ETSI GS NFV-SOL 023 V5.4.1 (2026-04)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; Specification of protocol and data model solutions for CMF - NFV-MANO reference point

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/NFV-SOL023ed541

Keywords
data models, MANO, NFV, protocol

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies the interfaces and reference points between CMF and VNFM to fulfil the requirements specified in ETSI GS NFV-IFA 033 [2]. The present document analyses existing solutions for ETSI GS NFV-IFA 033 [2] / ETSI GS NFV-IFA 026 [1] requirements. Based on the analysis results, the present document profiles them and includes OpenAPI representations for a RESTful protocol and data model specification for Certificate Notification interface and "Additional features" of Certificate Management interface since the subset of VNF Lifecycle Management interface refers to the ETSI GS NFV other specifications.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Architecture enhancement for Security Management Specification".

[2] ETSI GS NFV-IFA 033: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Reference points related to Security Manager and Certificate Management Function - Interface and Information Model Specification".

[3] ETSI GS NFV-SOL 002: " Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; RESTful protocols specification for the Ve-Vnfm Reference Point".

[4] ETSI GS NFV-SOL 013: " Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs".

[5] Void.

[6] Void.

[7] IETF RFC 8141: "Uniform Resource Names (URNs)".

[8] IETF RFC 2986: "PKCS #10: Certification Request Syntax Specification Version 1.7".

[9] IETF RFC 9483: "Lightweight Certificate Management Protocol (CMP) Profile".

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

[11] ETSI GS NFV-SOL 001: "Network Functions Virtualisation (NFV) Release 5; Protocols and Data Models; NFV descriptors based on TOSCA specification".

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

[13] IETF RFC 9810: "Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)".

[14] IETF RFC 9811: "Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)".

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

[16] IETF RFC 8737: "Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension".

[17] IETF RFC 9447: "Automated Certificate Management Environment (ACME) Challenges Using an Authority Token".

2.2 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, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] IETF RFC 2510: "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[i.3] IETF RFC 8894: "Simple Certificate Enrolment Protocol".

[i.4] IETF RFC 7030: "Enrolment over Secure Transport".

[i.5] Void.

[i.6] OpenAPI™ Specification.

[i.7] ETSI GS NFV-SOL 015: "Network Functions Virtualisation (NFV); Protocols and Data Models; Specification of Patterns and Conventions for RESTful NFV-MANO APIs".

[i.8] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.9] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

[i.10] IETF RFC 9480: "Certificate Management Protocol (CMP) Updates".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GR NFV 003 [i.1].

ACME	Automatic Certificate Management Environment
CA	Certification Authority
CMF	Certificate Management Function
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
EST	Enrolment over Secure Transport
OID	Object Identifier
PSE	Personal Security Environment
SCEP	Simple Certificate Enrolment Protocol

4 Overview of Certificate Management

4.1 Introduction

This clause provides an overview of certificate management interface on the reference point Cm-Vnfm specified in ETSI GS NFV-IFA 033 [2]. The present document supports below interfaces:

1) The Certificate Management interface as specified in clause 11.2 of ETSI GS NFV-IFA 033 [2]. The Certificate Management interface is exposed by the CMF and consumed by the VNFM. This is for the management of VNFCI and VNF OAM certificate in delegation mode. Profiling of the existing solution are specified in clauses 4.2.1 and 5 of the present document, and new APIs that are not supported by existing solution are specified in clause 5.6 by RESTful API.

2) A subset of the VNF LCM interface (operation occurrence event notifications and query VNF) exposed by the VNFM and consumed by the CMF as specified in clause 11.3 of ETSI GS NFV-IFA 033 [2]. This is for the management of VNFCI and VNF OAM certificate in direct mode. This interface is specified in clause 6 of the present document.

3) Certificate Notification Service interface as introduced in clause 11.4 of ETSI GS NFV-IFA 033 [2] over the Cm-Vnfm reference point with the VNFM as consumer of the service interface. This is specified in clause 7 of the present document.

4.2 Overview of protocols and data models

4.2.1 Summary of CMP

4.2.1.1 Introduction

This clause provides an overview over CMP as specified in IETF RFC 9810 [13] and IETF RFC 9811 [14] which are analysed to the requirements on the certificate management interfaces defined in ETSI GS NFV-IFA 033 [2]. The overview covers the high-level feature summary, involved entities, and provides how to support certificate management interface requirements with considering CMP.

NOTE: CMP version 2 is used in the current version of the present document.

4.2.1.2 Feature summary

The Certificate Management Protocol version 2 is an internet protocol standardized by the IETF for obtaining digital certificates within a Public Key Infrastructure (PKI). CMP provides set of features and flexibility, supporting types of cryptography. The main purpose and features are, facilitating the automated management of digital certificates, including issuance, updates, and revocation, which are operated between a Certificate Authority (CA) and an end entity.

Key features are:

- Self-contained Messages: CMP messages can use different transport mechanisms (unlike related protocols like EST and SCEP).
- Full Certificate Life Cycle Support: End entities can use CMP to obtain certificates from a CA, request updates, and handle revocations.
- Key Pair Generation: Typically done by the client side, but can also be done at the CA server side.
- Proof-of-Possession: Usually achieved through self-signatures of requested certificate contents, but CMP supports other methods.
- Proof-of-Origin: Supported in two formats: based on a shared secret (initially) and signature-based (using pre-existing certificates).
- Key Pair Recovery: Allows recovery of lost private keys stored by the CA.
- Other Requests: CMP supports various other request types, such as retrieving CA certificates and obtaining PKI parameters.

CMP supports messages related to certificate management as follows:

- initialization request message (ir), with ip response;
- certification request message (cr), with cp response;
- certification request message (p10cr), with cp response;
- certificate confirmation (certConf)key pair update operation (kur/kup);
- certificate update message;
- CA key pair update message;
- certificate discovery message;
- recovery message;
- revocation messages (rr/rp);
- PSE message;
- End Entity Initialization.

CMP messages are encoded in ASN.1 using the DER method. The protocol is independent of the transport mechanism, ensuring end-to-end security. Examples of transport options are HTTP, HTTPS, and CoAP.

A CMP protocol can be realized in several ways but all implementations shall support the basic authenticated scheme.

4.2.1.3 Involved entities

CMP has below involved entities:

- End Entities (EEs): is used here to refer to the entity to whom the certificate is issued.
- Certificate Authorities (CAs): Issue legal certificates and act as CMP servers.

- Registration Authorities (RAs): Mediate between EEs and CAs.

4.2.1.4 Entities mapping to the NFV Certificate management functions

The involved entities described in clause 4.2.1.3 are mapped to the below NFV certificate management functions as follows:

- End Entities (EEs): For the case of VNFC/VNF OAM certificate management, VNFC. For the delegation mode case, VNFM acts as a delegate for certificate management operations on behalf of VNFC.
- Certificate Authorities (CAs): For the case of VNFC/VNF OAM certificate management, CA.
- Registration Authorities (RAs): For the case of VNFC/VNF OAM certificate management delegation mode, CMF.

NOTE: The mapping above is a mapping of roles (i.e. mapped NFV entities have roles as described involved entities), and not a strict mapping in term of functionality and protocol details.

4.2.2 Summary of ACME

4.2.2.1 Introduction

This clause provides an overview of the ACME protocol as specified in IETF RFC 8555 [15], which is analysed in relation to the requirements on certificate management interfaces defined in ETSI GS NFV-IFA 033 [2]. The overview covers the high-level feature summary, involved entities, and explains how ACME supports automated certificate lifecycle management, including issuance, renewal, and revocation, in alignment with the interface requirements.

4.2.2.2 Feature summary

The Automatic Certificate Management Environment (ACME) protocol, as specified in IETF RFC 8555 [15], is an internet protocol designed to automate the process of certificate management within a Public Key Infrastructure (PKI). ACME enables secure and efficient interactions between Certificate Authorities (CAs) and clients, facilitating certificate issuance, renewal, and revocation with minimal manual intervention.

Key features are, e.g.:

- Automated Certificate Lifecycle Management: end-to-end automation for obtaining and managing certificates.
- Challenge-Based Validation: Clients prove domain control through standardized challenges (e.g. HTTP-01, DNS-01, TLS-ALPN-01), ensuring secure and verifiable certificate requests.
- RESTful Interface: HTTPS-based REST APIs for communication.
- Support for Multiple Identifiers: Allows requesting certificates for multiple domain names and supports wildcard certificates.
- Account Management: Clients register accounts with CAs, enabling persistent identity and authorization for certificate operations.
- Revocation: Provides mechanisms for clients to request certificate revocation when necessary.
- Extensibility: The protocol is designed to be extensible, allowing future enhancements and customizations.

