key rotation**: If the certificate management framework doesn't provide clear guidelines on key rotation, outdated or potentially compromised keys might continue in use.

**Regulatory violations:** Inadequate protection of cryptographic material can lead to violations of data protection regulations, resulting in penalties and reputational damage.

**Management challenges (Multiple NF instances)**: As the number of NF instances grows, ensuring that each instance securely generates and stores its private keys becomes operationally complex.

## Key Issue #21: Coordinating Certificate Management with VNF/CNF Lifecycle Activities

### General Description

The lifecycle activities of VNF/CNF are not always synchronized with the validity periods of their associated certificates. As these components evolve, undergo updates, or are replaced, it's crucial to ensure that their certificate management remains consistent and secure. Several scenarios highlight the importance of this coordination:

**Updating a VNF/CNF to a new version:** When updating or replacing a VNF/CNF, the handling of certificates becomes paramount. The updated component must maintain the same level of trust and authentication capabilities as its predecessor.

**Certificates stored in a vault or persistent storage:** If certificates are stored in a secure vault or other persistent storage solutions, a recreated or updated VNF/CNF should be able to access these without compromising security. The process for granting this access, especially in the context of updates or replacements, needs clear definition and robust security measures.

**Certificates embedded within the VNF/CNF:** For VNFs that store certificates internally, software component updates should not disrupt the availability or integrity of these certificates. It's essential to ensure that updates are seamless, without inadvertently affecting the stored certificates.

**Certificates managed by Kubernetes:** In environments where Kubernetes manages CNF containers and their certificates, updating or replacing CNF containers should not impact the availability or validity of the associated certificates. The orchestration platform must ensure that new container versions inherit the necessary certificates without security lapses.

### Security Threats

**Misalignment of certificate validity and component lifecycle (Expired certificates):** If the lifecycle of a VNF/CNF extends beyond the validity of its certificate, it might continue to operate with an expired certificate, leading to authentication failures or reduced trust.

**Inconsistent certificate management during updates (Loss of trust):** If an updated VNF/CNF doesn't maintain the same certificate or trust level as its predecessor, it can lead to trust breakdowns in the network, causing operational disruptions.

**Compromised certificate storage (Unauthorized access):** If the process of granting access to certificates in a vault or persistent storage isn't secure or if insecure vaults or storage solutions are used, malicious entities might gain unauthorized access to sensitive certificate data.

**Software update overwrites and loss of certificate integrity:** Updates to VNF/CNF components might inadvertently overwrite or corrupt internally stored certificates making them unusable or less secure, leading to potential authentication issues.

**Management overhead:** Coordinating certificate management with VNF/CNF lifecycle activities can increase operational complexity, leading to potential mismanagement or oversight.

## Key Issue #22: Supporting Public and Private Certificate Authorities (CA)

### General Description

To cater to the varied needs of different O-RAN network components and to offer flexibility in security configurations, the certificate management framework must be adept at managing a range of certificates. This includes client/server certificates, which facilitate secure interactions between O-RAN network entities, as well as intermediate certificates that form the chain of trust, and root certificates that anchor this trust.

Furthermore, the origin of these certificates can vary. They might be issued by public CAs, which are globally recognized and trusted entities, or by private CAs, which are often tailored for specific organizational or network needs. The O-RAN certificate management framework must seamlessly support and manage certificates from both these sources, ensuring that regardless of the CA's nature, the security and integrity of the O-RAN network remain uncompromised.

### Security Threats

**Mismanagement of multiple certificate sources:** Managing certificates from both public and private CAs can lead to inconsistencies in how certificates are validated, renewed, or revoked, potentially leaving vulnerabilities open or causing operational disruptions.

**Intermediate certificate compromise:** If an intermediate certificate is compromised, it can undermine the trust of any certificate issued under it.

**Root certificate exposure:** The exposure or compromise of a root certificate can jeopardize the entire trust chain.

**Private CA - Insufficient validation:** Private CAs, especially if not properly managed, might issue certificates without rigorous validation, leading to potential security risks.

**Private CA - Limited revocation capabilities:** Private CAs might not have the same robust infrastructure as public CAs for certificate revocation, leading to delays in revoking compromised certificates.

**Public CA - Global exposure:** Certificates from public CAs, being globally recognized, can be a target for attackers, leading to potential large-scale attacks or exposures.

**Public CA -** Third-party risks: Relying on external public CAs introduces third-party risks, where the compromise or mismanagement of the CA can impact the O-RAN network.

**Management overhead:** Coordinating certificate management from multiple sources (public and private CAs) can increase operational complexity, leading to potential mismanagement or oversight.

**Varied certificate standards:** Different CAs, especially across public and private domains, might have varied certificate standards or formats, leading to potential integration/interoperability challenges or security gaps.

**Regulatory violations:** Inadequate management or validation of certificates, especially from private CAs, can lead to violations of data protection or security regulations, resulting in penalties and reputational damage.

## Key Issue #23: Distribution of Intermediate and Root Certificates

### General Description

The management and distribution of intermediate and root certificates forms the backbone of the certificate trust chain. The O-RAN certificate management framework must be equipped with the capabilities that automate these processes. Specifically:

* Operators should have an automated mechanism to request both intermediate and root certificates from the Certificate Authorities (CA) responsible for issuing the deployment's certificates. This ensures timely and efficient acquisition of these critical trust anchors.
* Once acquired, there should be a straightforward method to load these certificates into the key stores of the various network components, be it PNF, VNF, or CNF. This ensures that every component in the network is aligned with the trust framework and can validate communications effectively.

### Security Threats

**Incomplete trust chain:** If intermediate or root certificates are not properly distributed or loaded, it can result in an incomplete or broken trust chain, leading to authentication failures or reduced trust.

**Unauthorized access during distribution:** If the distribution process isn't secure, certificates could be intercepted and potentially altered or replaced with malicious ones during transit.

**Exposure during Request:** An automated request mechanism that isn't properly secured can expose sensitive details or allow unauthorized entities to request certificates.

**Outdated certificates:** If the distribution process isn't timely, network components might operate with outdated intermediate or root certificates, leading to potential security risks.

**Misconfigurations:** Automated processes, if not properly configured, can lead to errors such as loading the wrong certificates or loading them into incorrect locations.

**CA compromise:** If the CA responsible for issuing certificates is compromised, it can lead to the distribution of malicious or unauthorized certificates.

**Regulatory violations:** Inadequate management or distribution of certificates can lead to violations of data protection or security regulations, resulting in penalties and reputational damage.

## Key Issue #24: CMPv2 Message Minimal Set and Robustness

### General Description

The O-RAN certificate management framework must clearly define the specific CMPv2 message set that will be supported. This not only standardizes the communication for certificate operations but also ensures that the network components have a consistent and robust protocol to rely on for certificate-related interactions. By specifying this minimal set, the framework aims to streamline certificate management processes, reduce ambiguities, and bolster the overall security and efficiency of the O-RAN network (3GPP TS 33.310 [i.2] clause 9.5 has a CMPv2 profile definition).

### Security Threats

**CMPv2 Exploits:** If the CMPv2 protocol or its implementation has vulnerabilities, attackers could exploit these to compromise certificate operations or gain unauthorized access.

**Inconsistent message handling:** Without a clearly defined message set, different network components might handle CMPv2 messages inconsistently, leading to potential security gaps or operational disruptions.

**Ambiguities in message processing:** Without a clear and minimal set of supported messages, there could be ambiguities in how messages are processed, leading to potential errors or security risks.

## Key Issue #25: RA and CA Capacity Estimation, Renewal Intervals and Credential Strength

### General Description

In the evolving landscape of O-RAN networks, the strength and validity of cryptographic credentials play a pivotal role in ensuring secure communications. Adhering to best practices, the current recommendations emphasize:

* Validity periods: Certificates should have validity periods that don't exceed one year. This ensures that credentials are regularly updated, reducing the window of vulnerability, and aligning with the dynamic nature of network environments.
* Elliptical Curve Cryptography (ECC): When leveraging ECC algorithms, it’s advised to use key lengths of three hundred eighty-four (384) bits. This strikes a balance between computational efficiency and security, providing robust protection against potential cryptographic attacks.
* Diffie-Hellman Cryptography: For systems employing Diffie-Hellman cryptographic algorithms, key lengths should be set to a minimum of two thousand and forty-eight (2048) bits. This ensures a high level of security, making it computationally challenging for adversaries to compromise the encryption.

### Security Threats

**Certificate expiry and renewal:**

* If certificates expire without timely renewal, it can lead to authentication failures or communication breakdowns.
* Longer validity periods can provide attackers with a more extended window to exploit potential vulnerabilities associated with a certificate.

**Brute Force attacks:** Insufficient key lengths can make cryptographic algorithms susceptible to brute force attacks.

**Cryptographic vulnerabilities:** As cryptographic research progresses, older algorithms or shorter key lengths might be found vulnerable. If not updated, they can be exploited.

**ECC - Weak Curves:** Not all elliptical curves provide the same security level. Using weak or compromised curves can lead to reduced security.

**DH - Man-in-the-Middle attacks:** Without proper authentication or with shorter key lengths, Diffie-Hellman can be vulnerable to man-in-the-middle attacks.

**Logjam Attack:** If not properly configured, Diffie-Hellman is susceptible to the Logjam attack, where attackers can downgrade to vulnerable TLS connections.

**Performance overhead:** While longer key lengths provide better security, they also come with a performance overhead, potentially affecting network efficiency.

## Key Issue #26: Namespace Conventions

### General Description

The certificate management framework should develop common namespace template examples (Cert Subject/SANs) to facilitate rapid integration with multiple vendor products and enable cross operator integration.

VendorName and OperatorName should be the only required inputs to generate all namespaces.

Namespace conventions should only be defined after the other key issues have been addressed. Additionally, it must be determined which entity, the client requesting a certificate or the CMPv2 implementation used by the client, is responsible for specifying each component of a named field, e.g., subject or SAN.

### Security Threats

**Inconsistent namespace use:** If namespace conventions are not consistently used across all certificates, it could lead to integration issues, misconfigurations, or erroneous trust establishment between entities.

**Integration challenges:** Without standardized namespace conventions, integrating multiple vendor products and enabling cross-operator integration might become cumbersome and error-prone, potentially leading to security loopholes.

**Impersonation threats:** In the absence of stringent namespace conventions, attackers might exploit the laxity to create certificates that impersonate legitimate entities, thereby gaining unauthorized access and compromising secure communications.

## Key issue #27: Handling of certificate revocation in O-RAN

### General Description

Certificates revocation procedures are a critical part of the overall certificate lifecycle management. Every certificate has a finite validity period, during which the certificate it is expected to be in use. However, prior to the expiration of the validity period, the Certification Authority (CA) may declare that a certificate that it issued can no longer be trusted due to multiple circumstances including suspected compromise of the private key.

How do we handle certificate revocation in O-RAN elements? Certificate validation requires access to revocation information, either in the form of a Certificate Revocation Lists (CRL) or an Online Certificate Status Protocol (OCSP) response. OCSP Responses are often included in a TLS handshake; this practice is called OCSP stapling.

RFC 5280 [i.30] defines a CRL as ‘a time-stamped list identifying revoked certificates that is signed by a CA or CRL issuer and made freely available in a public repository’. The method involves each CA/CRL issuer periodically issuing such list, in order to communicate the revocation status of the affected certificates. When a client wants to retrieve a CRL for a particular certificate, it retrieves it from a specified CRL Distribution Point (CRLDP) that is carried in the certificate itself. Typically, HTTP is used to fetch the CRL, and the locations supporting the download of the CRL are chosen to reduce the inherent latency of the procedure.

OCSP, defined in RFC 6960 [i.26], is ‘a protocol useful in determining the current status of a digital certificate without requiring CRLs’. It can be used in addition to or instead of CRLs. OCSP is often faster than CRL checking process. With OCSP stapling (refer to RFC 6066 [i.17]) the OCSP Response is fetched by the TLS server before the handshake, and then it is transported together with the certificate (“stapled”) during the handshake. OCSP stapling reduces latency and increases availability of the revocation information, hiding any OCSP Responder outages, even very short ones.

When a CA has revoked, or it is about to revoke, a particular certificate, it may issue an announcement for revocation, to enable the automated re-enrolment; see Section 5.3.15 of RFC 4210 [i.5]).

In some situations, an RA can detect revoked Vendor / Service Provider’s CA certificates. The RA should be able to issue signed revocation requests on behalf of end entities associated with it, whereas the end entity may not be able to do this itself, especially if access to the private key has been lost. This could be a use case to study, i.e., who and under what circumstances should/can sign the revocation request that will be accepted by the CA.

As part of the PNF/VNF/CNF lifecycle management procedures certificates associated with a decommissioned PNF/VNF/CNF should no longer be useable, therefore the decommissioning process must include a certificate revocation request to the issuing CA.

### Security Threats

**Mismanagement of revocation requests:** Ineffective handling or communication breakdowns regarding revocation requests could lead to compromised certificates remaining active. This allows for the potential misuse of compromised certificates, endangering secure communications and data integrity.

**Ineffective decommissioning:** If certificates of decommissioned PNF/VNF/CNF are not revoked effectively, they might be misused. This could lead to unauthorized activities, such as data breaches or network intrusions, under the guise of decommissioned entities.

**OCSP responder outages:** Dependency on OCSP responders for certificate validation could be risky in the event of outages. This could hinder the ability to validate certificate statuses, potentially disrupting secure communications.

**Compromised certificate continuance:** If a compromised certificate is not promptly revoked and announced, it may continue to be used maliciously. This could enable attackers to impersonate legitimate entities, decrypt secure communications, or inject malicious content.

**Incomplete revocation dissemination:** In some instances, revocation information may not be disseminated to all relevant entities in the network. This could lead to some entities continuing to trust a revoked certificate, posing security risks.

## Key issue #28: Risk of Service un-availability due to root CA Certificate updates for CNFs and VNFs

### General Description

CNFs and VNFs use certificates which are signed by intermediate or root CA certificates from operator’s choice of PKI.

A screenshot of a computer

Description automatically generated

Figure ‑: A possible system comprising different applications with different Root Certificates.

Figure 4‑1 gives a high level view of a possible system where different application groups of CNFs/VNFs may be using different root/sub-CA certificates for signing.

The root CA / sub-CA certificates used to sign certificates for CNFs and VNFs may need to be updated in the following scenarios:

* Root / sub CA certificate expiry
* Root/sub CA certificate revocation
* Operator deciding to change the CA for signing

In general, these scenarios can be referred to as a need for PKI migration. During the PKI migration procedure, all the certificates issued to CNFs / VNFs and signed by these root CA certificates need to be updated with new CA certificates. If such a PKI migration is needed during runtime, when system is already providing services:

* This can lead to slice / service un-availability
* Some CNFs can be handling UPF functionality
* Some CNFs can be handling various control plane functionalities
* If all CNFs/VNFs catering to a network slice use the same root CA, there is a risk of un-availability of the full slice.

Partial un-availability of services may still appear as network un-availability for end users.

### Security Threats

**Partial or complete service un-availability**: If intermediate or root CA certificates which are used to sign certificates for CNFs and/or VNFs need to be updated during runtime, it is likely to lead to partial or complete service un-availability.

**Network slice un-availability**: If all CNFs and/or VNFs of a particular network slice are impacted, it is likely to lead to unavailability of the network slice.

## Key issue #29: Certificate requirements for O-Cloud control plane

### General Description

The O-Cloud control plane acts as a pivotal component in managing and orchestrating cloud resources and services. Ensuring secure communications and operations within the control plane involves:

* Establishing a dedicated CA for the O-Cloud control plane to isolate and protect the certificate issuance and management processes specific to control plane components.
* Enforcing the use of TLS for all communications within the control plane components to ensure that data in transit is encrypted and authenticated, safeguarding it from unauthorized access and manipulation.