ACME supports messages related to certificate management as following:

- Account Creation and Management: Clients register with the CA by creating an account, which serves as the basis for authentication and authorization of subsequent operations.
- Order Resource: Request the issuance of a certificate for one or more identifiers (e.g. domain names). The order tracks the status of the request and associated validations.
- Authorization Resource: Represents the CA's authorization for the client to manage a specific identifier. It includes challenge objects that the client fulfils.

- Challenge Resource: Specifies the method by which the client proves control over an identifier. Examples of the challenge types are HTTP-01, DNS-01, and TLS-ALPN-01.
- Certificate Resource: Once all challenges are successfully completed, the CA issues the certificate and makes it available via this resource.
- Revocation Request: Allows clients to request the revocation of a previously issued certificate, either using the account key or the certificate's private key.
- Key Change Request: Enables clients to update the account key associated with their ACME account, ensuring continuity in case of key rotation.
- External Account Binding (EAB): Supports binding an ACME account to an external identity, often used in enterprise or hosted CA environments.

ACME messages are encoded in JSON and transmitted over HTTPS using RESTful APIs. This design ensures interoperability, ease of integration, and secure communication. The protocol is transport-dependent (HTTPS) but benefits from widespread support and simplicity in deployment.

This overview aligns ACME's capabilities with the certificate management interface requirements defined in ETSI GS NFV-IFA 033 [2], demonstrating how ACME supports automated and scalable certificate operations in NFV environments.

4.2.2.3 Involved entities

ACME has below involved entities:

- ACME clients: The entity using the protocol to request certificate management actions. An ACME client may run on a server system that requires valid X.509 certificates. Or, it may run on a separate server that does not consume the certificate but is authorized to respond to a CA-provided challenge.
- ACME server: The entity responding to client requests, performing the requested actions if the client is authorized.

4.2.2.4 Entities mapping to the NFV Certificate management functions

The involved entities described in clause 4.2.2.3 are mapped to the below NFV certificate management functions as follows:

- ACME clients: For the case of MANO certificate management, MANO entities.
- ACME server: For the case of MANO certificate management, CMF.

NOTE: The mapping above is a mapping of roles (i.e. mapped NFV entities have roles as described involved entities), and not a strict mapping in term of functionality and protocol details.

5 Certificate Management interface

5.1 Description

This interface allows the VNFM to invoke Certificate Management operations towards the CMF.

The operations provided through this interface are:

- Register
- Certificate Signing Request
- Deregister
- Revoke

- Query Subject Info
- Query Certificate Info

See more details of the operations defined in clause 11.2 of ETSI GS NFV-IFA 033 [2].

5.2 NFV operation mapping to profiled solution

5.2.1 Certificate Signing Request for VNFC/VNF OAM certificate management

Selected CMP message of the "certification request message (p10cr), with cp response" specified in IETF RFC 9810 [13], IETF RFC 9811 [14] and IETF RFC 9483 [9] is identified to map to the Certificate Signing Request operation specified in clause 11.2.3 of ETSI GS NFV-IFA 033[2], shown in table 5.2.1-1.

Table 5.2.1-1: CMP certification request message (p10cr), with cp response mapped to NFV Certificate Signing Request operation for certificate management

CMP message	Description
certification request message (p10cr), with cp response	A Certification request message contains as the PKIBody a CertificationRequest data structure, which specifies the requested certificates. This message is intended to be used for existing PKI entities who wish to obtain certificates. A Certification response message contains as the PKIBody a CertRepMessage data structure, which has a status value for each certificate requested, and optionally has a CA public key, failure information, a subject certificate, and an encrypted private key.

5.2.1a Certificate Signing Request for MANO certificate management

Selected ACME message of the "Certificate Issuance" specified in IETF RFC 8555 [15] is identified to map to the Certificate Signing Request operation specified in clause 11.2.3 of ETSI GS NFV-IFA 033 [2], shown in table 5.2.1a-1.

Table 5.2.1a-1: ACME Certificate issuance mapped to NFV Certificate Signing Request operation for certificate management

ACME message	Description
Certificate Issuance by sending a POST to server's newOrder resource	The client begins the certificate issuance process by sending a POST request to the server's newOrder resource. The body of the POST is a JWS object whose JSON payload is a subset of the order object, containing the fields that describe the certificate to be issued.

5.2.2 Revoke operation for VNFC/VNF OAM certificate management

Selected CMP message of the "revocation request message (rr), with rp response" specified in IETF RFC 9810 [13], IETF RFC 9811 [14] and IETF RFC 9483 [9] is identified to map to the Revoke operation specified in clause 11.2.5 of ETSI GS NFV-IFA 033[2], shown in table 5.2.2-1.

Table 5.2.2-1: CMP revocation request message (rr), with rp response mapped to NFV Revoke operation for certificate management

CMP message	Description
revocation request message (rr), with rp response	A Certification request message contains as the PKIBody a RevReqContent data structure, which specifies the revocation certificates. This message is intended to be used for existing PKI entities who wish to revoke certificates. The name of the requester is present in the PKIHeader structure. A revocation response message contains as the PKIBody a RevRepContent data structure, which has a status value for each certificate revoked, and optionally has a CRLs.

5.2.2a Revoke for MANO certificate management

Selected ACME message of the "Certificate Revoke" specified in IETF RFC 8555 [15] is identified to map to Revoke operation specified in clause 11.2.5 of ETSI GS NFV-IFA 033[2], shown in table 5.2.2a-1.

Table 5.2.2a-1: ACME Certificate Revoke mapped to NFV Revoke operation for certificate management

ACME message	Description
Certificate Revocation by sending a POST to server's certRevoke resource	The client begins the certificate revoke process by sending a POST request to the ACME server's revokeCert URL. The body of the POST is a JWS object whose JSON payload contains the certificate to be revoked.

5.2.3 Registration for MANO certificate management

Selected ACME message of the "Account Creation" specified in IETF RFC 8555 [15] is identified to map to Registration operation specified in clause 11.2.2 of ETSI GS NFV-IFA 033 [2], shown in table 5.2.3-1.

Table 5.2.3-1: ACME Account Creation mapped to NFV Registration operation for certificate management

ACME message	Description
Account Creation operation by sending a POST to server's new-account resource	A client creates a new account with the server by sending a POST request to the server's newAccount URL.

5.2.4 Deregistration for MANO certificate management

Selected ACME message of the "Account Deactivation" specified in IETF RFC 8555 [15] is identified to map to Deregistration operation specified in clause 11.2.4 of ETSI GS NFV-IFA 033 [2], shown in table 5.2.4-1.

Table 5.2.4-1: ACME Account Deactivation mapped to NFV Deregistration operation for certificate management

ACME message	Description
Account Deactivation operation by sending a POST to created-client's resource with status field of "deactivated"	A client deactivates an account by posting a signed update to the account URL with a status field of "deactivated". A deactivated account can no longer request certificate issuance or access resources related to the account, such as orders or authorizations.

5.2.5 Query Subject Info information for MANO certificate management

Selected ACME message of the "Get Account Information" specified in IETF RFC 8555 [15] is identified to map to Query Subject Info operation specified in clause 11.2.6 of ETSI GS NFV-IFA 033 [2], shown in table 5.2.5-1.

Table 5.2.5-1: ACME Get Account Information mapped to NFV Query Subject Info operation for certificate management

ACME message	Description
Query Subject Info by sending a POST-as-GET to server's account resource	The client begins the Query Subject Info process by sending a POST-as-GET request to the ACME server's account resource URL. The principles of "POST-as-GET" are specified in IETF RFC 8555 [15].

5.2.6 Query Certificate Info for MANO certificate management

Selected ACME message of the "Poll for status" specified in IETF RFC 8555 [15] is identified to map to Query Certificate Info operation specified in clause 11.2.7 of ETSI GS NFV-IFA 033 [2], shown in table 5.2.6-1.

Table 5.2.6-1: ACME Poll for status mapped to NFV Query Certificate Info operation for certificate management

ACME message	Description
Query Certificate Info Operation by sending a POST-as-GET to server's order resource	The client begins the Query Certificate Info process by sending a POST-as-GET request to the ACME server's order resource URL. The principles of "POST-as-GET" are specified in IETF RFC 8555 [15].

5.3 Sequence diagrams

5.3.1 Flow of the Registration of the Subject for VNFC/VNF OAM certificate management

The present clause describes the procedure for the Registration of an "Individual Subject" resource.

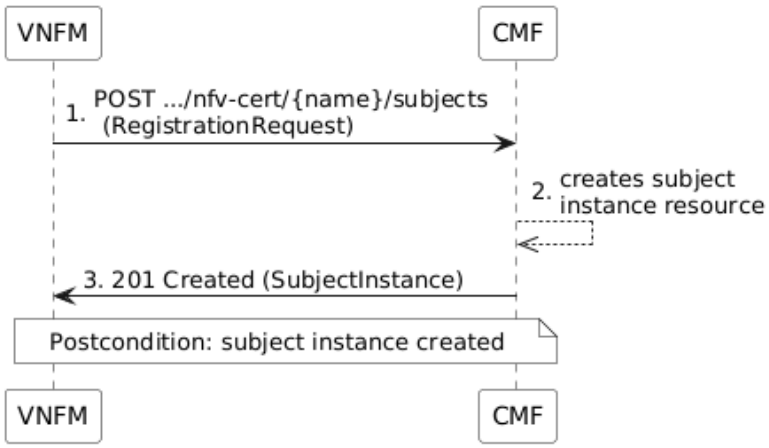

Figure 5.3.1-1: Flow of the registration of a Subject resource

The procedure consists of the following steps as illustrated in figure 5.3.1-1:

1) The VNFM sends a POST request to the "Subject" resource including in the message content a data structure of type "RegistrationRequest".

2) The CMF creates a new "Individual Subject" resource.

3) The CMF returns a 201 Created response containing a representation of the "Individual Subject" resource just created by the CMF and provides the URI of the newly-created resource in the "Location" HTTP header.

Postcondition: Upon successful completion, a new "Individual Subject" resource has been created.

5.3.1a Flow of the Registration for MANO certificate management

The present clause describes the procedure for the Registration of an "Account" resource.

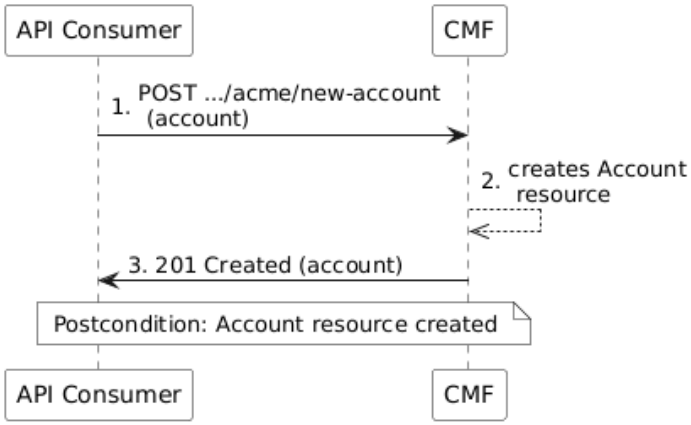

Figure 5.3.1a-1: Flow of the registration of a Account resource

The procedure consists of the following steps as illustrated in figure 5.3.1a-1:

1) The API consumer sends a POST request to the "Account" resource.

2) The CMF creates a new "Account" resource.

3) The CMF returns a 201 Created response containing a representation of the "Account" resource just created by the CMF and provides the URI of the newly-created resource in the "Location" HTTP header.

Postcondition: Upon successful completion, a new "Account" resource has been created.

5.3.2 Flow of the Deregistration of the Subject for VNFC/VNF OAM certificate management

The present clause describes the procedure for the Deregistration of an "Individual Subject" resource.

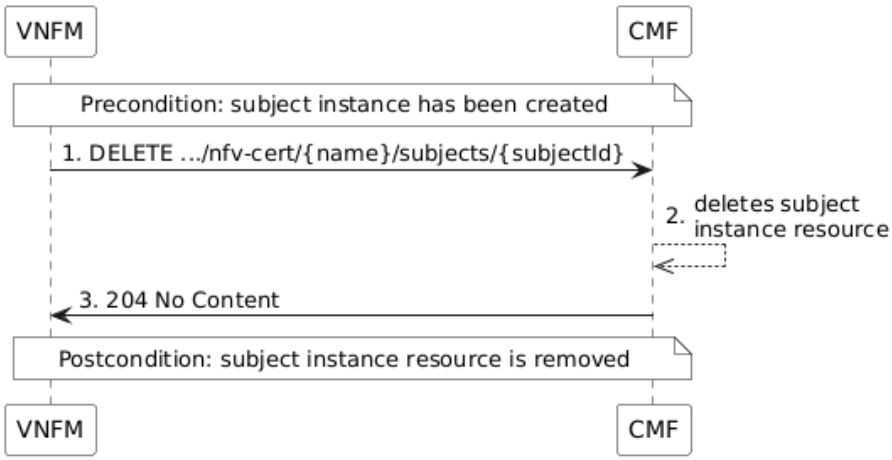

Figure 5.3.2-1: Flow of the deregistration of a Subject resource

Precondition: The resource representing the Subject instance to be deleted has been created.

The procedure consists of the following steps as illustrated in figure 5.3.2-1:

1) VNFM sends a DELETE request to the "Individual Subject" resource.

2) The CMF deletes the "Individual Subject" resource and the associated Subject identifier.

3) The CMF returns a "204 No Content" response with an empty message content.

Postcondition: The resource representing the Subject instance has been removed from the list of Subject instance resources.

5.3.2a Flow of the Deregistration for MANO certificate management

The present clause describes the procedure for the Deregistration of an "Account" resource.

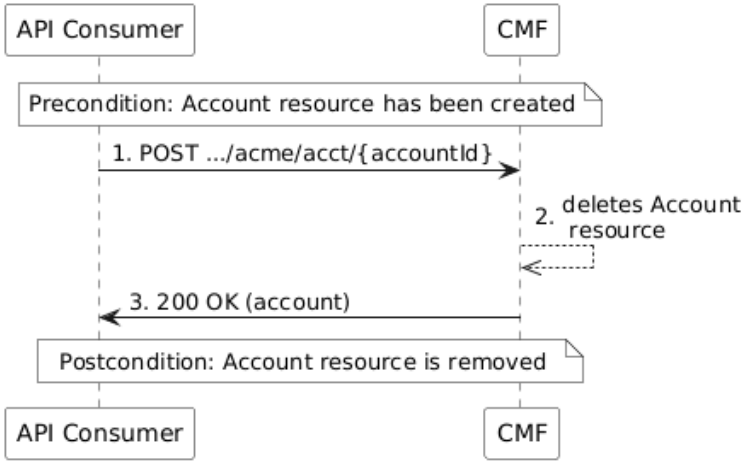

Figure 5.3.2a-1: Flow of the deregistration of a Account resource

Precondition: The resource representing the Account resource to be deleted has been created.

The procedure consists of the following steps as illustrated in figure 5.3.2a-1:

1) API Consumer sends a POST request to the Account resource.

2) The CMF deletes the Account resource.

3) The CMF returns a "200 OK" response and includes data structures of type account object in the message content.

Postcondition: The resource representing the Account has been removed.

5.3.3 Flow of the CSR Request for VNFC/VNF OAM certificate management

The present clause describes the procedure for the Certificate Signing Request.