### Security Threats

**Cross-domain security breaches in unified CA environments**: In a multi-domain (plane) environment, a security breach in one domain might cascade to others, especially if a common CA is used for certificate issuance across all domains.

**CA Compromise:** If a CA is compromised, all certificates issued by it, across all domains, are potentially untrustworthy, leading to widespread network vulnerability.

**Policy misalignment in Shared CA Environments:** Shared CAs might necessitate generalized policies that may not align with the specific security and operational needs of the control plane.

## Key issue #30: Certificate management for cloud deployment models

### General Description

Addressing the intricacies of certificate management is pivotal, especially when considering varied O-Cloud deployment models, namely private cloud, community cloud, public cloud, and hybrid cloud. Each deployment model presents unique challenges and requirements in terms of certificate issuance, renewal, and revocation, which necessitates a tailored approach to ensure secure and efficient operations.

### Security Threats

**Unauthorized access in multi-tenancy environments:** Public clouds often involve multi-tenancy, where multiple users or entities share the same resources. If certificate management is not meticulously handled, one tenant might unintentionally gain access to another tenant’s data or services, leading to potential data leakage, unauthorized data manipulation, or other security incidents.

**Complexity in hybrid cloud certificate coordination:** Hybrid cloud models, which integrate both private and public cloud solutions, necessitate coordinated certificate management to ensure secure data transfer and communication between different environments. Failure to synchronize and securely manage certificates might expose data during transfer, making it susceptible to interception or alteration by malicious entities.

**Internal trust models:** Private clouds often operate on an internal trust model, where the CA is implicitly trusted by all entities within the organization.Mismanagement in this context can lead to internal threats, where malicious actors within the organization or compromised internal systems exploit the trust placed in the CA to conduct attacks, such as impersonating legitimate services or users.

**Lack of external audit:** Unlike public CAs, which are often subject to external audits due to their widespread use on the public internet, private CAs might not be subject to the same level of oversight. This lack of external audit can sometimes lead to lax practices or oversights going unnoticed and unaddressed, potentially increasing the risk of mismanagement.

## Key issue #31: Void

Void

## Key issue #32: Void

Void

## Key issue #33: Certificate Profiling in O-RAN

### General Description

A certificate profile is basically a template used to specify fields and form of a certificate. The profiles allow to configure a set of parameters, which support the security posture of the system as well as interoperability. 3GPP has specified in TS 33.310 [i.2] on the top of RFC5280 [i.13], several certificate profiles for types of network elements (e.g. Security Gateway (SEG), SBA, etc.), protocol (e.g. TLS entity), CA type (e.g. interconnection, SEG CA, etc.) and procedures (e.g. base station enrolment). This key issue intends to study specific O-RAN certificate profiling requirements across the main network functions of the O-RAN architecture in addition to those specified in RFC5280 and 3GPP, especially for elements and systems expressly defined in O-RAN (e.g. O-RU, Near-RT RIC, Non-RT RIC, etc.).

Common certificate security parameters are defined in O-RAN Security Protocol specification [i.41], such as hash algorithms, signature algorithms, minimum key lengths, etc. However, certain network functions, sub-systems or protocols used in O-RAN may require specific certificate profiles, including e.g., rules for validity periods, extensions (e.g. subjectAltName, keyUsage, etc.).

Once the certificate profiles have been defined for O-RAN, the CA(s) serving O-RAN architecture shall check that the requests are matching the pre-defined profiles, as well as the network elements of the O-RAN architecture shall accept only profiled certs for authentication and encryption purposes.

### Security Threats

**Inconsistent security posture:** Without standardized certificate profiles, different elements within the O-RAN system might employ varying security parameters, leading to inconsistencies in the security posture across the network and potentially creating weak links that can be exploited by attackers.

**Compromised encryption and authentication:** If certificate profiles are not rigorously defined and enforced, certificates that do not adhere to optimal security practices may be used, potentially compromising the encryption and authentication mechanisms within the O-RAN network.

**Misalignment with external standards:** If O-RAN-specific certificate profiles diverge significantly from established standards (e.g., RFC5280 [i.13], 3GPP TS 33.310 [i.2]), it may introduce complexities and challenges in ensuring alignment and compatibility with external systems and networks.

**Non-compliance with regulatory requirements:** Certificate profiles that do not align with regulatory or industry-specific requirements for cryptographic standards and data protection may expose the O-RAN network to legal and compliance risks.

**Vendor-specific vulnerabilities:** If certificate profiles are not standardized and are heavily influenced by vendor-specific implementations, it may introduce vulnerabilities specific to certain products or solutions within the O-RAN system.

## Key issue #34: Void

Void

## Key issue #35: Void

Void

## Key issue #36: Certificate sharing or not-sharing in Apps/VNFs/CNFs

### General Description

Sharing case: In the virtual environment, the NF is distributed in the virtual environment and there is no physical boundary for internal communication. If the private key has multiple copies, the risk of key disclosure is increased: transferring the private key faces communication attack, and, multiple copy or multiple access means one copy disclosure will pose a threat to all VMs/Containers using that certificate. Therefore, sharing private key and certificate should be actively discouraged unless carefully implemented.

Not sharing case: For this case, multiple certificates for one App/VNF/CNF brings some complexities for management:

* Complexity in operation and maintenance (e.g. complex to configure the mapping between certificates and VMs/Containers
* Complexity in updating/revoking a certificate. The CA/RA workload is increased
* Complexity to O-Cloud dynamic orchestration. Each time the VM/Container scales and/or migrates, the certificate is expected to be either initially applied or revoked. The application and revoke are network communication and will lead to time latency for the orchestration.

### Security Threats

***Threats from Sharing Certificates:***

**Widespread compromise:** A single compromise of a private key that is shared across multiple VMs/Containers can cascade into a network-wide security incident, affecting various applications and services. This could lead to unauthorized access, data breaches, and potential downtimes.

**Communication interception:** The transmission of private keys across the network can be intercepted by malicious actors, especially if the communication channels are not adequately secured. This interception can facilitate unauthorized access and data manipulation.

**Unauthorized access:** The availability of multiple copies of a private key increases the vectors through which unauthorized entities might gain access. Unauthorized access can lead to data breaches.

***Threats from Not Sharing Certificates:***

**Operational disruptions:** Managing multiple certificates for each App/VNF/CNF can introduce operational challenges, particularly in ensuring that each certificate is correctly configured and mapped. Misconfigurations or erroneous mappings can lead to service disruptions, inaccessible services, and potential non-compliance with regulatory standards.

**Delayed orchestration:** The necessity to apply or revoke certificates during scaling or migration operations introduces a latency that can impede the swift orchestration of services. This delay can impact the agility of the O-Cloud environment, affecting its ability to promptly scale, migrate, or recover services, which is crucial in maintaining service availability and reliability.

## Key issue #37: Lightweight solution

### General Description

The certificate management solution should be lightweight to support low resource devices and reduce the footprint and computational overhead associated with certificate management. Striking a balance between maintaining a robust, secure certificate management system and ensuring that it is not resource-intensive is pivotal to support various applications within the O-Cloud environment. Implementing a lightweight certificate management solution, while beneficial for low-resource applications, can introduce several security threats that need to be meticulously considered and mitigated.

### Security Threats

**Limited security protocols:** Using lightweight solutions may necessitate the use of simplified or less secure cryptographic algorithms and protocols. These might not be equipped to safeguard against advanced persistent threats or sophisticated cyber-attacks, thereby making the system susceptible to unauthorized access and data breaches.

**Inadequate revocation capabilities:** Efficient certificate revocation is crucial to prevent unauthorized access, especially in cases where a certificate is compromised. Lightweight solutions might struggle to promptly manage revocation processes, thereby extending the vulnerability window.

**Insufficient audit and logging**: Limited resources might restrict the ability to maintain comprehensive logs and audits, which are crucial for identifying and investigating security incidents and ensuring regulatory compliance.

## Key issue #38: Interoperability

### General Description

The key management solution should be specified in an unambiguous and well-defined manner to allow easy interoperability of implementations. If protocols are underspecified the O-RAN specification should add a profile that fills the gaps.

### Security Threats

**Inconsistent implementation across vendors:** Different vendors might interpret and implement certificate management protocols differently, leading to inconsistencies that could be exploited by malicious actors. This can lead to unauthorized access, data breaches, and disrupted communication between NFs in the O-RAN system.

**Inconsistent revocation handling:** Varied approaches to managing certificate revocations across implementations could result in the persistent use of revoked certificates within certain NFs of the O-RAN system. Consequently, this might allow malicious or compromised NFs to continue operating within the network, perpetuating ongoing security threats.

**Inadequate certificate authentication:** Divergent certificate validation methodologies across O-RAN NFs may result in suboptimal verification processes, paving the way for security compromises. Consequently, this may allow unauthorized access and potentially cause data leaks due to the acceptance of invalid or expired certificates.

## Key issue #39: Crypto agility

### General Description

The solution should be easy to extend with new crypto algorithms as the threat landscape changes (eg. post-quantum crypto).

### Security Threats

**Outdated algorithm exploitation:** Persistent use of outdated cryptographic algorithms may expose the O-RAN system to adversaries who have developed capabilities to exploit known vulnerabilities. The exploitation of outdated cryptographic methods could lead to unauthorized access, manipulation of sensitive data, and potential disruption in communication within the O-RAN system.

**Quantum computing threats:** The advent of quantum computing threatens the security of traditional cryptographic algorithms, which may become obsolete or insecure. The O-RAN system might be susceptible to breaches by quantum-enabled adversaries, leading to unauthorized access and potential data breaches, thereby compromising user privacy and operational data.

## Key issue #40: Void

Void

## Key Issue #41: CMPv2

### General Description

Certificate Management Protocol version 2 (CMPv2) is the most commonly supported and used protocol for certificate management in mobile networks. CMPv2 is specified by 3GPP and O-RAN Alliance WG4 for the M-Plane. The lack of specification for CMPv2 in the O-RAN Alliance’s Security Protocols Specifications allows a security gap and could impact vendor interoperability. It would be beneficial to the O-RAN community to update the Security Protocols Specifications to include CMPv2.

### Security Threats

**Inconsistent implementation and interoperability issues:** Without a standardized specification for CMPv2, different vendors might implement the protocol in slightly different ways. This inconsistency can lead to vulnerabilities if one vendor's implementation is less secure than another's, to interoperability issues, where systems from different vendors might not communicate seamlessly.

## Key Issue #42: Certificate management for Shared O-RU

### General Description

In a multi-operator shared O-RU environment, diverse certificate policies and practices among operators can lead to inconsistencies in certificate management, challenges in synchronizing updates, and complexities in establishing mutual trust, making coordinated and harmonized operations crucial for security and functionality.

### Security Threats

Different operators might have varying certificate policies, leading to potential inconsistencies in certificate issuance, renewal, and revocation.

Coordinating certificate issuance, renewal, and revocation across multiple operators for a shared O-RU can introduce complexities and potential inconsistencies.

If a certificate or security update is required for the shared O-RU, synchronizing and coordinating this across multiple operators can be challenging.

Ensuring that all operators trust each other's certificates and establishing mutual trust in a multi-operator environment can be complex.

## Key Issue #43: NF with an expired certificate

### General Description

Initializing an NF with an expired certificate in an O-RAN system not only risks operational disruptions due to failed secure connections with other network components but also heightens vulnerability to impersonation and man-in-the-middle attacks as attackers can exploit the invalid certificate, especially if network entities are lax in certificate validity checks.

### Security Threats

The NF might not be able to establish secure connections with other components of the network, leading to service disruptions. Other entities might reject connections from the NF due to its expired certificate.

Expired certificates can be a target for attackers. They might exploit the lack of a valid certificate to launch impersonation or man-in-the-middle attacks, especially if other components in the network aren't stringent about checking certificate validity.

# Solutions

## Solution #1: Automation of PSK/Refnum based Certificate Enrolment

### Description

Zero-touch based automation of PSK/Refnum based Certificate Enrolment can be considered, using robust key (re-) generation and secure key (re-)distribution techniques.

RFC 4210 [i.5] Section 4.2.2.2 Basic Authenticated Scheme talks about Initial Authentication Key (IAK) and reference value-based Certificate Enrolment. In this Technical Report, IAK is referred to as PSK (Pre-shared Key) and reference value is referred to as Refnum. In order to use this mechanism for initial certificate enrolment for CNF/VNFs in O-RAN, when any CNF / VNF is deployed in an O-Cloud environment, operator provisions and distributes a PSK-Refnum pair to each newly deployed CNF/VNF.

A Zero-touch automation of PSK/Refnum based Certificate Enrolment can be implemented by the operator, using robust key (re-)generation and secure key (re-)distribution techniques. From security point of view, ensure that the automated provisioning and distribution of PSK/Refnum is secure, and PSK/Refnum are provided only to authenticated and validated CNFs/VNFs. Such automations are implementation specific and follow relevant security mechanisms similar to those followed for distributing other system specific configurations.

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

The solution proposed here relies on operator’s implementation for automated provisioning and distribution of PSK/Refnum. The security mechanisms for such provisioning and distributions can be similar to other system specific configurations and no new standardization relevant aspects are proposed by this solution.

### Potential Security Requirements

Any automated PSK/Refnum generation and distribution systems implemented by the operator should ensure that no rogue CNF/VNF can obtain valid PSK/Refnum values.

## Solution #2: Study the use of BRSKI

### Description

Study the use of BRSKI instead of OR along with CMPv2. This solution partially addresses key issue #41.

In this study, the possible applicability and use of BRSKI in O-RAN for secure bootstrapping of new devices is described based on the understanding of RFC 8995 [i.28].

Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol provides a solution for secure “zero-touch (automated)” bootstrap of new (unconfigured) devices.

Following are important aspects to be considered for this.

* The architecture of BRSKI is relevant for “zero-touch” bootstrapping of devices which are “Drop-Shipped” from different vendors, and their ownership needs to be tracked.
  + Drop-Ship: The physical distribution of equipment containing the “factory default” configuration to a final destination. In zero-touch scenarios, there is no staging or pre-configuration during drop-ship. The “zero-touch” aspect is considered from this drop-shipping perspective.
    - As stated in RFC 8995 [i.28], BRSKI “is intended to scale to thousands of devices located in hostile environments, such as ISP-provided Customer Premises Equipment (CPE) devices that are drop-shipped to the end user. The situation where an order is fulfilled from a distributed warehouse from a common stock and shipped directly to the target location at the request of a domain owner is explicitly supported.”
    - From O-RAN architecture perspective, PNFs need to be deployed in the live network are not drop-shipped to the end user. PNFs are managed and owned by operators and do not have a separate domain owner or an end user.
    - Based on above understanding, from O-RAN architecture perspective, no equipment is considered for drop-shipping.
  + From wireless networks point of view, IoT devices may be considered for drop-shipping, however, in current architecture, these devices are not considered to be managed by the telecom network. Hence, using BRSKI for IoT devices can be considered as not applicable from O-RAN point of view.
  + RFC 8572 [i.31] describes Secure Zero Touch Provisioning as a bootstrapping strategy enabling devices to securely obtain bootstrapping data with no installer action beyond physical placement and connecting network and power cables. The techniques described in this RFC enable devices to establish secure NETCONF and/or RESTCONF connections with deployment-specific network management systems. This is more relevant for new PNF deployments which require to connect to the operator’s NMS using NETCONF connections. Hence, this RFC 8572 [i.31] can be more relevant for O-RAN and can be considered for live network deployments by operators.
* For devices that intend to become part of an ANI [i.RFC 8993 [i.29]] that includes an Autonomic Control Plane [i.RFC 8994 [i.30]], the BRSKI protocol MUST be implemented. The ACP is normally constructed on a hop-by-hop basis. Therefore, many interactions in the ANI are based on the ANI adjacency table.
  + Deployment of an O-RAN network does not require a hop-by-hop network construction using ACP. PNFs can be deployed independently and secure communications with PNFs can be established after initial certificate enrolment using CMPv2. Datacenters hosting CNFs/VNFs also do not require automatic hop-by-hop construction. Considering these aspects, it is understood that O-RAN does not consider any devices or equipment intending to become a part of the ANI, and hence does not mandatorily need usage of BRSKI.
* BRSKI terms new devices as “pledges” and these new devices communicate with a “registrar” for bootstrapping. Bootstrapping is complete when the cryptographic identity of the new key infrastructure is successfully deployed to the device. The established secure connection can be used to deploy a locally issued certificate to the device as well.
  + Using CMPv2 new NFs connect to Registration Authority (RA) for initial enrolment. After this initial enrolment, the NF gets Operator’s certificates which it can use for secure communications.
  + Conceptually, the logical flow is similar between CMPv2 and BRSKI. The main difference is with respect to the applicability of BRSKI which is for drop-shipped devices and is mandatory for any devices intending to become a part of the ANI.
  + CMPv2 based solutions, viz. solution #5 and solution #10 described in this TR provide the required support for initial certificate enrolment of newly deployed PNFs, and are sufficient to address the bootstrapping of PNFs.

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

Considering the study described above, usage of BRSKI is not applicable for any PNF/CNF/VNF used in O-RAN, specifically because BRSKI is relevant for drop-shipped devices intending to be part of ANI. From O-RAN point of view, none of the devices are drop-shipped and not considered to be part of ANI. BRSKI may be applicable for IoT devices, but these are not managed by telecom networks.

Also, there is no specific reason or requirement to replace CMPv2 with BRSKI. CMPv2 provides the required protocols for automated certificate management and there are no additional benefits seen by using BRSKI. Moreover, known techniques like SZTP [i.31] which are more relevant for O-RAN, enable non-technical personnel to bring up devices in remote locations without the need for an operator input.

Moreover, BRSKI is considered mandatory for networks deployed using ANI. However, none of the O-RAN components including PNFs and data-centers hosting the CNFs/VNFs require hop-by-hop construction using ACP. Therefore, BRSKI is not mandatory for O-RAN deployments.

### Potential Security Requirements

None.

## Solution #3: Study the use of EST

### Description

Enrolment over Secure Transport (EST) [i.32] defines a lightweight and straightforward protocol for managing certificate provisioning and enrolment in Public Key Infrastructure (PKI) environments. It focuses on certificate enrolment, and renewal while ensuring the security and integrity of the process by utilizing secure transport protocols like HTTPS. The EST service is located between a Certification Authority (CA) and a client.

The EST clients and server are both equipped with essential information to establish mutual authentication and authorization. The initialization data may consist of shared secrets, network service names, locations (e.g., Uniform Resource Identifier (URI) [i.39]), and trust anchor information. This data forms the foundation for secure communication and access control between the EST components.

This solution addresses Key issue 37 for defining a lightweight solution for certificate management using simple PKI message types as defined in RFC 7030 [i.32] over secured transport for certificate enrolment, and renewal. Revocation requests are supported via the /fullcmc interface using the Revocation Request Control defined in clause 6.11 of RFC 5272 [i.35]. This procedure allows certified end entities to make requests for the revocation of certificates. The retrieval of certificate revocation status can be performed using OCSP [i.26] and OCSP stapling [i.17].

EST Extensions as defined in RFC 8295[i.34] adds /crls interface to support CRL distribution. The /crls path component allows servers to distribute CRLs while clients retrieve their certificate(s) and CA certificate(s) as well as peer certificates. Client’s request CRLs with an HTTP GET [i.[38](https://datatracker.ietf.org/doc/html/rfc7231)], using an operation path of "/crls". "The CRL response and its handling follow the same procedures outlined in clause 4.1.3 of [i.32], with one or more CRLs returned in the CRL-only message.

#### Certificate-less TLS Authentication

The steps below document the initial enrolment procedure as per clause 3.3.3 of EST [i.RFC 7030 [i.32]]. Certificate-less Mutual Authentication defines a scenario where the client and server do not have certificates or trust anchors to perform mutual authentication. In such cases, TLS-SRP Transport Layer Security-Secure Remote Password (TLS-SRP) can be used, where username and password are pre-configured. TLS-SRP is based on zero-knowledge protocol which provides strong protection against password guessing and eavesdropping and is resistant to dictionary attacks.

The outlined message flow shows the EST Protocol for enrolment using https. The mutual authentication while establishing the https session is done using the TLS-SRP credentials.

1. Operator CA Server information (Example - FQDN/IP, Port, TLS-SRP username and password) is to be configured in NE.
2. TLS-SRP user credentials is created in the EST Server for enrolment requests.
3. TLS connection is established based on TLS-SRP [i.29].
4. NE initiates the EST CA Certification procedure to download the Operator CA (Root) certificates (or trust chain).
5. Server responds with a configured operator CA (Root) certificate in response to the CA Certification procedure request from a NE.
6. NE forms the Certificate Signing Request (CSR) and initiates EST simple enrolment procedure to download the Operator Device Certificate.
7. Server responds with a Device certificate signed by Operator CA in response to the simple enrolment request from an NE.

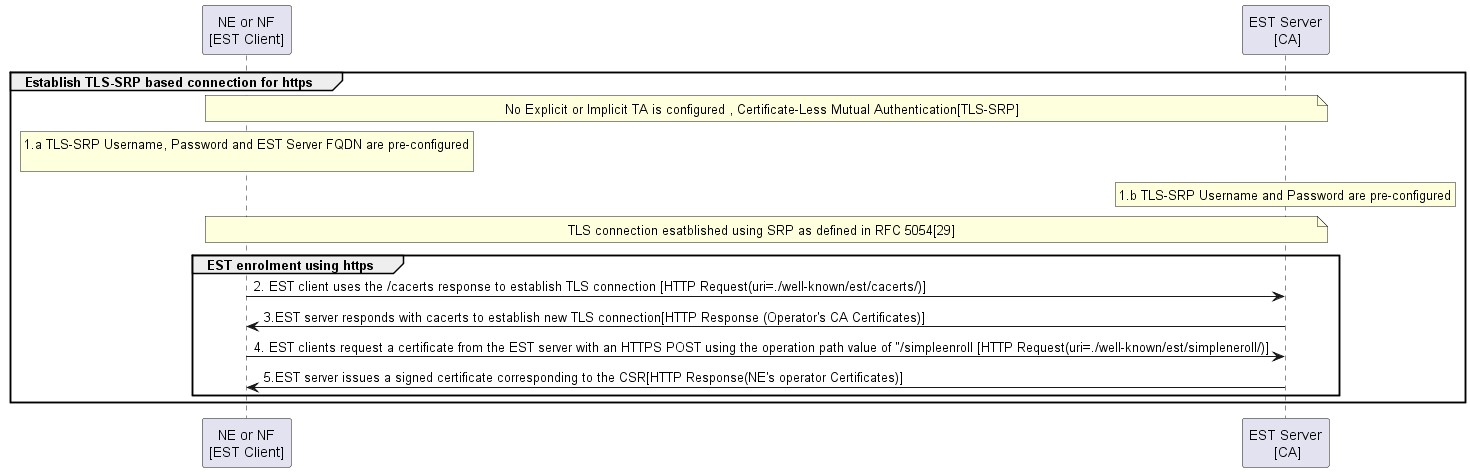


Figure 5‑1: Certificate-less TLS Authentication

#### Certificate TLS Authentication

The steps below document the initial enrolment procedure as per clause 3.3.1 of EST [i.RFC 7030 [i.32]]. The EST client authenticates the EST server using the certificate validation as defined in RFC 5280 [i.13]. The authorization method for the EST server depends on whether the EST Client is configured with an Explicit TA Database as per clause 3.6.1 of RFC 7030 [i.32] or an Implicit TA Database as per clause 3.6.2 of RFC 7030 [i.32]. In the below scenario, an explicit TA database has been configured for mutual authentication between EST Client and Server.

The outlined message flow shows the EST Protocol for enrolment using https. The mutual authentication while establishing https session is done using the certificates.

1. NE's Vendor certificate and Private Keys are pre-installed.
2. Vendor CA Certificate (or trust chain) is installed in the Operator CA server trust store.
3. NE has received the Operator CA server details (Example - FQDN/IP, Port, Operator CA certificate).
4. TLS connection is established based on the Explicit TA database.
5. NE forms the CSR and initiate EST simple enrolment procedure to download the Operator Device Certificate.
6. Server validates the client’s identity and responds with a Device certificate signed by Operator CA in response to the simple enrolment request from a NE.

A screenshot of a computer program

Description automatically generated

Figure 5‑2: Certificate-based TLS Authentication.

### Impacts on Existing Interfaces and Functionality

Impacts on Existing Interfaces and Functionality are FFS.

### Solution Evaluation

The choice for selecting a certificate management protocol could depend upon the PKI environment. EST provides a lightweight solution in case the environment does not govern a complex PKI infrastructure and features. The EST server authenticates and authorizes the EST client based on the method described in clause 4.3.1.1 and 4.3.1.2. The recommended method for establishing TLS secured http connection between EST client and server should be based on certificate based TLS authentication. EST could also be used between the client and RA and co-exist with CMPv2.

Benefits:

* Lightweight Protocol with simple PKI messaging types.
* Secured Transport using HTTPS.
* Source Code is open-sourced.
* Efficient and well-suited for edge deployments where the resources are constrained.
* Supports Elliptic Curve Cryptography.

Limitations:

* In scenarios where a client doesn't have proper configuration or trust anchors, manual intervention by a human user is required to verify CA certificate information.

### Potential Security Requirements

An O-RAN element that requires digital certificates should support the Enrolment over Secure Transport (EST) to securely provision RSA or ECC certificates over HTTPS, as described in RFC 7030. EST is a lightweight certificate management protocol that allows enrolment/renewal of digital certificates over a secured https and support all the below conditions.

1. An O-RAN element which has not been bootstrapped with digital certificates.
2. An O-RAN element using vendor certificates but missing trust anchor database or CA information not being passed by the DHCP options.

## Solution #4: Study the use of ACME

### Description

Study the use of ACME instead of OR along with CMPv2.

O-Cloud hosts O-RAN functions such as O-DU, O-CU, Near-RT RIC platform services, xApps, and O-Cloud control plane components. (e.g., Kubernetes control plane components).

The CMPv2 protocol can be used to provision certificates to O-DU, O-CU functions. However, for cloud-native applications (such as xApps), Near-RT RIC platform components, and O-Cloud control plane components deployed as pods, ACME offers a solution for automated certificate management.

Manually maintaining the certificates for cloud-native applications and O-Cloud control plane components present challenges:

* Large number of TLS certificates to manage across Kubernetes clusters and namespaces.
* Manually replace certificates every time when they expire.
* Certificates expire at different times; service outages may result if certificates are not renewed in time.
* Updating Kubernetes secrets manually is error-prone.
* Manual certificate management is time-consuming and error-prone.
* The risk-mitigating practice of rotate keys and certificates frequently aggravates the onerousness of manual certificate management.

#### Overview of ACME

ACME is a certificate management protocol defined in RFC 8555 [i.42]. A popular use of ACME is to request certificate from Let's Encrypt, a free public CA. The protocol is also supported by some commercial CAs.

The ACME builds on several existing technologies, most of which are commonly used in web API designs:

* HTTPS (transport)
* JSON (message format)
* TLS server authentication (authentication of messages from server)
* JWS (authentication of messages from clients)
* PKCS #10 (CSR)

ACME supports several certificate management use cases:

* requisition (a.k.a. enrolment)
* certificate revocation
* subject identifier validation

In ACME, a client needs to have an account to be able to use the service of an ACME server. A client account is identified with an account key pair. Among certificate enrolment protocols, ACME is unusual in that it has provisions for extensible, automated in-protocol processes for validating identifiers (e.g. DNS domain) of certificate subjects. This allows ACME accounts to be set up by clients without pre-established credentials, as a client's eligibility to receive a certificate with a particular subject identifier not based on trust of the client, but independent validation of the client's control of the subject identifier. RFC 8738 [i.43] extends ACME to issue certificates with IP address identifiers using http-01 and tls-alpn-01 challenges. Additional extensions and proposed extensions can be found at <https://datatracker.ietf.org/wg/acme/documents/>.

ACME has mechanisms for integrating with external systems. “External account binding” allows an ACME account to be tied to an account external (using a MAC-authenticated credential), and allows authorization to be performed via the external account. ACME also supports an operation called preauthorization, which allows a client to request authorization for a subject identifier outside of the context of a certificate request sequence.

In ACME, a certificate request sequence involves the creation and update of several types of objects:

* order
* authorization
* challenge

Messages from the client are authenticated using JWS signed with the client's account private key. To protect against replay attacks, requests from the client contain a replay-nonce. Some of the request-response exchanges are asynchronous in the general case. In those exchanges, after receiving an immediate response from the server, the client may need to poll the server periodically until a status change has occurred.

#### ACME Certificate Enrolment Flow

Issue challenge (e.g. http-01, dns-01)

Validate challenge

Provision resources to fulfill challenge

Submit order

Operator CA

Issue certificate

(Renew certificate before expiry )

ACME Server

ACME Client

Figure 5‑3: A simplified depiction of the workings of ACME

In ACME, message exchanges happen over HTTPS. The ACME specification defines a way of using an HTTP POST request to perform what an HTTP GET request usually does, but with JWS message authentication. The usage is called POST-as-GET in the protocol specification.

A typical certificate request sequence in ACME involves the follow steps:

1. **Order creation:** The client performs an HTTP POST to submit a request; the ACME server creates and returns an order object.
2. **Challenge retrieval:** The client uses POST-as-GET request(s) to retrieve the authorization objects referenced in the order object. In the general case, multiple authorization objects may be involved.
3. **Challenge fulfillment:** For each of the authorization object(s), the client selects one (of possibly multiple) challenge in the authorization object, takes action to fulfill the challenge, and POSTs to a URL to notify the ACME server of the challenge selected and it has been fulfilled.
4. **Challenge validation:** The ACME server verifies that the client has fulfilled the indicated challenges, e.g. by performing an HTTP request or a DNS query. This validation step may take a variable amount of time.
5. **Polling for status change:** The client performs POST-as-GET requests to check the status of the authorization object(s), until their status(es) are no longer “pending”.
6. **Order finalization:** The client POSTs to a URL contained in the order object, including a CSR in the request. There may be a variable amount of delay before the ACME server issues a certificate.
7. **Polling for status change:** The client performs POST-as-GET requests to check the status of the order object(s), until its status is “ready”.
8. **Certificate download:** The client performs a POST-as-GET to download a newly-issued certificate from a URL in the updated order object.

#### Integration with Kubernetes via cert-manager

cert-manager (name spelled in all lowercase) is an add-on to Kubernetes (K8s). As of August 2022, cert-manager is a CNCF project of maturity level “sandbox” (in a progression of three maturity levels: sandbox, incubating, and graduated.) cert-manager can generate key pairs and request certificates from CAs and provision the key pairs and certificates to containerized applications, in a Kubernetes construct called secrets. cert-manager can be integrated with CAs of several types. Using a built-in ACME client, cert-manager can request certificates from CAs that support an ACME interface. cert-manager can also monitor certificates it manages and automatically requests replacements for certificates before they expire.

#### Remarks

Compared with other certificate management protocols, ACME is rather “chatty” in that a typical certificate request sequence involves a relatively large number of request-response exchanges.

Although the pre-integration with ACME makes cert-manager an attractive certificate management option for containerized applications orchestrated using Kubernetes, private keys generated by cert-manager are only protected by access control. Private keys are exposed in plaintext form to anyone who has or managed to obtain privileged access (e.g., superuser access) inside a container.

### Impacts on Existing Interfaces and Functionality

Impacts on Existing Interfaces and Functionality are FFS.