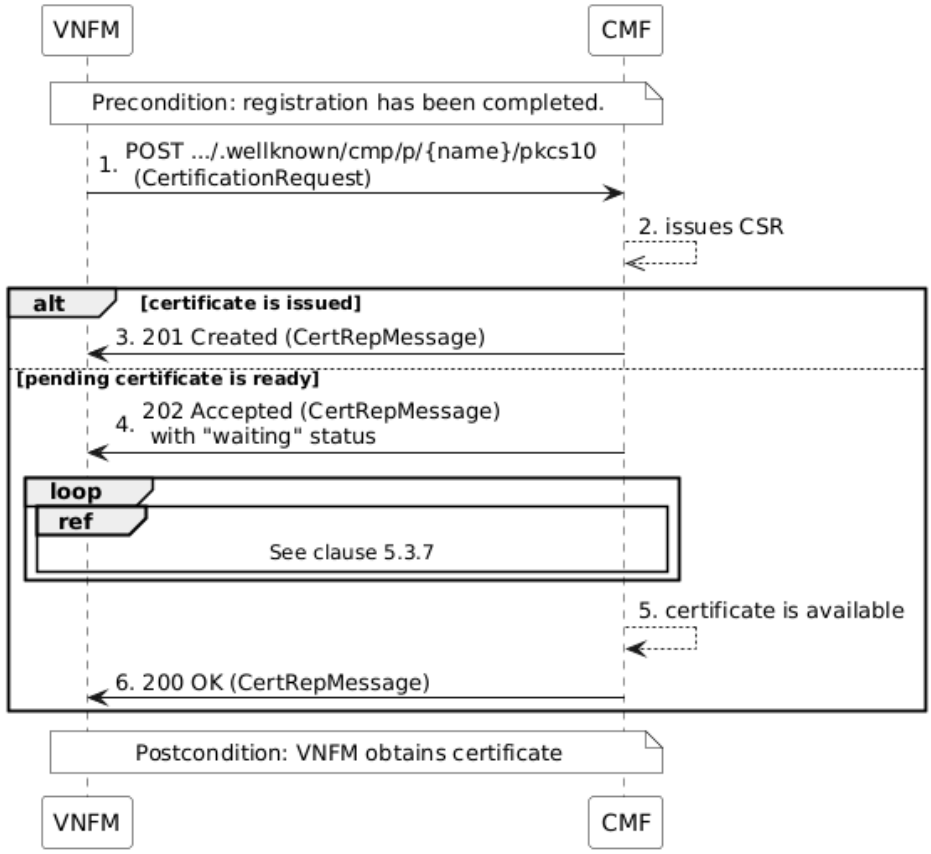

Figure 5.3.3-1: Flow of the CSRRequest

Precondition: Registration of subject has been completed.

The procedure consists of the following steps as illustrated in figure 5.3.3-1:

1) VNFM sends a POST request to pkcs10 URI including in the message content a data structure of type "CertificationRequest".

2) The CMF issues CSR.

3) If the certificate is available, the CMF returns a 201 Created response containing CertRepMessage and certificate.

4) If the operation to issue is pending that certificate is ready, the CMF returns a "202 Accepted" response containing the message content a data structure of type "CertRepMessage" with "waiting" status.

5) Until certificate is available, VNFM sends a POST request to pkcs10 URI to polling status as clause 5.3.6.

6) After certificate is available, the CMF returns a "200 OK" containing the message content a data structure of type "CertRepMessage" and certificate.

Postcondition: Upon successful completion, the VNFM obtains certificate.

5.3.3a Flow of the CSR Request for MANO certificate management

The present clause describes the procedure for the Certificate Signing Request.

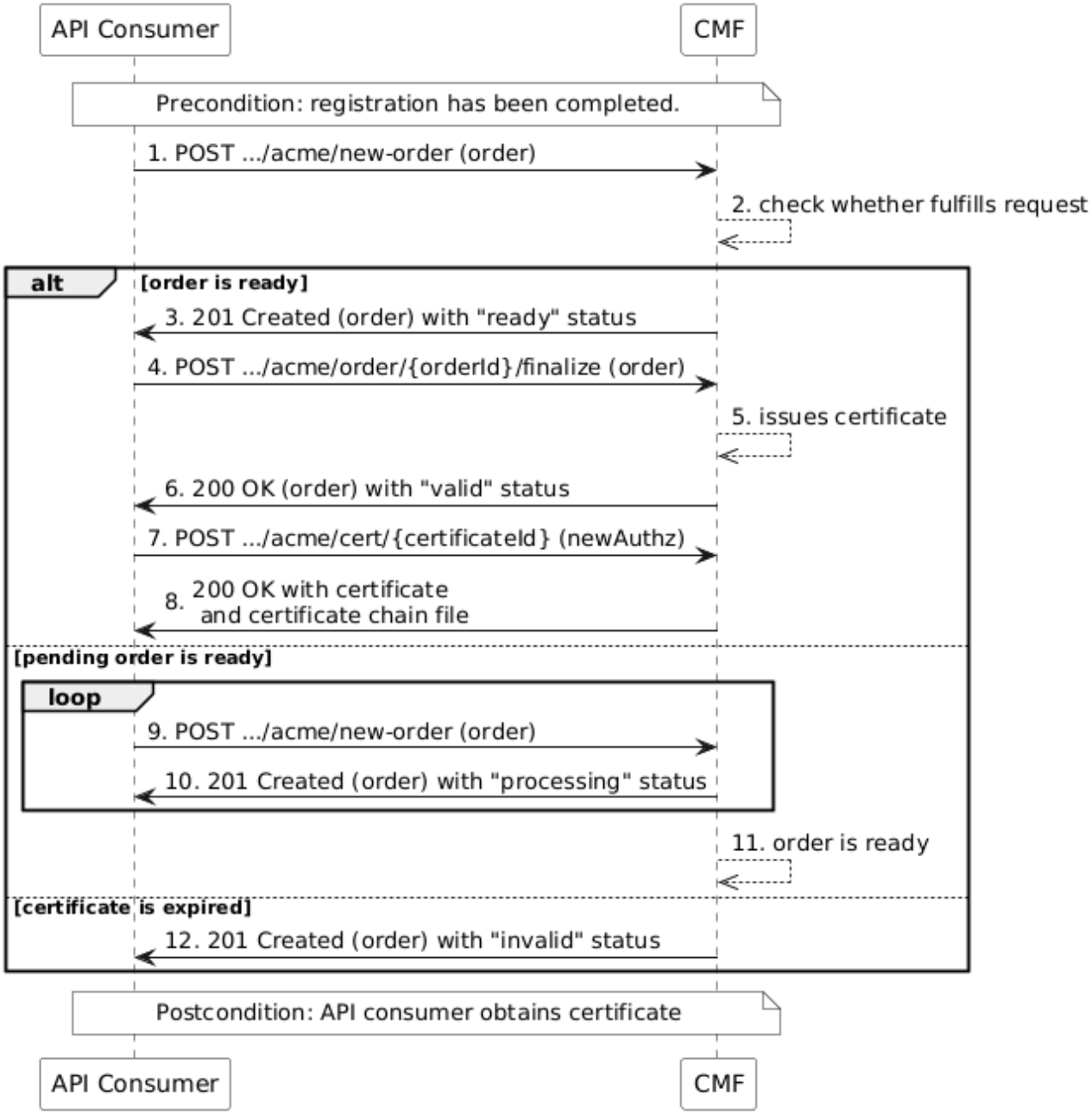

Figure 5.3.3a-1: Flow of the CSR Request

Precondition: Registration has been completed.

The procedure consists of the following steps as illustrated in figure 5.3.3a-1:

1) API consumer sends a POST request to the "Order" resource.
2) The CMF checks whether fulfils request.
3) If the order is ready, the CMF returns a 201 Created response containing order object with "ready" status.
4) API consumer sends a POST request to finalize resource.
5) CMF issues certificate.
6) The CMF returns a "200 OK" response and includes data structures of type order object with "valid" status.
7) API consumer sends a POST request to Certificate resource with newAuthz object.

8) The CMF returns a "200 OK" response and includes certificate and certificate chain files.

9) Until order is ready, API consumer sends a POST request to Order resource.

10) If the operation of order is pending, the CMF returns a "201 Created" response containing the message content a data structure of type order object with "processing" status.

11) CMF processes order until order is ready.

12) If the operation of order is expired, the CMF returns a "201 Created" response containing the message content a data structure of type order object with "invalid" status.

Postcondition: Upon successful completion, the VNFM obtains certificate.

5.3.4 Flow of the Revocation of the certificate for VNFC/VNF OAM certificate management

This clause describes the procedure for the Revocation.