### Solution Evaluation

Addressing Key Issue #37, ACME provides a solution for PKI certificate management protocol and procedures. In contrast to CMPv2, ACME is a dedicated protocol for certificate provisioning that is based on easy-to-implement REST interfaces and the HTTP protocol. It is therefore easier to implement in resource-restricted client implementations as well as in the certificate authority (trust center). CMPv2, however, is a very complex binary (ASN1-based) protocol with a feature set that well exceeds what is needed for certificate provisioning.

Addressing Key Issue #38, ACME provides a solution for PKI certificate management protocol and procedures. Because of its dedication to certificate provisioning and the use of RESTful APIs it is easier to understand for developers leading potentially to a better conformance and therefore higher interoperability of ACME implementations. For CMPv2, however, variances in implementations may lead to more interoperability problems due its higher complexity and the need to observe a large number of specifications with regard to its deployment in an O-RAN context (ie. original RFCs, 3GPP profiles, potentially O-RAN Alliance profiles).

## Solution #5: Initial Certificate Enrolment of PNFs using vendor certificates

### Description

This solution addresses Key Issue #3 and Key Issue #4.

When a new physical network function (PNF) gets deployed in a network, it can obtain operator’s CA signed certificate in order to establish secure communications with other network functions. An operator may prefer using vendor-signed certificates for automated initial certificate enrolment. This solution proposes the procedure to use vendor-signed certificates for initial certificate enrolment of PNFs. This solution proposal refers to vendor certificate-based initial registration and certificate enrolment as described in 3GPP TS 33.310 [i.2] clause 9 “Certificate enrolment for base stations”.

The solution is summarized as below:

Pre-conditions:

When a PNF is deployed in the network, for initial certificate enrolment, it requires vendor-signed certificate and the related private key, and operator’s CA certificate.

* Also, PNF needs to be configured with the URL/IP address for RA/CA.
  + As described in 3GPP TS 28.315 [i.44] clause 5.3, operators may deploy their management infrastructure in a manner that either IP address or FQDN of RA/CA is known to the PNF.
  + The plug-and-connect concepts as described in 3GPP TS 28.314 [i.45] and 3GPP TS 28.315 [i.44] should be followed.
* CA/RA has the vendor’s root certificate pre-provisioned.
  + 3GPP TS 28.314 [i.45] clause 4.1.3.1 should be followed for root certificate acquisition.
  + RA is an optional entity, and the registration function can be directly implemented with the CA component. RFC 4210 [i.5] (for CMPv2) describes possible reasons for the presence of RA in Appendix A of the RFC.

Initial Certificate Enrolment:

* 3GPP TS 33.310 [i.2] Annex G presents an example CMPv2 message flow for initial enrolment, and this should be followed.
* When PNFs have connectivity with CA/RA, and above pre-conditions are satisfied, vendor-signed certificate gets used to perform initial certificate enrolment.
* PNF presents the vendor-signed certificate to CA/RA during CMPv2: Initialization Request. CA/RA having vendor’s root certificate can authenticate this request and, the CMPv2 protocol can be followed, as defined in RFC 4210 [i.5], to establish the trust.

This trust establishment allows newly deployed PNFs to obtain operator CA issued certificate along with the chain of trust.

### Impacts on Existing Interfaces and Functionality

An O-RAN PNF requiring a PKI certificate will need to support CMPv2 and will need a pre-installed vendor certificate. Offline interfaces will be required to configure the URL/IP address of the RA/CA in the PNF.

Offline interfaces will also be required to pre-provision vendor’s trust anchor in RA/CA.

Pre-condition: In order to facilitate vendor certificate-based initial enrolment of PNFs, vendor’s trust anchor is pre-installed in operator’s RA/CA.

### Solution Evaluation

This solution addresses Key Issue #3 and Key Issue #4.

### Potential Security Requirements

In order to facilitate vendor certificate-based initial enrolment of PNFs, vendors should pre-install vendor-signed certificates in PNFs.

In order to facilitate vendor certificate-based initial enrolment of PNFs, operators should pre-configure the FQDN/IP address of RA/CA in PNFs.

## Solution #6: Certificate management and secure storage of Application private keys within O-Cloud

### Description

The O-Cloud platform should have a certificate manager (e.g., "cert-manager" for Kubernetes [i.https://cert-manager.io]) that supports secure protocols such as ACME and (CMPv2 is not yet implemented), which can be used to obtain certificates from other sources. This certificate manager is used to inject certificates in O-RAN Applications. In order to do that, the certificate manager should use a trusted CA to sign the certificate request.

ACME or CMPv2 protocols support the integration with a PKI-as-a-Service to obtain certificates from any PKI, whether public or private, that support security modules like HSMs. This enables secure, automatic issuance of a unique, trusted identity certificate for every application and O-Cloud component.

Certificates and private keys should be stored within the O-Cloud platform as secrets (e.g., native k8s Secrets Objects). Private keys should be protected in terms of confidentiality and integrity.

### Generation of key pair and modes of operation

The ETSI GR NFV-SEC 005 [i.11] clause 8 is describing the key-generation and distribution for NFV certificate lifecycle management, specifically three different concepts are shown.

In this clause the different key-generation concepts have been taken as basis for further development of the key-generation and certificate enrolment.

The following Figure **5**‑**4** is depicting the system level view for the secure storage and certificate management.

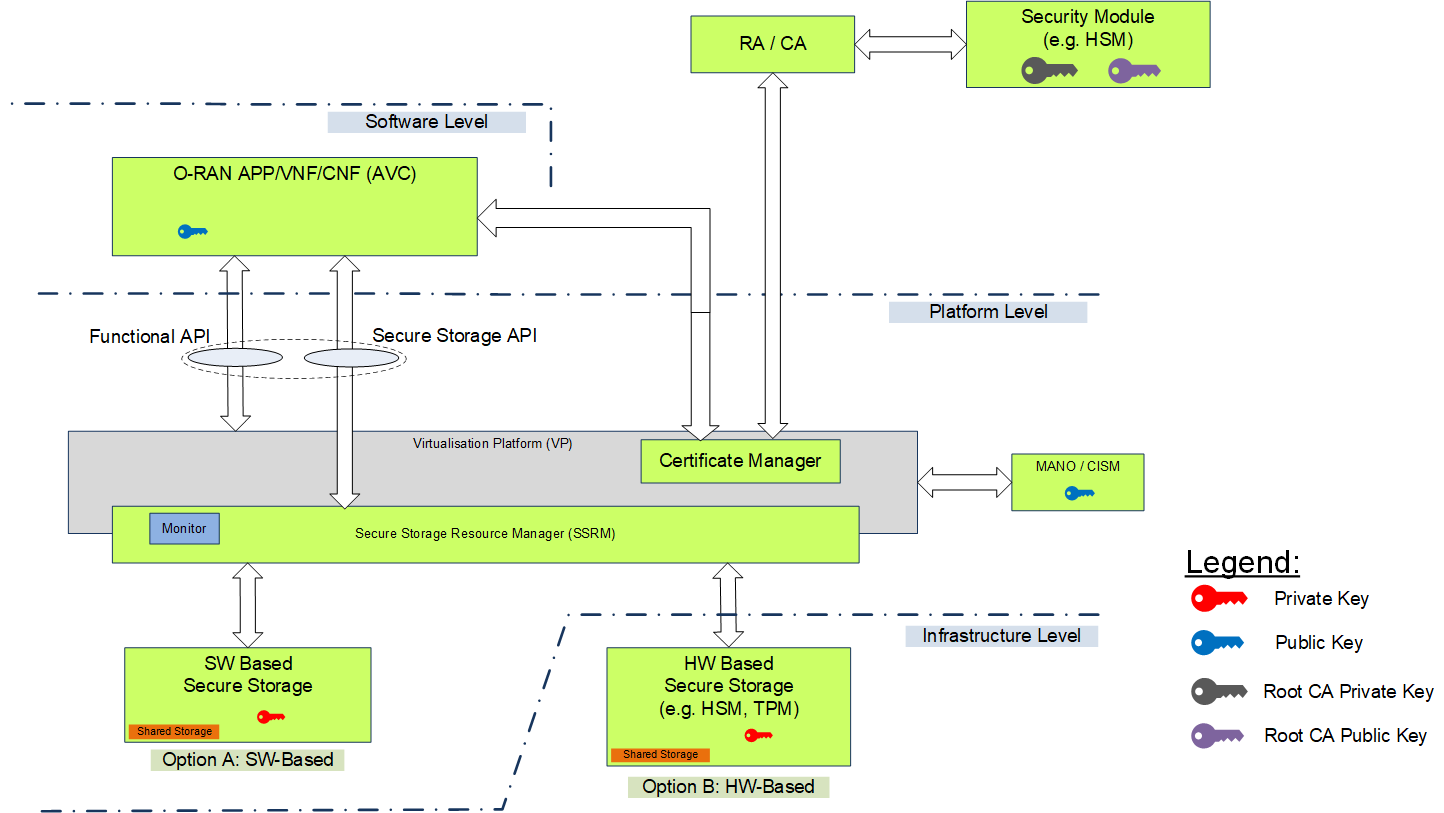


Figure 5‑4: Secure Storage and Certificate Management Architecture (System Level View)

The following is applicable:

* The Virtualisation Platform (VP) includes the Secure Storage Resource Manager (SSRM). The SSRM is managing the interface to either the SW based or HW based secure storage solution. The VM/Container is owning a more ‘internal’ interface to SSRM (which is like a primitive between protocol stacks). The SSRM is providing service for key-pair generation and provision of the public key, is providing digital signatures, is providing key-management, etc.
* The underlying HW based secure storage can be either implemented by a TPM device (HW or SW) or can be by a (physically) connected HSM module.
* Any Application or certificate manager have access to SSRM service.
* The management and orchestration system (e.g., MANO for VM [i.11], CIS/CISM for Container [i.12]) is receiving the operator public key on request for distribution to other Applications.
* The Operator RA/CA has connected its own HSM module which is creating the private key for signing requests.

#### Generation of the key pair by the Virtualization Platform

In this mode, the key pair is generated by the SSRM following the request of the certificate manager. The certificate manager could automatically ensure certificates are valid and up to date and attempt to renew certificates at a configured time before expiry.

The following steps are followed to request and store certificates:

1. An Application creates and sends a certificate resource request to the certificate manager
2. The certificate manager requests from the SSRM the generation of a key pair and sends a Certificate Signing Request (CSR) to the CA
3. The CA signs the certificate with its own private key and returns it to the certificate manager.
4. The certificate manager stores the signed certificate in the secret storage volume with the O-Cloud platform (e.g., in etcd).
5. Authenticated and authorized Application can read the signed certificate from the secret storage volume for use and for digital signing service is (direct) requesting digital signature from the SSRM by providing the digest for signing.

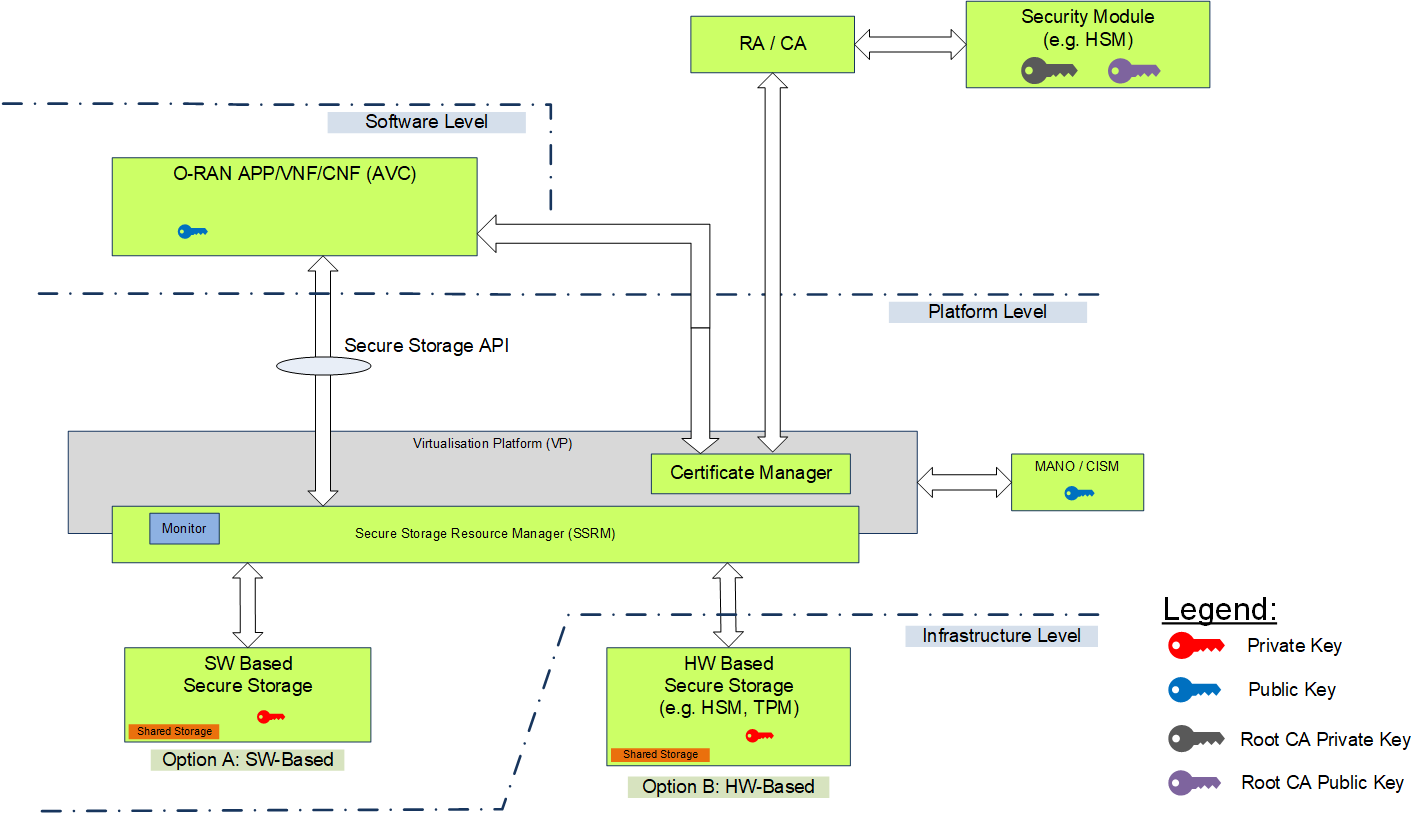


Figure 5‑5: Key-generation by the Virtualisation Platform

#### Generation of the key pair by Trusted Application

In this mode, the key pair is generated by the Trusted (i.e., authenticated, and authorized) Application. In this mode, the life cycle of the certificate is to be managed by the Application and it is the responsibility of the Application to renew the certificates before they expire.

The following steps are followed to request and store certificates:

1. Trusted Application generates a key pair.
2. The Trusted Application sends the public key back to the certificate manager. The certificate manager sends the CSR to the CA for signing.
3. The CA signs the certificate with its own private key and returns it to the certificate manager.
4. The certificate manager returns the signed certificate.
5. The trusted Application requests the SSRM to store its private key with the signed certificate in the secure storage.

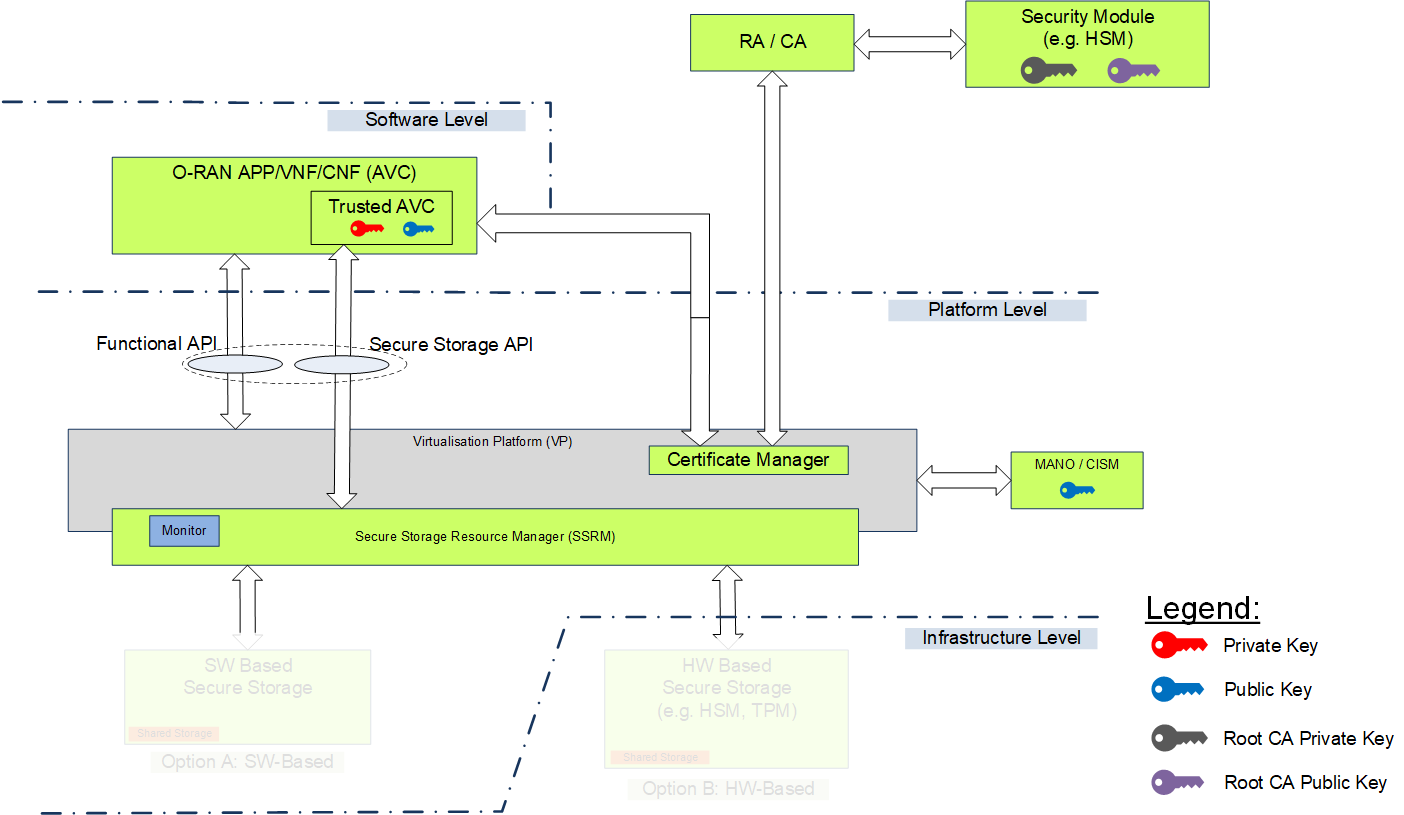


Figure 5‑6: Key-generation by the Trusted Application

#### Generation of the key pair by a HW security module (e.g., HSM, TPM)

In this mode, the key pair is generated by the connected HW security module (e.g., HSM, TPM). The security module is connected to the virtualization platform via the SSRM, which is then used for generation of a key pair.

In this mode, the life cycle of the certificate is to be managed by the Application and it is the responsibility of the Application to renew the certificates before they expire.

The following steps are followed to request and store certificates:

1. An Application creates and sends a certificate resource request to the certificate manager
2. The certificate manager is creating a key-pair generation request to the security module. The security module is creating the key-pair and is sending the public key back to the certificate manager. The certificate manager sends the CSR to the CA for signing.
3. The CA signs the certificate with its own private key and returns it to the certificate manager.
4. The certificate manager returns the signed certificate.
5. The security module stores the private key, and the signed certificate is going to the Application.

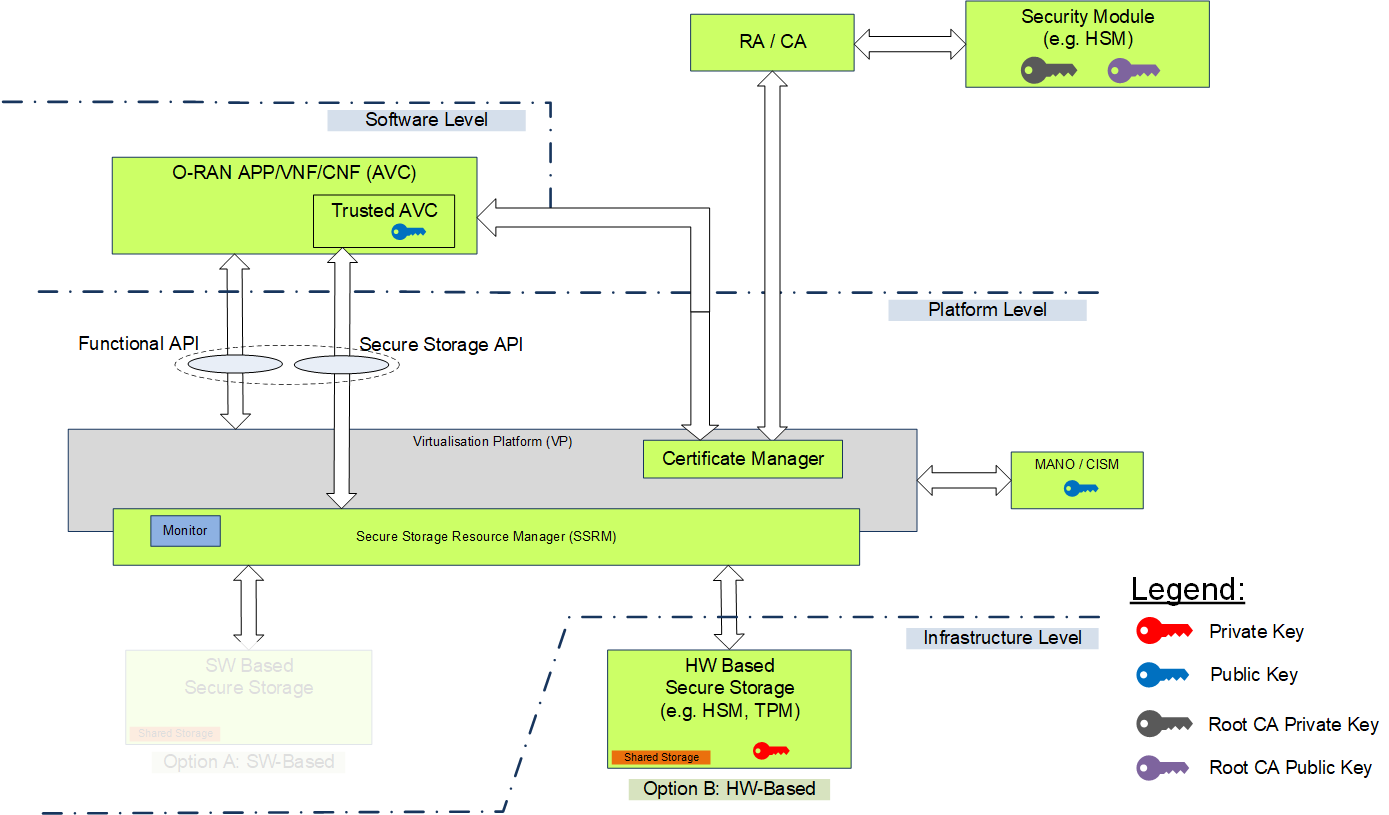


Figure 5‑7: Key-generation by the Secure Module (e.g., HSM, TPM)

### Secure key and file storage

Encryption/decryption functionality is provided by the management platform and handled by the CPU’s accelerated instruction, providing accelerated data at rest for both AES encryption and decryption. The main assets involved in the encryption/decryption of private keys are the key encryption key (KEK), the disk encryption key (DEK) and/or the secret encryption key (SEK). Different solutions for protecting those keys in terms of integrity and confidentiality are currently used. Such potential solutions include:

#### Secure Key and File Storage Mechanisms – Architecture Framework

The main purpose for implementing a secure storage is to guarantee the secrecy of a private key (asymmetric cryptography) and/or of a file which might hold sensitive information. The secure storage in this context is a composition of sub-functions which all together are required to provide service to upper layer for a proper secure key and file protection.

The following Figure **5**‑**8** depicts the overall architecture framework for a secure key and file storage.

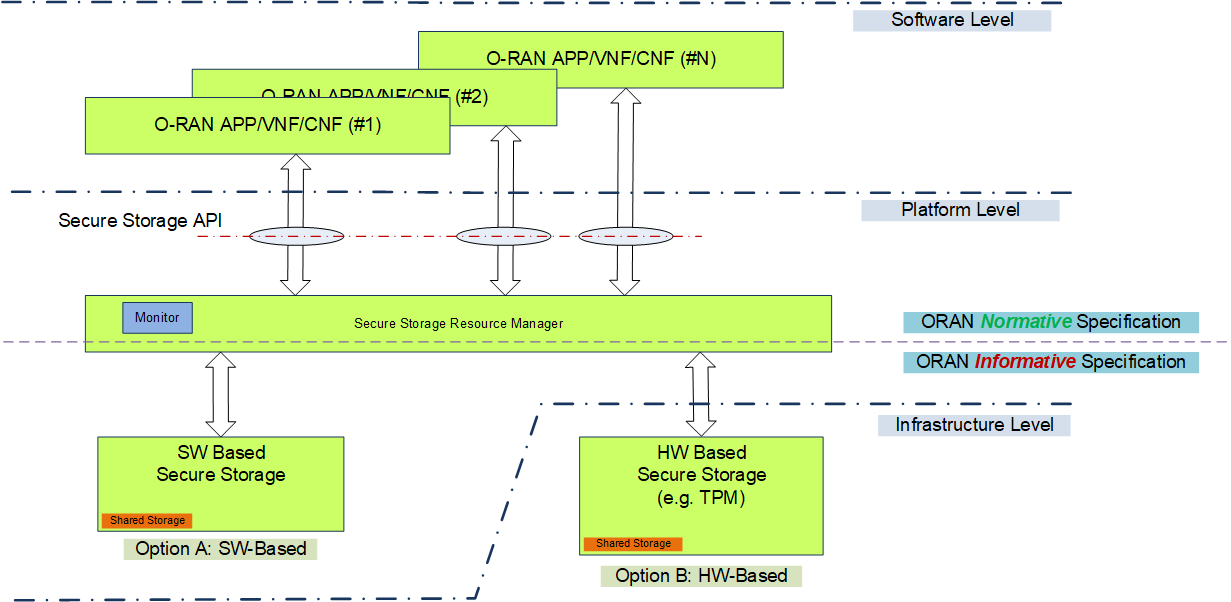


Figure 5‑8: Secure Key and File Storage Architecture Framework (overview)

The SSRM is providing service to any application, i.e., is creating private-public key pair, is providing digital signing requests on received digests, is returning the digital certificates, etc. Any application is connecting to SSRM via a standardised Secure Storage API (SSAPI). This API is independent of the underlying secure storage mechanism. The storage mechanism can be built up by a single secure storage instance or by multiple secure storage instances. Their management is up to the SSRM.

The following is applicable:

* The O-RAN Application is interfaced to the Secure Storage Resource Manager (SSRM) via a Secure Storage API.
* The role of the SSRM is to provide service on secure storage to any Application, and to hide the underlying protection mechanism which can be either SW-based and/or HW-based. The Monitor function belongs to the SSRM and is for tracking purposes or could be used as proxy towards the system O&M.
* The secure storage mechanism could be a SW based approach (e.g., vTPM) and/or HW-based (e.g., TPM, HSM).
* The HW-based solution option is impacting the HW and therefore is belonging to Infrastructure. The SSRM (including the SS API) and the SW-based solution option is belonging to the Platform. The O-RAN Application is belonging to the application SW level.

#### Scenarios for protecting keys within the secret storage volume

##### Use of TPM (Hardware TPM or vTPM)

In this solution, two scenarios are possible, among others:

1. Scenario 1: Private keys are not encrypted individually. All private keys are stored in a disk encrypted by the DEK. DEK is stored in a TPM for automatic decryption at boot.
2. Scenario 2: Private keys could by encrypted individually by SEKs. SEKs are stored in a disk encrypted by the KEK. KEK is stored in a TPM.





Figure 5‑9: Scenarios for protecting keys within the secret storage volume based on TPM

##### Use of KMS server

There is a specific SEK for each private key. The SEK is used to encrypt the private key and is itself encrypted by the KMS server’s KEK. The KMS server may use an HSM for the storage of the KEK and the encryption of SEKs. The HSM if used by the KMS server may or may not be the same as the HSM used by the CA.



Figure 5‑10: Key protection based on KMS

### Impacts on Existing Interfaces and Functionality

Solution #6, focusing on the implementation of certificate management and secure storage of application private keys within the O-Cloud, substantially impacts the O-Cloud architecture by elevating its security framework. The O-Cloud should incorporate the following components and mechanisms:

The O-Cloud should support a certificate manager for the automated handling of digital certificate lifecycle processes, including the generation, issuance, renewal, and revocation of certificates. This certificate manager should be capable of integrating with various Certificate Authorities (CAs) and support secure protocols such as ACME, CMPv2, etc., for seamless certificate procurement. It must be designed to facilitate secure, automatic issuance of unique, trusted identity certificates for every application and component within the O-Cloud.

The O-Cloud should support secure storage and deletion mechanisms for protecting private keys during their entire lifecycle. This involves several critical components and processes:

1. Secure key generation: Private keys should be generated in a secure environment, possibly using HSMs or TPMs, to ensure that they are never exposed to less secure environments or unauthorized entity.
2. Encrypted storage: Once generated, private keys should be stored in encrypted form. The encryption should be strong enough to prevent unauthorized access.
3. Access control: Strict access controls should be implemented to ensure that only authorized applications can access the private keys.
4. Regular updates and renewal: The O-Cloud should support automated renewal and update processes for keys and certificates, ensuring that they are replaced or updated before they expire or become vulnerable due to advancements in cryptographic attacks or if there is a need to change the CA signing the certificates for Applications. Also, during any such updates, it should be ensured that there is no service interruption.
5. Secure deletion: When a private key is no longer needed, it should be securely deleted. Secure deletion ensures that the key is irrecoverable, preventing any possibility of unauthorized use. This can be achieved through techniques like cryptographic erasure, where the key is made inaccessible by destroying the encryption key used to encrypt the private key.
6. Backup: While maintaining the security of private keys, the O-Cloud should also support secure backup. These backups should be encrypted and stored securely.

### Solution Evaluation

This solution addresses Key Issue #20.

### Potential Security Requirements

In addition to the existing security requirements in Clause 5.1.8.6 of [i.47] focused on the secure storage and deletion of sensitive data within the O-Cloud platform, the following potential security requirements are proposed to ensure secure handling of private keys and certificates within the O-Cloud:

* The O-Cloud should provide mechanisms for managing the entire lifecycle of digital certificates, including (re-)issuance, renewal, revocation, and expiration.
* The O-Cloud should support automated renewal processes for certificates to avoid service interruptions due to expired/revoked certificates or during any PKI migration (change in CAs used for signing Application certificates).
* The O-Cloud should support integration with trusted CAs for the issuance of certificates.
* The O-Cloud should support for various certificate management protocols like CMPv2 and ACME.
* The O-Cloud should implement secure and robust mechanisms for the generation of cryptographic keys. This includes using high-entropy sources for randomness and adhering to industry-standard cryptographic algorithms such as NIST SP 800-133 [i.48] and SOG-IS [i.49], ensuring the keys are of sufficient strength and quality.
* The O-Cloud should raise alarms and/or notifications if the secure storage space has exceeded the configured limits and more data cannot be stored.

## Solution #7: CMPv2

### Description

CMPv2 is described in RFC 4210 [i.5].

### Impacts on Existing Interfaces and Functionality

An O-RAN PNF, VNF, or CNF requiring a PKI certificate will need to support CMPv2.