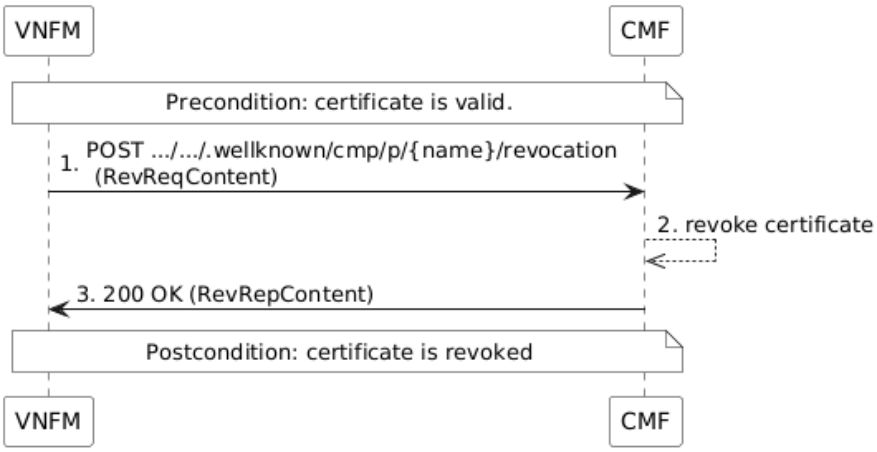

Figure 5.3.4-1: Flow of the revocation of a Certificate resource

Precondition: The Certificate is valid.

The procedure consists of the following steps as illustrated in figure 5.3.4-1:

1) VNFM sends a POST request to the revocation URI including in the message content a data structure of type "RevReqContent".

2) The CMF revokes the certificate.

3) The CMF returns a "200 OK" response containing the message content a data structure of type "RevReqContent".

Postcondition: The Certificate is revoked.

Error handling: In the case where certificate is not available, such as certificate is expired, appropriate error information is provided in the response.

5.3.4a Flow of the Revocation of the certificate for MANO certificate management

This clause describes the procedure for the Revocation.

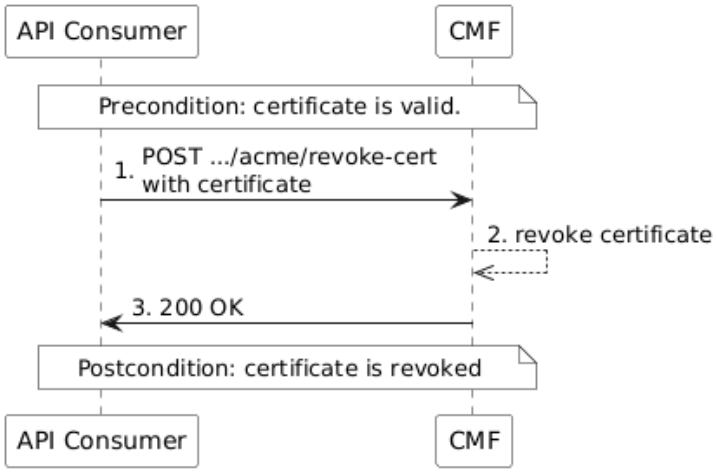

Figure 5.3.4a-1: Flow of the revocation of a Certificate resource

Precondition: The Certificate is valid.

The procedure consists of the following steps as illustrated in figure 5.3.4a-1:

1) API consumer sends a POST request to the revocation URI including in the message content a data structure of type "JWS".

2) The CMF revokes the certificate.

3) The CMF returns a "200 OK" response without content.

Postcondition: The Certificate is revoked.

Error handling: In the case where certificate is not available, such as certificate is expired, appropriate error information is provided in the response.

5.3.5 Flow of the Query of the subject for VNFC/VNF OAM certificate management

This clause describes a sequence for Querying/reading information about a Subject instance.

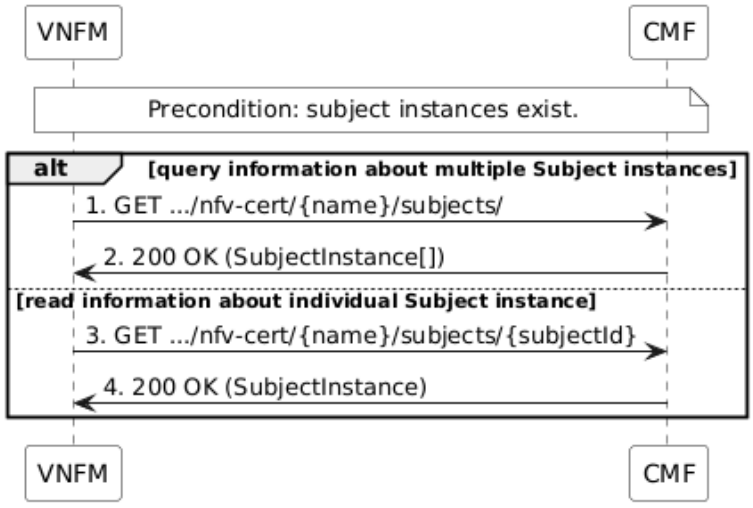

Figure 5.3.5-1: Flow of the query of a Subject resource

Precondition: One or more resources representing the Subject instance are available.

The procedure consists of the following steps as illustrated in figure 5.3.5-1:

1) If the VNFM intends to query all Subject instances, it sends a GET request to the "Subject instances" resource.

2) The CMF returns a "200 OK" response to the VNFM and includes zero or more data structures of type "SubjectInstance" in the message content.

3) If the VNFM intends to read information about a particular Subject instance, it sends a GET request to the "Individual Subject instance" resource, addressed by the appropriate Subject instance identifier in its resource URI.

4) The CMF returns a "200 OK" response to the VNFM and includes one data structure of type "SubjectInstance" in the message content.

Error handling: In case of failure, appropriate error information is provided in the response.

5.3.5a Flow of the Query of the Subject for MANO certificate management

This clause describes a sequence for reading information about a "Account" resource as Subject.

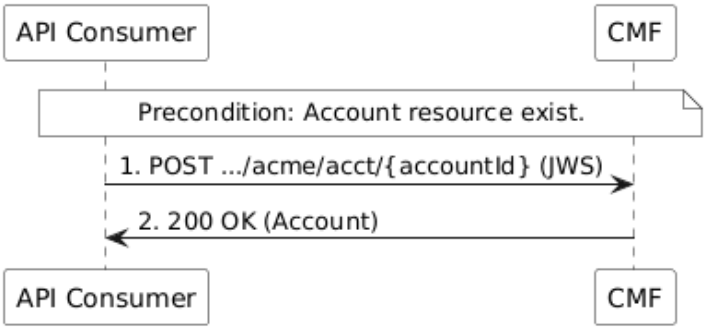

Figure 5.3.5a-1: Flow of the query of an "Account" resource

Precondition: "Account" resource is available.

The procedure consists of the following steps as illustrated in figure 5.3.5a-1:

1) If the API consumer intends to read information about a particular Account resource, it sends a POST-as-GET request with JWS to the "Account" resource, addressed by the appropriate "Account" resource identifier in its resource URI.

2) The CMF returns a "200 OK" response to the API consumer and includes one data structure of type "Account" in the message content.

Error handling: In case of failure, appropriate error information is provided in the response.

5.3.6 Flow of the Query of the certificate for VNFC/VNF OAM certificate management

This clause describes a sequence for Querying/reading information about a certificate.

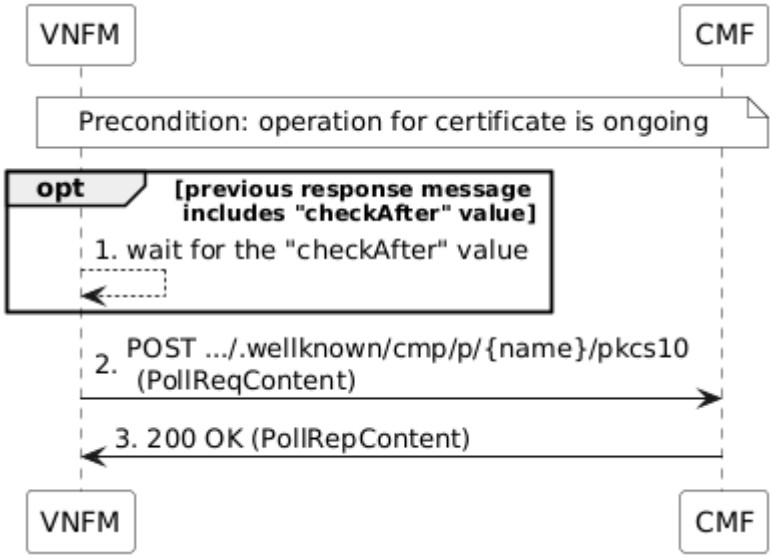

Figure 5.3.6-1: Flow of the query of a Certificate resource

Precondition: The operation for the certificate is ongoing.