### Solution Evaluation

Current O-RAN specifications require CMPv2 for the management of the O-RU [i.10].

CMPv2 provides a solution for PKI certificate management protocol and procedures.

CMPv2 provides the following functionality for O-RAN certificate management.

* CMPv2 supports automatic certificate enrolment, rekey, and renewal procedures.
* CMPv2 provides built-in integrity protection and authentication.
* CMPv2 provides revocation support for VNFs and CNFs with the operation of Revocation Request/Response, Revocation Announcement and CRL Announcement. This support allows for an authorized orchestrator to revoke a certificate for a VNF or CNF before it is removed.
* It is not recommended to have CMPv2 provide revocation support for a PNF for the following reasons:
  + Most Certificate Policies require a human review and authorization of revocation request due to the severity of consequences.
  + The revocation requests are typically submitted by humans rather than machines that own the certificates. Once a PNF is compromised, it cannot be relied upon to request revocation for its own certificate and other elements in a domain may not be able to make practical use of an automated CMPv2 revocation messaging.
  + Human operators may mistake an unapproved revocation request with an actual act of revocation and take pre-mature actions.
  + CRLs are better provided by CRL servers (either LDAP or HTTP access as stated in clause 6.1.1 of the 3GPP TS 33.310[i.2]) that simply act as web-servers with no trust authority. This provides much better scalability properties than an RA/CA responding to high volume of CMP requests for CRLs.
* An O-RAN PNF, VNF, or CNF can use CMPv2 protocol or out-of-band procedures to register at the CA/RA.
* An O-RAN PNF, VNF, or CNF can use CMPv2 protocol to initiate the certificate request to the CA/RA, and receive the certificate from the CA/RA in a secure and automated procedure.
* An O-RAN PNF, VNF, or CNF can use CMPv2 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.

### Potential Security Requirements

Potential security requirements:

* An O-RAN PNF, VNF or CNF requiring a PKI certificate should support CMPv2 as defined in RFC-4210 [i.5].
* An O-RAN PNF, VNF, or CNF supporting CMPv2 should have the URL, FQDN, and/or IP address for the RA/CA pre-configured or configurable. The RA/CA are defined in RFC-4210 [i.5]. For an instance of a PNF being configurable, an O-RAN PNF can be configured with the IP address or FQDN of one or more Certification Authority (CA/RA) servers using DHCP Option 43 as specified in clause 4.2.2 of 3GPP TS 32.509 [i.8].
* An O-RAN PNF, VNF, or CNF supporting CMPv2 should raise notification and/or alarm if any polling request (as defined in RFC-4210 [5] clause 5.3.22) sent to CMPv2 server fails.
* CRL servers (either LDAP or HTTP access as stated in clause 6.1.1 of the 3GPP TS 33.310[2]) should be used to check the revocation status of certificates.
  + If the check for revocation status fails for any reason, e.g., connectivity to CRL server fails, or DNS resolution of CRL server fails, then an alarm should be raised to enable operator to take appropriate actions.
* Details of any revoked certificate should be updated in CRL servers by the operator’s PKI.
  + If, for some reason, this update fails, alarm and/or notifications should be raised to notify the operator.

## Solution #8: Vendor Root CA Certificate Renewal notification

### Description

The PNFs using vendor-signed certificates for initial certificate enrolment shall raise a notification when vendor root CA certificate is about to expire in x days. The notifications are raised with severity increasing closer to expiration: As an example:

* WARNING when the certificate expires within the threshold
* MINOR when the certificate expires within 1/3 of the threshold
* MAJOR when the certificate expires within 1/6 of the threshold
* CRITICAL when the certificate expires within 1/30 of the threshold or 3 days, whichever is largest. This severity is used also after certificate expiration.

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

In many deployments, the validity periods of vendor root CA certificates are very long. Moreover, once a PNF is enrolled using vendor-signed certificates, the need for using vendor root CA certificates for authenticating PNFs is very rarely required. Such a scenario may only be necessary if a PNF deployed many years ago requires a factory recovery for some reason and is intended to be used as a fresh deployment after vendor root CA certificate expires.

This solution proposes notifications (alarms) to be raised with increasing levels of severity as the expiry date of vendor root CA certificate approaches. Operators need to keep track of such notifications and ensure timely updates of vendor certificates if necessary in order to ensure no impacts on system availability.

### Potential Security Requirements

It is recommended that PNFs which use vendor-signed certificates for initial certificate enrolment monitor the expiry of the root CA certificate used to sign the certificate. When the expiry of the vendor root CA certificate is approaching, PNFs can raise notifications (alarms) with increasing levels of severity as the expiry date gets closer.

## Solution #9: Mitigating the risk of system overload due to bulk certificate updates

### Description

This solution proposes an optional Certificate Update Orchestrator (CUO), which monitors various possible triggers for certificate updates, and orchestrates the certificate updates in a staggered manner in order to prevent potential service outage during simultaneous certificate updates for a large number of NFs (PNFs/CNFs/VNFs). Operators may implement such an orchestrator in their datacenters where NFs are hosted. In some implementations, this may be implemented as an application running in the datacenter where SMO is hosted, or in the O-Cloud.

Figure **5**‑**11** illustrates a possible implementation of CUO, showing the interfaces it may use. Implementations of CUO may vary, but this application should include the following functionalities in order to mitigate the risks detailed in Key Issue #13.

* CUO schedules the required certificate updates in various network functions (physical as well as virtual) in a staggered manner.
  + The schedule can be derived in a manner that services or functions related to neighboring cells do not update the certificates simultaneously. This can ensure that the connected UEs will have at least one RL, and end-user service experience is not degraded due to any certificate updates.
  + Time of initiation of certificate update in every network function can be planned and executed according to this schedule
* CUO monitors and predicts the time required for updating certificates in various network functions
  + it maintains an internal database where the past records of time taken for certificate updates are stored
  + this database can be used in order to train ML algorithms for predicting the time required for updating certificates
* CUO also monitors and predicts the need for certificate renewals due to expiry, as well as updates due to revocation
* CUO coordinates with SON/RIC in order to increase the coverage of neighboring cells when certificate updates are performed on a specific cell. This can ensure zero impacts on end-user service experience during certificate updates.
* CUO monitors the network performance parameters during the certificate update procedure executions, and reinforces the analytics to derive continuously enhanced scheduling for certificate updates
* CUO monitors the network performance parameters and considers lower network traffic for initiating and scheduling certificate update procedures.

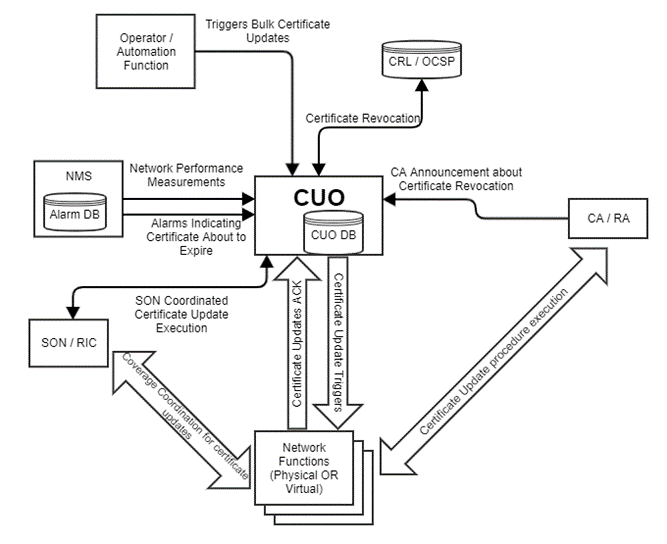


Figure 5‑11: Certificate Update Orchestrator

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

This solution provides details of possible implementations which can help operators ensure that automated certificate management does not lead to un-intentional service outages in the live network. Such applications can be implemented by the operator and deployed in datacenters hosting the SMO, or in the O-Cloud, enabling easy access of data required for certificate update orchestration.

Any automated certificate management system would benefit from avoiding simultaneous certificate updates for several network entities. This can be followed as a guideline.

### Potential Security Requirements

None.

## Solution #10: Usage of PSK/Refnum for Initial Certificate Enrolment for PNFs

### Description

This solution addresses key issue #2 of this TR. As described in RFC 4210 [i.5] Section 4.2.2.2 Basic Authenticated Scheme, Initial Authentication Key (IAK) and reference value can be used for initial certificate enrolment using CMPv2. In this document, IAK is referred to as PSK (Pre-shared Key) and reference value is referred to as Refnum.

For PNFs, operators and vendors need to establish offline (out-of-band) secure methods in order to pre-provision PSK and Refnum values in PNFs which are planned to be newly deployed. The out-of-band methods may be automated, and clause 4.1 of this Technical Report can be referenced for any such automation.

* PSK is used to sign the CMPv2 certification request, which is the first message sent from the PNF after initial deployment in the live network. PNF sends this request to operator’s PKI using pre-configured network details of operator’s PKI.
* The integrity of CMPv2 certification request is verified by the operator’s PKI using the PSK. Also, operator’s PKI verifies proof of possession of Refnum value which is included in the certification request.
* After successful verification of CMPv2 certification request, as per previous step, subsequent procedure is followed according to RFC 4210 Section 4.2.2.2 Basic Authenticated Scheme.
* Upon successful completion of PSK/Refnum based initial enrolment, the newly deployed PNF receives the operator’s CA signed certificate, which is used for all subsequent establishment of secure connections with operator’s PKI.
  + PSK/Refnum values should not be used for any communications after initial enrolment.
  + If a factory recovery is required, new PSK/Refnum values should be provisioned by the operator.

### Impacts on Existing Interfaces and Functionality

No new impacts identified by this solution.

### Solution Evaluation

This solution ensures backward compatibility for PNFs using PSK/Refnum based initial certificate enrolment.

### Potential Security Requirements

Any offline or out-of-band PSK/Refnum generation and distribution systems implemented by the operator should ensure that no rogue PNF can obtain valid PSK/Refnum values.

## Solution #11: Certificate renewal procedure

### Description

There are two possible scenarios when certificate renewal is required for any network function in O-RAN:

1. Certificate is about to expire in near future
2. NF is initialized but has an already expired certificate.

#### Certificate is about to expire in near future

As mentioned in key issue #42, in order to ensure that there is no service un-availability due to certificate expiry, certificates should be automatically renewed with sufficient time before expiry.

This solution proposes the following:

* Operators can define a certificate renewal strategy, which could depend on the number of days to expiry or depending upon the alarm severity. Operators may also want to define a strategy for staggered certificate renewals.
* When any certificate is about to expire in the near future, associated NF (PNF/CNF/VNF) sends alarms to NMS.
  + There can be multiple alarms with different severity. For example, if a certificate is about to expire on 30th day a Minor alarm is raised, if a certificate is about to expire on 15th day a Major alarm is raised, and when there are less than 5 days remaining for the certificate expiry a Critical alarm is raised.
  + NOTE that when a higher severity alarm is raised for the same certificate expiry, the lower severity alarm should be automatically cleared.
* Automated certificate management system monitors these alarms and schedules certificate updates using CMPv2 protocol.

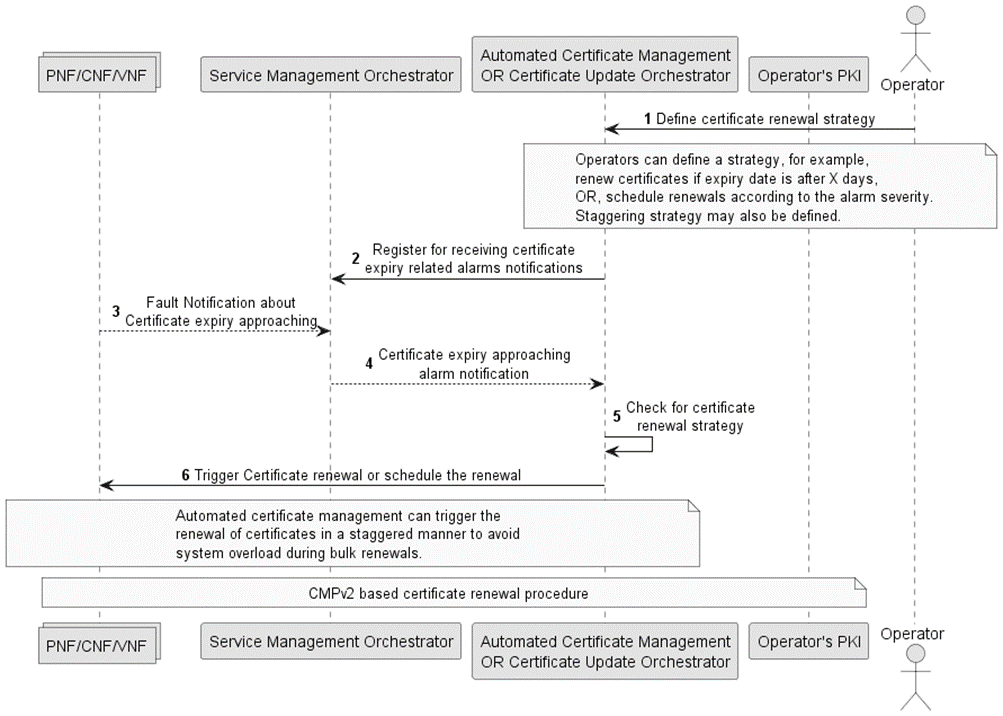


Figure ‑: Certificate renewal procedure

#### NF is initialized but has an already expired certificate

If any NF is already initialized but has an expired certificate, it will fail to establish any secure connections. In this scenario, a Critical alarm should be raised frequently for the same until the certificate gets renewed. For example, one critical alarm can be raised per day and it can trigger the operator to obtain a new certificate sooner. The provisioning of updated certificates needs to be done offline. Until such time that the NF gets a renewed certificate, the NF should not be allowed to establish connection to the network.

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

This solution addresses Key Issue #42.

### Potential Security Requirements

Network management system should provide alarms/notifications to automated certificate management systems alerting about the certificates about to expire in the near future.

Automated certificate management system should monitor the expiry time of certificates used by all network functions and ensure that the certificates are renewed automatically before the expiry.

If, for some reason, the certificates for NF(s) expire without getting renewed, Critical alarms should be raised till such a certificate gets renewed. Also, NF(s) with such expired certificates should not be allowed to establish connections with the O-RAN network.

## Solution #12: Certificate Profile for O-RAN TLS Entity

### Description

This solution addresses key issue #33 of the TR. The solution addresses specific certificate profiling requirements for elements, interfaces and systems expressly defined in O-RAN.

#### Certificate Profiling Requirements for TLS Entity

The present clause defines the certificate profile requirements for the O-RAN nodes that use the TLS protocol for secured communication in the O-RAN network. The nodes involved and the interfaces are described in the table below. The present clause addresses the certificate profile requirements for the TLS end entity that behave either as client, server or both.

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case** | **Interface** | **Nodes involved** | **Security Mechanism** |
| 1 | Open Front Haul(M-Plane) | O-RU and O-DU /SMO | mTLS, SSHv2, FTPES [i.e, O-RU becomes the client] |
| 2 | A1 Interface | Near-RT RIC and Non-RT-RIC | mTLS |
| 3 | Open Front Haul (CUS-Plane) | O-DU and O-RU | IEEE 802.1X with EAP-TLS |
| 4 | O1 | SMO and O-RAN Management Elements | mTLS |
| 5 | O2 | SMO and O-Cloud | mTLS |
| 6 | E2 | Near-RT RIC (xApps) and O-CU-CP and O-CU-UP | NDS/IP(IPsec) or DTLS |
| 7 | F1 | O-CU-CP and O-DU (F1-C) O-CU\_UP and O-DU(F1-U) | NDS/IP(IPsec) or DTLS |

* The architecture for issuing TLS client and server certificates is as per 3GPP 33.310 [i.2] clause 5.1.1.2. TLS certificates will be directly signed by the CA in the operator domain that the entity belongs to.
* The common rules for all certificates defined in 3GPP33.310 [i.2], clause 6.1.1, clause 6.1.3.a will apply to this present clause.
* All certificates used during the enrolment process of O-RAN entities will follow the requirements given in clause 4.X.1.3 of the present document.
* The CA-browser forum [i.20] has the following requirement for the certificate operational and key usage periods. Certificates issued on or after 1 September 2020 should not have a Validity Period greater than 397 days.
* **SubjectAltName** :
* According to RFC 5280[i.13], subjectAltName can be an Internet electronic mail address, a DNS name, an IP address, and a Uniform Resource Identifier (URI). As per RFC 6125[i.18], an application service can be identified by a name or names carried in the subject field (i.e., a CN-ID) and/or in one of the following identifier types within subjectAltName entries (DNS-ID, SRV-ID. URI-ID).
* RFC 6066 [i.17], which is applicable to TLS 1.2, defines that currently, only server names supported in SNI extension to TLS are DNS hostnames where "HostName" contains the fully qualified DNS hostname (FQDN) of the TLS server. RFC 6066 [i.17] also defines that literal IPv4 and IPv6 addresses are not permitted in "HostName". In practice, this means that at least one subjectAltName attribute with FQDN is to be included in server-side TLS end-entity certificates and subjectAltName will not contain only IP address in TLS server certificates.
* **Extensions:**

Mandatory critical key usage:

* digitalSignature for both TLS client and Server certificates. This applies for RSA signature certificate, ECDSA signature certificate, or DSA signature certificate.
* According to TLS1.3 RFC 8446 [i.15] key agreement may be used for Diffie-Hellman certificates. This applies for the ECDH certificate, DH certificate.

Optional and non-critical TLS Feature Extension: RFC7633[i.19] defines a certificate extension that indicates that clients expect stapled OCSP responses with a value of “status\_request(5)” for the certificate and aborts the handshake ("hard-fail") if such a response is not available.

As per RFC 9325 for the common use cases of public key certificates in TLS, servers ought to support the following as a best practice: OCSP RFC 6960 [i.26] and OCSP stapling using the status\_request extension defined in RFC 6066[i.17] The exact mechanism for embedding the status\_request extension differs between TLS 1.2 and 1.3. As a matter of local policy, server operators may request that CAs issue must-staple [i.19] certificates for the server and/or for client authentication.

Certificate Policies: A certificate policy (CP) is a designated set of rules that defines the applicability of a certificate to a particular community or a class of application with common security requirements. A CP is represented in a certificate by an "Object Identifier" (OID). The process of crafting a certificate policy can be derived from the guidelines defined in IETF RFC 3647[i.27].

### Impacts on Existing Interfaces and Functionality

No new impacts were identified by this solution.

### Solution Evaluation

The following table defined below captures the certificate profile for the TLS end entity (Client and Server).

|  |  |  |  |
| --- | --- | --- | --- |
| **O-RAN TLS Client and Server Certificate Profile** | | | |
| Version | | v3 | |
| Serial Number | | Must be Unique Positive Integer in the context of the issuing CA | |
| Subject DN | | (C=<country>), O=<Organization Name>, CN=<Some distinguishing name>. Organization and CN can be in UTF8 format. Note that C is optional element. | |
| cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>. Note that ou is an optional element. | |
|  | |
| Validity Period | | 1 year or less | |
| Signature | | See clause 6.1.1 of 3GPP 33.310[i.2] for the list of supported signature algorithms. | |
| Subject Public Key Info | | See clause 6.1.1 of 3GPP 33.310[i.2] for the list of supported public key types. | |
| **Extensions** | **Mandatory** | **Criticality** | **Value** |
| keyUsage | TRUE | TRUE | digitalSignature for TLS clients and servers |
| extendedKeyUsage | FALSE | FALSE | id-kp-clientAuth TLS clients |  |
| id-kp-serverAuth for TLS servers |  |
| Entities that may be both client and server will have both OIDs set. |  |
| certificatePolicies | FALSE | FALSE | If added, then it should be populated with a CP object identifier(OID). These OIDs correspond to specific policies established by the certificate issuer. |  |
| authorityKeyIdentifier | FALSE | FALSE | This is same as the subjectKeyIdentifier of the Issuer’s certificate. CA utilizes the method as defined in section 2 of RFC 7093[i.24]. |  |
| subjectKeyIdentifier | FALSE | FALSE | This is calculated by the issuing CA utilizing method as defined in section 2 of RFC 7093[i.24]. |  |
| cRLDistributionPoint | TRUE | FALSE | distributionPoint |  |
| According to RFC 5280 [i.13] this indicates if the CRL is available for retrieval using access protocol and location with HTTP URI or LDAP. |  |
| subjectAltName | TRUE | TRUE | Clause 4.12.1.1 details the use of subjectAltName in TLS client and Server certificates. |  |
| authorityInfoAccess | FALSE | FALSE | id-ad-caIssuers |  |
| According to RFC 5280 [i.13] id-ad-caIssuers describes the referenced description server and the access protocol and location, for example, using one or multiple HTTP and/or LDAP URIs.The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user. |  |
| id-ad-ocsp |  |
| According to RFC 5280 [i.13] id-ad-ocsp defines the location of the OCSP responder using HTTP URI. |  |
| TLS feature extension | FALSE | FALSE | id-pe-tlsfeature: “status\_request(5)” |  |
| This can be used according to RFC 7633 [i.19] to prevent downgrade attacks that are not otherwise prevented by the TLS protocol; RFC 7633[i.19] also defines a certificate extension that indicates that clients expects stapled OCSP responses with a value of “status\_request(5)” for the certificate and aborts the handshake ("hard-fail") if such a response is not available. |  |

### Potential Security Requirements

The TLS entity certificates should adhere to the certificate profile outlined in clause 5.12.3, based on their respective roles. The CA responsible for handling the certificate signing request should ensure compliance in accordance with the certificate profile specified in clause 5.12.3.

## Solution #13: Identifying RA and CA as separate logical entities with flexible deployment options

### General Description

This solution addresses Key Issue #1.

Reference : RFC 4210 [i.5] Appendix A :

The reasons that justify the presence of an RA can be split into those that are due to technical factors and those which are organizational in nature.

* If hardware tokens are in use, then not all end entities will have the equipment needed to initialize these; the RA equipment can include the necessary functionality (this may also be a matter of policy).
  + NOTE: This aspect may not be directly related to certificate management, and hence not important for this study.
* Some end entities may not have the capability to publish certificates; again, the RA may be suitably placed for this.
* The RA will be able to issue signed revocation requests on behalf of end entities associated with it, whereas the end entity may not be able to do this (if the key pair is completely lost).

Some of the organizational reasons that argue for the presence of an RA are the following.

* It may be more cost effective to concentrate functionality in the RA equipment than to supply functionality to all end entities (especially if special token initialization equipment is to be used).
* Establishing RAs within an organization can reduce the number of CAs required, which is sometimes desirable.
* RAs may be better placed to identify people with their “electronic” names, especially if the CA is physically remote from the end entity.
  + NOTE: Authenticating a human with a certificate is outside the scope of O-RAN, and therefore, this point is not relevant for this study.
* For many applications, there will already be in place some administrative structure so that candidates for the role of RA are easy to find (which may not be true of the CA).

Based on the above description from RFC 4210 [i.5], it is recommended that operators assess the organizational policies and requirements for making a decision on whether or not, there is a need for having RA and CA deployed separately for O-RAN.

From O-RAN perspective, considering PNFs, CNFs and VNFs as “end entities” to whom certificates need to be issued by operator’s CA, a separate RA can be considered for the following scenarios:

1. For registration of xApps, Near-RT RIC can act as RA
2. For registration of rApps, Non-RT RIC can act as RA
3. Similarly, for registration of PNFs, RA may be hosted in SMO.
4. As an alternative deployment, RA can be hosted in O-Cloud and it can cater to registration of all PNFs/CNFs/VNFs

.

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

This solution addresses Key Issue #1.

### Potential Security Requirements

From O-RAN standardization point of view, RA and CA should be considered as separate logical entities. Operator may decide on deploy these entities in an integrated manner or separately.

## Solution #14: Securing Root CA Private Key

### General Description

Solution #14 addresses Key Issue #20 Secure Storage of Trust Anchors and Private Keys.

Securing the root CA private key is critical for the integrity of Public Key Infrastructure (PKI). A compromised root CA private key can lead to unauthorized certificate issuance, enabling identity spoofing and undermining trust in the entire PKI ecosystem. To secure root CA private keys, it’s essential to maintain Root CA offline as a security best practice.

**Importance of maintaining Root CA offline**

The Primary objective of keeping the root Certificate Authority (CA) offline is to secure the private key associated with the root CA. The root CA private key security is critical because it is used to sign certificates issued by intermediate or Subordinate CAs, and its compromise could lead to fraudulent or unauthorized certificate issuance, impacting the trust of the O-RAN operator public key infrastructure.

By maintaining the root CA offline, the private key is protected from various threats and unauthorized access, and thereby enhancing the security of the PKI infrastructure.

Keeping the root CA offline, often referred to as “offline root CA”, means that private key of the root Certificate Authority (CA) is stored on a system that is not connected to any network or the internet. It is physically isolated from other systems and kept in a secure, air-gapped environment. This isolation reduces the risk of the root CA private key being exposed to online threats and unauthorised access and enhancing the security and trustworthiness of the PKI in O-RAN systems.

The root CA needs to be online only during its initial setup and when issuing certificates for intermediate or Subordinate CAs. Once these intermediate or subordinate CAs certificates are signed, the root CA can be taken offline and stored securely. The root CA serves as a trust anchor for the PKI, and its primary role is to issue certificates for subordinate or intermediate CAs. Subordinate or Intermediate CAs then handle the issuance of certificates to O-RAN VNFs/CNFs, while root CA remains securely offline to maintain PKI integrity.

Note: while it’s common for a root CA’s private key to be stored in HSM for added security, the term “root CA offline” refers to the network connectivity of the root CA system, not the specific use of an HSM. HSM provides additional layers of security by storing the private key in tamper-resistant hardware, but it doesn’t directly affect the network connectivity status of the root CA system. [i.7]

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

This solution addresses Key Issue #20.

### Potential Security Requirements

From O-RAN standardization point of view, it’s recommended to maintain Root CA offline status.

Note: This recommendation applies only if Private CA uses intermediate CAs.

## Solution #15: Certificate enrolment for new NF Deployment using CMPv2

### General Description

Figure 5‑13 illustrates the steps performed to configure enrolment certificate for new NF Deployment. The enrolment certificate shall be used for secured communication between SMO and Cloudified NF. The below procedure is specified as part of Instantiate Network Function on O-Cloud in clause 3.2.1 of ORAN TS Cloudification and Orchestration Use Cases and Requirements for O-RAN Virtualized RAN [i.52].

| Use case stage | Evolution / specification | <<Uses>> Related use |
| --- | --- | --- |
| Goal | Provisioning enrolment certificate for new NF Deployment to perform initial configuration |  |
| Actors and Roles | NFO Service Consumer - Any service consumer allowed to consume NFO services [i.52];  SMO -A Service Management and Orchestration framework [i.51];  NFO – Network Function Orchestration [i.51];  OAM Functions – Operations, Administration and Maintenance function [i.51] ;  Operator PKI- Operator Public Key infrastructure;  O-Cloud-Cloud platform that provides O-RAN standardized interfaces, hosting O-RAN defined software components [i.52];  Cloudified NF- A RAN Network Function software that is deployed in the O-Cloud via one or more NF Deployments [i.52];  NF Deployment - A software deployment on O-Cloud resources that realizes all or part of a Cloudified NF [i.52];  End Entity: user of PKI certificates and/or end user system that is the subject of a certificate [i.13]; |  |
| Pre-conditions | i. NFO has credentials to communicate with PKI.  ii. Certificate Authority to issue the NF Certs to End Entity which is created in PKI.  iii. All End Entity associated trust domains are already created in PKI. |  |
| Begins when | New NF is ready for deployment. |  |
| Step 1 (M) | NFO Service Consumer requests to NFO to instantiate new NF Deployment on the O-Cloud. |  |
| Step 2 (M) | NFO invokes Operator PKI via the vendor specific PKI interface to create End Entity associated to NF Deployment via O1 interface. |  |
| Step 3(M) | Operator PKI configures the End Entity and responds with enrolment data to NFO.  Enrolment data consists of: CMP details associated with provisioned End Entity, including one-time password in section 2.2.3 of RFC 7030 [i.32]; Root CA certificate details. |  |
| Step 4 (M) | NFO incorporates the enrolment data in NF Deployment initial configuration (including PKI server details). NF Deployment should consume these data to request certificate and CA trust certs towards operator PKI. |  |
| Step 5 (M) | NFO triggers NF Deployment in O-Cloud using O2-dms interface, this trigger may be in several steps, for instance secrets shall be shared in secured way before actual NF Deployment starts. |  |
| Step 6 (M) | O-Cloud creates new NF Deployment instance. |  |
| Step 7(O) | The NFO receives information about the success/failure of the NF Deployment instantiation in the O-Cloud. |  |
| Step 8(M) | NF Deployment requests Operator PKI using the initial configuration with received one-time password to enroll certificates. |  |
| Step 9(M) | Operator PKI responds with enrolment certificate to the NF Deployment instance, including the trust anchors of the domains the node will communicate to. |  |
| Ends when | Initial configuration and enrolment certificate is configured for the new NF Deployment. |  |
| Exceptions | None identified |  |
| Post-conditions | Trust established between the Cloudified NF and SMO. |  |

A screenshot of a computer

Description automatically generated

Figure ‑ Certificate enrolment for new NF Deployment

### Impacts on Existing Interfaces and Functionality

None.

### Solution Evaluation

This solution addresses Key Issue #6: Initial Certificate Enrolment for new NFs.

### Potential Security Requirements

**REQ-SEC-CMF-VNF\_CNF-X:** SMO shall configure all the initial information for certificate enrolment procedure for NF Deployment.

# Conclusions

## Key Issue #41: CMPv2

The following proposed normative specifications support PKI certificate management protocol and procedures for an O-RAN PNF, VNF, or CNFs using PKI certificates:

An O-RAN PNF, VNF or CNF requiring a PKI certificate shall support CMPv2 as defined in RFC-4210 [i.5].

An O-RAN PNF, VNF, or CNF supporting CMPv2 shall have the URL, FQDN, and/or IP address for the RA/CA pre-configured or configurable. The RA/CA are defined in RFC-4210 [i.5]. For an instance of a PNF being configurable, an O-RAN PNF can be configured with the IP address or FQDN of one or more Certification Authority (CA/RA) servers using DHCP Option 43 as specified in clause 4.2.2 of 3GPP TS 32.509 [i.8].

## ACME as Optional Certificate Management Protocol

An O-RAN network function requiring a PKI certificate may optionally support ACME as defined in RFC-8555 [i.42] in addition to CMPv2. This is especially beneficial for use with O-Cloud implementations that currently often use ACME as a certificate management protocol via the ACME plugin for the cert-manager component of Kubernetes which is a common technology for dynamic o-cloud deployments.

The ACME solution as described in clause 4.4 addresses the following key issues:

1. Key Issue #37: Lightweight solution (refer to clause 5.2 for details)

2. Key Issue #38: Interoperability (refer to clause 5.3 for details)

## Usage of PSK/Refnum for initial certificate enrolmentenrolment for PNFs, CNFs and VNFs

This clause presents conclusions for solutions #1 and #10.

As described in RFC 4210 [i.5] Section 4.2.2.2 Basic Authenticated Scheme, Initial Authentication Key (IAK) and reference value can be used for initial certificate enrolment using CMPv2. In this document, IAK is referred to as PSK (Pre-shared Key) and reference value is referred to as Refnum.

For backward compatibility, PSK/Refnum-based initial certificate enrolment can be used for PNFs.