The procedure consists of the following steps as illustrated in figure 5.3.6-1:

1) If the VNFM intends to query the status of operation for the certificate, the VNFM waits for the "checkAfter" values of previous message.

2) The VNFM sends a POST request to the pkcs10 URI including in the message content a data structure of type "PollReqContent".

3) The CMF returns a "200 OK" response to the VNFM containing the message content a data structures of type "PollRepContent".

Error handling: In case of failure, appropriate error information is provided in the response.

5.3.6a Flow of the Query of the certificate for MANO certificate management

This clause describes a sequence for reading information about an "Order" resource as certificate.

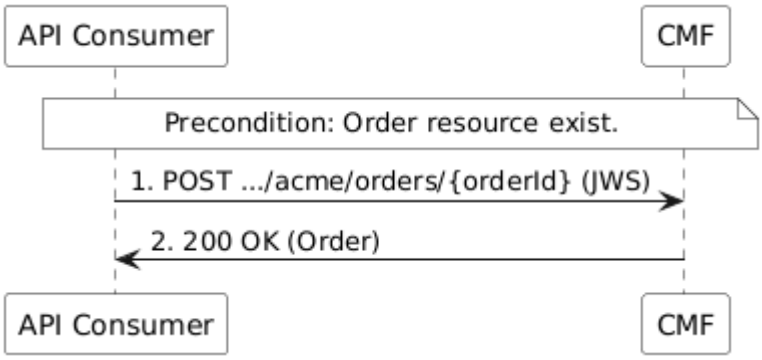

Figure 5.3.6a-1: Flow of the query of an "Order" resource

Precondition: Order resource is available.

The procedure consists of the following steps as illustrated in figure 5.3.6a-1:

1) If the API consumer intends to read information about a particular Order resource, it sends a POST-as-GET request with JWS to the Order resource, addressed by the appropriate Order resource identifier in its resource URI.

2) The CMF returns a "200 OK" response to the API consumer containing the message content a data structures of type Order.

Error handling: In case of failure, appropriate error information is provided in the response.

5.4 URI structure and methods

URI paths of the API for certificate related will use the base URI specification defined in clause 6.1 of IETF RFC 9483 [9]. The URI paths in clauses below are defined relative to the above base URI. Figure 5.4-1 shows the overall URI structure defined for the Certificate Management interface of certificate related.

URI paths of the API for subject related shall use the base URI specification defined in clause 4.1 of ETSI GS NFV-SOL 013 [4]. The string "nfv-cert" shall be used to represent {apiName}. The URIs in clauses below are defined relative to the above base URI. Figure 5.4-2 defines the URI structure for Certificate Management interface of subject related.

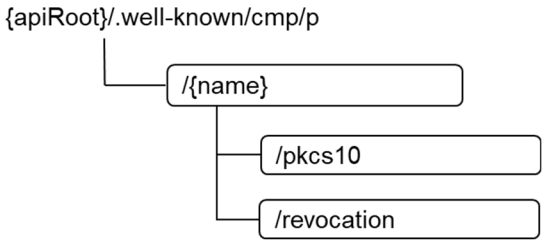

Figure 5.4-1: Resource URI structure of the Certificate Management interface for certificate related

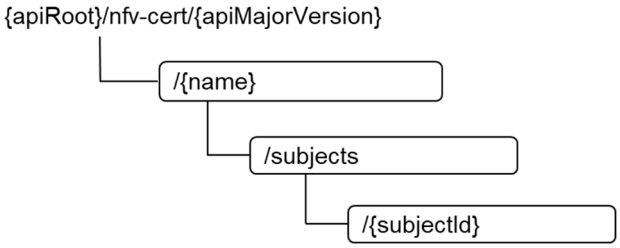

Figure 5.4-2: Resource URI structure of the Certificate Management interface for subject related

Table 5.4-1 lists the URI paths, and the applicable HTTP methods as defined in clause 6.1 of IETF RFC 9483 [9] and IETF RFC 6712 [12] and the present document. Table B.2-1 provides information about the mapping between these HTTP methods and operations as defined in ETSI GS NFV-IFA 033 [2]. {name} is certificate type as follows:

- vnfci-certificate
- vnfoam-certificate

The CMF will respond to requests for all HTTP methods on the URIs in table 5.4-1.

Table 5.4-1: URIs and methods overview of the Certificate Management interface

URI	HTTP Method	Meaning
/.wellknown/cmp/p/{name}/pkcs10	POST	Certificate Signing Request for VNFCI certificate and VNF OAM certificate
/.wellknown/cmp/p/{name}/revocation	POST	Revoke VNFCI certificate and VNF OAM certificate
/nfv-cert/{name}/subjects	GET	Query multiple Subject instances
	POST	Register subject as end entity
/nfv-cert/{name}/subjects/{subjectId}	GET	Read an "Individual Subject" resource
	DELETE	De-Register subject as end entity

5.5 Input/Output parameter mapping between NFV data model and profiled solution data models

5.5.1 Introduction

This clause provides the mapping of the CMP protocol input/output parameters for VNFC/VNF OAM certificate management and for the following operations to be profiled by CMP as per clause 5.2:

- Certificate Signing Request; and
- Revoke operation.

The protocol CMP has the structure of "PKIMessage", which includes "PKIHeader" and "PKIBody". The "parameter" of "PKIBody" indicates the type of "operation" for the supported profiled operations.

This clause also provides the mapping of the ACME protocol input/output parameters for MANO certificate management and for the following operations to be profiled by ACME as per clause 5.2:

- Account Creation;
- Certificate Issuance;
- Account Deactivation; and
- Certificate Revocation.

5.5.2 Input parameters to Certificate Management interfaces for VNFC/VNF OAM certificate management

5.5.2.1 Introduction

This clause specifies principal mapping of the CMP protocol input parameters and Certificate Management interfaces for the interfaces defined in ETSI GS NFV-IFA 033 [2] with considering CMP principles, used over the Cm-Vnfm reference point.

5.5.2.2 CMP PKIMessage structure

Table 5.5.2.2-1 indicates CMP PKIMessage structure.

Table 5.5.2.2-1: CMP PKIMessage structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
header	(Not applicable)	(Not applicable)	Data type of PKIHeader. The common part of PKI messages.
body	(Not applicable)	(Not applicable)	Data type of PKIBody. This contains message-specific information.
protection	(Not applicable)	(Not applicable)	Data type of PKIProtection. If used, contains bits that protect the PKI message.
extraCerts	(Not applicable)	(Not applicable)	Data type of SEQUENCE SIZE of CMPCertificate.

5.5.2.3 CMP PKIHeader structure

Table 5.5.2.3-1 indicates CMP PKIHeader structure.

Table 5.5.2.3-1: CMP PKIHeader structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
pvno	(Not applicable)	(Not applicable)	Protocol Version Number. Fixed value "2" shall be set.
sender	(Not applicable)	(Not applicable)	Name of the sender of the Request.
recipient	(Not applicable)	(Not applicable)	Name of the recipient of the Request.
messageTime	(Not applicable)	(Not applicable)	Time of production of this message.
protectionAlg	(Not applicable)	(Not applicable)	Algorithm used for calculation of protection bits.
senderKID	(Not applicable)	(Not applicable)	The value of the SubjectKeyIdentifier if present in the CMP protection certificate.
recipKID	(Not applicable)	(Not applicable)	To identify specific keys used for protection
transactionID	(Not applicable)	(Not applicable)	Identifies the transaction.
senderNonce	(Not applicable)	(Not applicable)	Cryptographically secure and fresh 128 random bits.
recipNonce	(Not applicable)	(Not applicable)	The value of the senderNonce of the previous message in the same transaction.
freeText	(Not applicable)	(Not applicable)	Context-specific instructions.
generalInfo	certType (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)	(Not applicable)	It shall contain two of the attributes. The first generalIInfo shall contain the set of: • InfoType for Certificate type • Infovalue for Choice of or VNFC or VNF OAM Unless the InfoValue of the first generalIInfo is MANO, the second generalIInfo shall contain the set of: • InfoType for Type of VNFC certification handling • Infovalue for Choice of direct or delegation
>infoType	certType (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)	(Not applicable)	Indicate the type of Info. The namespaces and conventions for the values of this attribute that is OID defined as clause 5.7. Permit values: • Certification type • Type of VNFC certification handling

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
>infoValue	certType (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)	"certificateType" in CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44), for the case of "InfoType" is "Certification type" "certificate_base_profile" of properties in tosca.nodes.nfv.Certificate (ETSI GS NFV-SOL 001 [11], clause 6.8.19) for the case of "InfoType" is "Type of VNFC certification handling"	If the value of "InfoType" is "Certification type", it shall be set. Permit values: • VNFCI certificate • VNF OAM certificate If the value of "InfoType" is "Type of VNFC certification handling", it shall be set. Permit values: • Direct mode • Delegation mode Only the value "Delegation mode" is allowed for this version of the present document.

5.5.2.4 CMP PKIBody structure

Table 5.5.2.4-1 indicates CMP PKIBody structure.

Table 5.5.2.4-1: CMP PKIBody structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
ir [0] CertReqMessages, --Initialization Req	(Not applicable)	-	-
ip [1] CertRepMessage, --Initialization Resp	(Not applicable)	-	-
cr [2] CertReqMessages, --Certification Req	(Not applicable)	-	-
cp [3] CertRepMessage, --Certification Rep	certificate (ETSI GS NFV-IFA 033 [2], clause 11.2.3.3)	CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	PKIBody a CertRepMessage data structure.
p10cr [4] CertificationRequest, --PKCS #10 Cert. Req.	csr (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2)	CertificateBaseProfile (ETSI GS NFV-SOL 002 [3], clause 5.5.3.39)	CertificationRequestInfo data structure, as specified in PKCS #10 IETF RFC 2986 [8].
popdecc [5] POPODecKeyChallContent --pop Challenge	(Not applicable)	-	-
popdecr [6] POPODecKeyRespContent, --pop Response	(Not applicable)	-	-
kur [7] CertReqMessages, --Key Update Request	(Not applicable)	-	-
kup [8] CertRepMessage, --Key Update Response	(Not applicable)	-	-
krr [9] CertReqMessages, --Key Recovery Req	(Not applicable)	-	-
krp [10] KeyRecRepContent, --Key Recovery Resp	(Not applicable)	-	-
rr [11] RevReqContent, --Revocation Request	CertificateId (ETSI GS NFV-IFA 033 [2], clause 11.2.5.2)	(Not applicable)	When requesting revocation of a certificate (or several certificates), this data structure is used.
rp [12] RevRepContent, --Revocation Response	Operation results (ETSI GS NFV-IFA 033 [2], clause 11.2.5.4)	(Not applicable)	The revocation response is the response to the revocation request message. If produced, this is sent to the requester of the revocation.
ccr [13] CertReqMessages, --Cross-Cert. Request	(Not applicable)	-	-
ccp [14] CertRepMessage, --Cross-Cert. Resp	(Not applicable)	-	-

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
ckuann [15] CAKeyUpdAnnContent, --CA Key Update Ann.	(Not applicable)	-	-
cann [16] CertAnnContent, --Certificate Ann.	(Not applicable)	-	-
rann [17] RevAnnContent, --Revocation Ann.	(Not applicable)	-	-
crlann [18] CRLAnnContent, --CRL Announcement	(Not applicable)	-	-
pkiconf [19] PKIConfirmContent, --Confirmation	(Not applicable)	-	-
nested [20] NestedMessageContent, --Nested Message	(Not applicable)	-	-
genm [21] GenMsgContent, --General Message	(Not applicable)	-	-
genp [22] GenRepContent, --General Response	(Not applicable)	-	-
error [23] ErrorMsgContent, --Error Message	(Not applicable)	-	
certConf [24] CertConfirmContent, --Certificate confirm	(Not applicable)	-	-
pollReq [25] PollReqContent, --Polling request	(Not applicable)	-	-
pollRep [26] PollRepContent --Polling response	(Not applicable)	-	-

5.5.2.5 CMP Certification Request structure

Table 5.5.2.5-1 indicates CMP Certificate Request structure.

Table 5.5.2.5-1: CMP Certification Request structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
certificationRequestInfo	csr (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)	CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	The request of the EE for a new certificate using a PKCS #10 certificate request.
>version			Version number of this request. "0" is PKCS #10 v1.7.
>subject			Distinguished name of the certificate subject.
>subjectPKInfo			Information of public key of this certificate.
>>algorithm			Algorithm of this certificate's public key.
>>subjectPublicKey			Public key of this certificate.
>attributes			Extension of this certificate. The subjectAltName extension will be present if the subject name includes a subject alternative name.
signatureAlgorithm	(Not applicable)		Algorithm of this certificate's signature.
signature	(Not applicable)	(Not applicable)	Self-signature for proof-of-possession.

5.5.2.6 CMP Revocation Request structure

Table 5.5.2.6-1 indicates CMP RevReqContent structure.

Table 5.5.2.6-1: CMP RevReqContent structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
certDetails	(Not applicable)	CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	Allows the requester to specify as much as they can about the cert for which revocation is requested defined as CertTemplate in clause 5 of IETF RFC 4211 [10].
>version	(Not applicable)		Version of this certificate.
>serialNumber	(Not applicable)		Serial number of this certificate.
>signingAlg	(Not applicable)		Algorithm of this certificate's signature.
>issuer	(Not applicable)		Issuer of this certificate.
>validity	(Not applicable)		valid period for this certificate.
>>notBefore	(Not applicable)		Start date of valid period for this certificate.
>>notAfter	(Not applicable)		End date of valid period for this certificate.
>subject	(Not applicable)		Subject of this certificate.
>publicKey	(Not applicable)		Public key of this certificate.
>issuerUID	(Not applicable)		Unique ID of issuer. This field has been deprecated as IETF RFC 9810 [13].
>subjectUID	(Not applicable)		Unique ID of subject. This field has been deprecated as IETF RFC 9810 [13].
>extensions	(Not applicable)		Extension of this certificate.
crlEntryDetails	(Not applicable)	(Not applicable)	New CRL entry.

5.5.2a Input parameters to Certificate Management interfaces for MANO certificate management

5.5.2a.1 Introduction

This clause specifies the mapping of the ACME protocol input parameters and Certificate Management interfaces for the interfaces defined in ETSI GS NFV-IFA 033 [2] considering ACME principles, used over the Cm-Vnfm reference point.

5.5.2a.2 ACME Account Creation

Table 5.5.2a.2-1 describes ACME account creation structure, by sending POST method on "newAccount" resource.

Table 5.5.2a.2-1: ACME Account Creation by sending POST method on "newAccount" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.
>contact	subjectName (ETSI GS NFV-IFA 033 [2], clause 11.2.2.2-1)	CerrtSubjectData (ETSI GS NFV-SOL 002 [3], clause 5.5.3.31)	An array of URLs that the server uses to contact the client for issues related to this account. The server may notify the client about server-initiated revocation or certificate expiration.
>termsOfServiceAgreed	(Not applicable)	(Not applicable)	A value of true, indicates the client's agreement with the terms of service. This field cannot be updated by the client.
>onlyReturnExisting	(Not applicable)	(Not applicable)	If this field is present with the value "true", then the server does not create a new account if one does not already exist. This allows a client to look up an account URL based on an account key.
>externalAccountBinding	(Not applicable)	(Not applicable)	Indicates approval by the holder of an existing non-ACME account to bind that account to this ACME account. This field cannot be updated by the client.
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.

5.5.2a.3 ACME Certificate Issuance

Table 5.5.2a.3-1 describes ACME Certificate Issuance structure, by sending POST method on "newOrder" resource.

Table 5.5.2a.3-1: ACME Certificate Issuance by sending POST method on "newOrder" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS. See note.
>kid	(Not applicable)	(Not applicable)	The account URL received by POSTing to the newAccount resource. See note.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.
>identifiers	subjectId (ETSI GS NFV-IFA 033 [2], clause 11.2.2.2-1)	CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	An array of identifier objects that the client requests to submit an order for.
>>type			The type of identifier.
>>value			The value of the identifier.
>notBefore	csr (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)		value of the notBefore field in the certificate.
>notAfer			value of the notAfter field in the certificate.
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.
NOTE: Either "jwk" parameter or "kid" parameter shall be included.			

Table 5.5.2a.3-2 describes ACME Certificate Issuance structure, by sending POST method on "finalize" resource.