Based on the potential security requirements proposed in clause 4.1.4 and 4.10.4, the following normative security requirement can be added to the O-RAN security requirements specification:

Any offline or out-of-band (automated or manual) PSK/Refnum generation, distribution and provisioning systems implemented by the operator should ensure that no rogue PNF/CNF/VNF can obtain valid PSK/Refnum values.

## Vendor root CA certificate renewal notification

This clause proposes conclusions for solution #8, which addresses key issue #8.

A new security requirement can be added in O-RAN security requirements specifications for the potential security requirement proposed in clause 5.8.4 of this Technical Report.

Also, it is recommended that operators monitor notifications which may be raised when vendor root CA certificate is about to expire and take appropriate actions to ensure that there is no impact on system availability.

Proposed new security requirement:

PNFs which use vendor-signed certificates for initial certificate enrolment should monitor the expiry of the vendor root CA certificate used to sign the certificate. When the expiry of the vendor root CA certificate is approaching, PNFs should raise notifications (alarms) with increasing levels of severity as the expiry date gets closer.

## Initial certificate enrolment for PNFs using vendor certificates

This clause proposes conclusions for solution #5, which addresses Key Issue #3 and Key Issue #4.

New security requirements can be added in O-RAN security requirements specifications for the potential security requirements proposed in clause 5.5.4 of this Technical Report.

## Certificate renewal procedure

This clause proposes conclusions for solution #11, which addresses key issue #42.

New security requirement can be added in O-RAN security requirements specifications for the potential security requirements proposed in clause 5.11.4 of this Technical Report.

## RA and CA as separate logical entities

This clause proposes conclusions for solution #13, which addresses key issue #1.

No new security requirements are required for this because it is up to the operator to make a decision whether to deploy RA and CA as independent entities or in an integrated manner.

## EST as Optional Certificate Management Protocol

An O-RAN element requiring a X.509 certificate may optionally support EST as defined in RFC-7030 [i.32] in addition to CMPv2. This is especially beneficial in scenarios where the environment does not require a complex PKI infrastructure for certificate management and also offers a practical solution in scenarios where an O-RAN network element lacks digital certificate bootstrapping or is missing CA information for enrolment. The EST solution as described in clause 5.3 addresses the following key issues:

1. Key Issue #37: Lightweight solution (refer to clause 5.2 for details)

## Use of BRSKI in O-RAN

No normative specifications are necessary for BRSKI as described in Solution #2, which address key issues #1, #2, #10, #37, #38, and #41.

See Clause 5.2.3 Solution Evaluation for further information.

## Mitigating the risk of system overload due to bulk certificate update

No normative specifications are necessary to address Solution #9, which addresses key issue #13.

See Clause 5.9.3 Solution Evaluation for further information on best practices to mitigate the risk of system overload due to a bulk certificate update.

## Key Issue #20: Certificate Management and Secure Storage of Private Keys

Following conclusions are made on the Key-Issue #20 “Certificate Management and Secure Storage of Applications Private Keys”:

For the evaluation two different solution concepts will be considered.

The first concept is the based on an O-Cloud platform hosting a ‘Secure Storage Resource Manager (SSRM)’. This SSRM is managing the interface to either the SW based or HW based secure storage solution. On the north-bound interface the SSRM is providing a common Secure Storage API that can be used by application to request service from the SSRM, while on the south-bound interface the SSRM is hiding the underlying method for key and file storage. The private key is never leaving the secure key storage and any service request that involves the private key is going via the SSRM.

### Evaluation and Assessment for local security module managed by SSRM within the O-Cloud

Advantages:

* Compliance Requirements: Certain regulatory frameworks may require the use of local security modules (e.g., HSM [i.6], [i.46]) for specific security controls. Utilizing a local security module can help meet compliance requirements.
* Reduced Dependency: By having a local security module, organizations reduce their reliance on external systems or services, providing greater control over key management.

Considerations:

* Higher Cost: Security modules are specialized devices and can be more expensive to acquire and maintain compared to using a KMS.
* Limited Scalability: Local security modules have finite capacity, and scaling may require additional security modules or infrastructure investments.
* Operational Complexity: Local security modules require dedicated management, configuration, and maintenance, which may add complexity to the overall O-Cloud architecture and administration.

The second concept is based on a remote Key Management System (KMS). The KMS is external to the O-Cloud, which means it is located outside of the O-Cloud infrastructure. It is responsible for storing and managing private keys by an HSM and issuing key-encryption keys which are used to protect the secure storage volumes.

### Evaluation and Assessment for the KMS

Advantages:

* Key Lifecycle Management: KMS solutions often include features for key rotation, revocation, and auditing, enabling effective key lifecycle management.
* Integration with O-Cloud: KMS solutions offered by cloud service providers can seamlessly integrate with other cloud services, simplifying key management in O-Cloud.

Considerations:

* Dependence on External Service: Utilizing a KMS requires reliance on an external service, which may introduce dependencies and potential availability concerns. Organizations need to ensure proper backup and disaster recovery measures.
* Data Privacy: With a KMS, cryptographic key material is stored and managed by a third-party service. Organizations should consider the privacy implications and evaluate the trustworthiness of the KMS provider.

### Conclusion

It is concluded to go for normative work based on the O-Cloud with local security modules managed by an embedded Secure Storage Resource Manager (SSRM). A local security module offers enhanced physical protection and security measures for cryptographic keys, making it a robust solution for safeguarding sensitive information within the O-Cloud infrastructure.

**Rationale:** By using a local security module, it can be ensured that the cryptographic keys remain within the boundaries of the O-Cloud environment, reducing reliance on external services and enhancing control over key management. While a local HSM may introduce certain considerations such as cost, scalability, and operational complexity, the benefits of its enhanced security and compliance adherence can outweigh these factors in security-sensitive environments like O-Cloud.

## Cert Profile for O-RAN TLS Entity

This clause proposes conclusions for solution #12, which addresses key issue #33.

New security requirements can be added in O-RAN Protocol Specifications for the potential security requirements proposed in clause 5.12.4 of this Technical Report.

The certificate profile defined in clause 5.12.3 of this Technical Report can be applied O-RAN NFs (PNF/VNF/CNF) and O-RAN interfaces that use the TLS protocol for establishing secured communication.

## Certificate enrollment for new NF Deployment using CMPv2

This clause proposes conclusions for solution #15, which addresses key issue #6.

Based on the potential security requirements proposed in clause 5.15.4, the following normative security requirement can be added to the O-RAN security requirements and control specification:

The certificate enrollment procedure for NF deployment defined in clause 5.15.1 of this Technical Report should be applied to O-RAN NFs (VNF/CNF) for establishing secure communication.

# Key Issues-Solutions mapping

This clause contains the mapping of the proposed solutions to the key issues.

Table 7-1 Mapping of Key Issues to Solutions

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Sol. #1** | **Sol. #2** | **Sol. #3** | **Sol. #4** | **Sol. #5** | **Sol. #6** | **Sol. #7** | **Sol. #8** | **Sol. #9** | **Sol. #10** | **Sol. #11** | **Sol. #12** | **Sol. #13** | **Sol. #14** | **Sol. #15** |
| *Key issue #1* |  | X | X |  | X | X |  |  |  |  |  |  | X |  |  |
| *Key issue #2* | X | X | X |  |  |  |  |  |  | X |  |  |  |  |  |
| *Key issue #3* |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| *Key issue #4* |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| *Key issue #5* | VOID | | | | | | | | | | | | | | |
| *Key issue #6* | X |  |  |  |  | X |  |  |  |  |  |  |  |  | X |
| *Key issue #7* | VOID | | | | | | | | | | | | | | |
| *Key issue #8* |  |  | X |  |  | X | X | X |  |  |  |  |  |  |  |
| *Key issue #9* | VOID | | | | | | | | | | | | | | |
| *Key issue #10* |  | X | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #11* | VOID | | | | | | | | | | | | | | |
| *Key issue #12* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| *Key issue #13* |  |  |  |  |  | X | X |  | X |  |  |  |  |  |  |
| *Key issue #14* | VOID | | | | | | | | | | | | | | |
| *Key issue #15* | VOID | | | | | | | | | | | | | | |
| *Key issue #16* | VOID | | | | | | | | | | | | | | |
| *Key issue #17* | VOID | | | | | | | | | | | | | | |
| *Key issue #18* |  |  |  |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #19* |  |  |  |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #20* |  |  |  |  |  | X | X |  |  |  |  |  |  | X |  |
| *Key issue #21* |  |  |  |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #22* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #23* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #24* |  |  |  |  |  |  | X |  |  |  |  |  |  |  |  |
| *Key issue #25* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #26* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #27* |  |  | X |  | X | X | X |  |  |  |  |  |  |  |  |
| *Key issue #28* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #29* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #30* |  |  | X |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #31* | VOID | | | | | | | | | | | | | | |
| *Key issue #32* | VOID | | | | | | | | | | | | | | |
| *Key issue #33* |  |  | X |  |  | X | X |  |  |  |  | X |  |  |  |
| *Key issue #34* | VOID | | | | | | | | | | | | | | |
| *Key issue #35* | VOID | | | | | | | | | | | | | | |
| *Key issue #36* |  |  |  |  |  | X | X |  |  |  |  |  |  |  |  |
| *Key issue #37* | X | X | X | X | X |  | X |  |  |  |  |  |  |  |  |
| *Key issue #38* |  | X |  | X |  |  |  |  |  |  |  |  |  |  |  |
| *Key issue #39* |  |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
| *Key issue #40* | VOID | | | | | | | | | | | | | | |
| *Key issue #41* |  | X |  |  |  |  | X |  |  |  |  |  |  |  |  |
| *Key issue #42* |  |  |  |  |  |  | X |  |  |  | X |  |  |  |  |
| *Key issue #43* | X |  | X |  |  | X | X |  |  |  |  |  |  |  |  |

# Annex: Change history/Change request (history)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Revision** | **Doc status** | **Author** | **Description** |
| 2022.02.22 | V01.00.01 | Draft | SFG | Document creation, template |
| 2022.03.08 | V01.00.02 | Draft | SFG | Updated template |
| 2022.04.12 | V01.00.03 | Draft | SFG | Added key issues generated by the CMF subworking group. |
| 2022.06.14 | V01.00.04 | Draft | SFG | Incorporated the following CRs:  RMI-2022.04.26-SFG-Certificate-management-CR-002  RMI-2022.05.10-SFG-Certificate-management-CR-003  NOK-2022.05.10-SFG-Certificate-management-Multiple certificates per interfaces - CR\_03  NOK-2022.05.10-SFG-Certificate-management-merge of key issues 5 and 7-CR\_02  NOK-2022.05.10-SFG-Certificate-management-Moving Key issues to Solutions-CR\_01 |
| 2023.01.10 | V01.00.05 | Draft | SWG | Incorporated the following CRs:  ATT-2022.06.07- SFG-Certificate-management-architecture-CR\_01-r2  NOK-2022.07.04-SFG-Certificate-management-vendor-cert-based-enrolment\_CR\_05-r8  NOK-2022.07.04-SFG-Certificate-management-PSK\_Refnum-CR\_04\_r8  RMI.COM-2022.08.22-WG11-CR-0001-Certificate-Management-Study-on-ACME  ORA-2022.09.27-WG11-CR-0025-Certificate-Management-SecStorageHSMv04  ATT-2022.10.24-SFG-CMPv2-solution-CR\_02-r1  NOK-ORA-2022.12.06-WG11-CR-0013-Certificate-Management-SecStorage\_v01 |
| 2023.06.30 | V01.00.06 | Draft | SWG | Incorporated the following CRs:  DT-2023.01.31-SFG-TR-Certificate-Management-Framework-ACME-optional\_v5  ERI-2023.01.25-WG11-CR0019-CertificateManagementFramework-TR-v01  NOK-2023.02.01-WG11-CR-0046-Certificate-management-Bulk\_Updates\_r2  NOK-2023.02.01-WG11-CR-0045-Certificate-management-PSK\_Refnum  NOK-2023.05.02-WG11-CR-0047-Certificate-management-Renewal-v01  SYM-2023.05.09-SFG-CR-0009-CertificateProfile\_TechnicalReport\_v07 |
| 2023.09.12 | V01.00.07 | Draft | SWG | Incorporated the following CRs:  NOK-2023.07.06-WG11-CR-0084-Certificate-management-RA-CA-v03  AKA-2023.07.10-WG11-CR-0001-Align-Certificate-Management-terminology\_v02  SYM-2023.06.27-SFG-CR-0019-CertificateProfile\_TR\_Conclusion\_v03  WG11-2023.07.25-WG11-CR-0007-Key issue-Solutions mapping\_v02  NOK-2023.07.06-WG11-CR-0085-Plug-and-connect-PNFs-v03  NOK-2023.08.07-WG11-CR-0099-BRSKI\_v02 |
| 2023.10.24 | V01.00.08 | Draft | SWG | WG11-2023.09.08-WG11-CR-0010-Key issues-1-to-11-42-43-v02  ATT-2023.09.12-WG11-CR-69-Solution-Evaluation-Reorganization  NOK-2023.09.08-0107-Key issue-Solutions mapping  WG11-2023.09.25-WG11-CR-0013-Key issues-12-to-25-v03  NOK-2023.08.07-WG11-CR-0106-KI28-PKI-Migration  NOK-2023.08.07-WG11-CR-0118-Soltion-PKI-Migration-v2  SYM.AO-2023.08.22-WG11-CR-0022-CertificateManagemet-EST\_Protocol-v07  NOK-2023.10.17-WG11-CR-0117-Solution%231\_Solution%2310\_Updates  NOK-2023.10.17-WG11-CR-0119-Solution%238\_Updates\_v2  NOK-2023.10.17-WG11-CR-0120-Conclusions\_Sol5\_11\_13  WG11-2023.09.25-WG11-CR-0014-Key issues-9 11 and 26-to-41-v01 |
| 2024.03.13 | V02.00 | Draft | SWG | NOK-2023.06.20-WG11-CR-0083-Conclusion\_on\_Certificate-Management-SecStorage\_v06  RMI-2023.10.17-WG11-CR-0013-Securing private keys\_v2  ATT-2023.10.19-0070-Key-issue-Solutions-mapping-update  SYM.AO-2023.11.28-WG11-CR-0032-EST\_Protocol\_Conclusion-v03  ATT-2023.11.28-WG11-CR-0031-CertMgmtTR\_KeyIssues33and36Updates-v3  ATT-2023.12.19-WG11-CR-0032-CertMgmtTR\_Conclusion\_Solution2-v2  ATT-2023.12.19-WG11-CR-0033-CertMgmtTR\_Conclusion\_Solution9-v1  WG11-2024.01.08-WG11-CR-0021-CertMgmtTR\_PSR\_Solution6-v2  NOK-2023.10.17-WG11-CR-0138-Solution\_8\_Conclusion-correction  SYM-2024.01.30-WG11-CR-0041-CertificateProfile\_Conclusion-v03 |
| 2024.06.26 | V03.00 | Draft | SWG | NEC-2024.04.09-WG11-CR-0017-CertMgmtFrmk\_Abbreviations\_and\_Acronyms\_Updates-v1  ERI-2024.05.14.-WG11-CR0124-CertificateManagementFramework-KeyIssue40mapping-v01  ERI-2024.05.14-WG11-CR0126-CertificateManagementFramework-Subjectaltname-v02  ERI-2024.05.28-WG11-CR0133-CertificateManagementFramework-CertificateEnrolmentforNewCNF-v04 |
| 2024.11.04 | V04.00 | Draft | WG11 | NOK-2024.07.12-WG11-CR-0175-CertMgmt-req-CRL-failure-alarms-v02  NOK-2024.07.12-WG11-CR-0176-CertMgmt-req-storage-space-alarms-v02  ERI-2024.06.25-WG11-CR0144-CertificateManagementFramework-Clause6.13Conclusion for solution5.15-v03  NOK-2024.09.16-WG11-CR-0197-CMPv2-polling-failure-alarms-v03 |