Table 5.5.2a.3-2: ACME Certificate Issuance by sending POST method on "finalize" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS. See note.
>kid	(Not applicable)	(Not applicable)	The account URL received by POSTing to the newAccount resource. See note.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
>csr	csr (ETSI GS NFV-IFA 033 [2], clause 11.2.3.2-1)	CertificateBaseProfile (ETSI GS NFV-SOL 002 [3], clause 5.5.3.39)	A CSR encoding the parameters for the certificate being requested. The CSR is sent in the base64url-encoded version of the DER format.
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.
NOTE: Either "jwk" parameter or "kid" parameter shall be included.			

Table 5.5.2a.3-3 describes ACME Certificate Issuance structure, by sending POST method on "certificate" resource.

Table 5.5.2a.3-3: ACME Certificate Issuance by sending POST method on "certificate" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS. See note.
>kid	(Not applicable)	(Not applicable)	The account URL received by POSTing to the newAccount resource. See note.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.
>"(blank)"	(Not applicable)	(Not applicable)	Sending POST on "certificate" resource with payload blank downloads the issued certificate.
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.
NOTE: Either "jwk" parameter or "kid" parameter shall be included.			

5.5.2a.4 ACME Account Deactivation

Table 5.5.2a.4-1 describes ACME Account Deactivation structure, by sending POST method on "account" resource.

Table 5.5.2a.4-1: ACME Account Deactivation by sending POST method on "account" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS. See note.
>kid	(Not applicable)	(Not applicable)	The account URL received by POSTing to the newAccount resource. See note.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.
>status	(Not applicable)	(Not applicable)	A client deactivates an account by posting a signed update to the account URL with a status field of "deactivated".
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.
NOTE: Either "jwk" parameter or "kid" parameter shall be included.			

5.5.2a.5 ACME Certificate Revocation

Table 5.5.2a.5-1 describes ACME Certificate Revoke structure, by sending POST method on "revokeCert" resource.

Table 5.5.2a.5-1: ACME Certificate Revoke by sending POST method on "revokeCert" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
protected	(Not applicable)	(Not applicable)	JSON Web Signature (JWS) protected header.
>alg	(Not applicable)	(Not applicable)	This field shall not contain "none" or a Message Authentication Code (MAC) algorithm.
>jwk	(Not applicable)	(Not applicable)	The public key corresponding to the private key used to sign the JWS.
>nonce	(Not applicable)	(Not applicable)	The unique value that enables the verifier of a JWS to recognize when replay has occurred. It shall be an octet string, encoded according to the base64url encoding. If the value of a "nonce" header parameter is not valid according to this encoding, then the verifier shall reject the JWS as malformed.
>url	(Not applicable)	(Not applicable)	The URL to which this JWS object is directed. The value of the "url" header parameter shall be a string representing the target URL.
payload	(Not applicable)	(Not applicable)	Payload in a JSON Web Signature (JWS) object, signed using the account's private key.
>certificate	certificate (ETSI GS NFV-IFA 033 [2], clause 11.2.3.3-1)	"serialNumber" in CertificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	The certificate to be revoked, in the base64url-encoded version of the DER format.
>reason	(Not applicable)	(Not applicable)	One of the revocation reasonCodes to be used when generating OCSP responses and CRLs. If this field is not set, the server should omit the reasonCode CRL entry extension when generating OCSP responses and CRLs.
signature	(Not applicable)	(Not applicable)	The MAC value computed with the MAC key provided by the producer.

5.5.3 Output parameters to Certificate Management interfaces for VNFC/VNF OAM certificate management

5.5.3.1 Introduction

Clause 5.5.3 specifies principal mapping of the CMP protocol output parameters and Certificate Management interfaces for the interfaces defined in ETSI GS NFV-IFA 033 [2] with considering CMP principles, used over the Cm-Vnfm reference point.

5.5.3.2 CMP CertRepMessage structure

Table 5.5.3.2-1 indicates CMP CertRepMessage structure.

Table 5.5.3.2-1: CMP CertRepMessage structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
caPubs	(Not applicable)	"certificateChain" in CmfInfo (ETSI GS NFV-SOL 002 [3], clause 5.5.3.45)	A trust anchor, e.g. root certificate, of the certificate contained in certOrEncCert when the certifiedKeyPair field is present.
response	(Not applicable)	(Not applicable)	CertResponse message.
>certReqId	(Not applicable)	(Not applicable)	Will be set "0".
>status	(Not applicable)	(Not applicable)	PKIStatusInfo structure specified in clauses 3.6.4 and 4 of IETF RFC 9483 [9] will be present.
>>status	(Not applicable)	(Not applicable)	Status of this certificate. Allowed values: • "accepted" • "grantedWithMods" • "rejection"
>>statusString	(Not applicable)	(Not applicable)	Human-readable text.
>>failInfo	(Not applicable)	(Not applicable)	Will be absent when "status" is "accepted" or "grantedWithMods".
>certifiedKeyPair	(Not applicable)	(Not applicable)	Will be present when "status" is "accepted" or "grantedWithMods".
>>certOrEncCert	(Not applicable)	(Not applicable)	Will be present when status is "accepted" or "grantedWithMods".
>>>certificate	certificate (clause 11.2.3.3-1 of ETSI GS NFV-IFA 033 [2])	certificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	newly enrolled X.509 certificate.
>>>encryptedCert	(Not applicable)	(Not applicable)	EncryptedKey.
>>privatekey	(Not applicable)	(Not applicable)	Will be absent when local key generation or "status" is "rejection".
>>publicationInfo	(Not applicable)	(Not applicable)	Action indicates whether or not the requestor wishes the CA/RA to publish the certificate defined for PKIpublicationInfo in clause 6.3 of IETF RFC 4211 [10].
>rspInfo	(Not applicable)	(Not applicable)	analogous to the id-regInfo-utf8Pairs string defined for regInfo of CertReqMsg in clause 7.1 of IETF RFC 4211 [10].

5.5.3.3 CMP Revocation Response structure

Table 5.5.3.3-1 indicates CMP RevRepContent structure.

Table 5.5.3.3-1: CMP RevReqContent structure

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
status	(Not applicable)	(Not applicable)	PKIStatusInfo structure specified in clauses 3.6.4 and 4 of IETF RFC 9483 [9] will be present.
>status	(Not applicable)	(Not applicable)	Status of this certificate. Allowed values: • "accepted"; • "grantedWithMods"; • "rejection".
>statusString	(Not applicable)	(Not applicable)	Human-readable text.
>failInfo	(Not applicable)	(Not applicable)	Will be absent when "status" is "accepted" or "grantedWithMods".
revCerts	(Not applicable)	(Not applicable)	IDs for which revocation was requested.
crls	(Not applicable)	(Not applicable)	the resulting CRLs.

5.5.3a Output parameters to Certificate Management interfaces for MANO certificate management

5.5.3a.1 Introduction

Clause 5.5.3a specifies the mapping of the ACME protocol output parameters and Certificate Management interfaces for the interfaces defined in ETSI GS NFV-IFA 033 [2] considering ACME principles, used over the Cm-Vnfm reference point.

5.5.3a.2 ACME Account Creation

Table 5.5.3a.2-1 describes ACME account creation response.

Table 5.5.3a.2-1: ACME Account Creation response

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
status	(Not applicable)	(Not applicable)	The status of the account resource.
contact	(Not applicable)	(Not applicable)	An array of URLs that the server uses to contact the client for issues related to this account. The server may notify the client about server-initiated revocation or certificate expiration.
orders	(Not applicable)	(Not applicable)	A URL from which a list of orders submitted by this account can be fetched via a POST-as-GET request.

5.5.3a.3 ACME Certificate Issuance

Table 5.5.3a.3-1 describes ACME Certificate Issuance response.

Table 5.5.3a.3-1: ACME Certificate Issuance response for new order

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
status	(Not applicable)	(Not applicable)	The status of the authorization transaction that the client shall complete before certificate issuance.
expires	(Not applicable)	(Not applicable)	Time of valid period that the client shall complete authorization transaction for any authorization referenced in the authorizations parameter. If the client failrs to complete required authorization before the expires time, the server changes the status of the order to invalid and may delete that order resource.
notBefore	(Not applicable)	(Not applicable)	value of the notBefore field in the certificate.
notAfter	(Not applicable)	(Not applicable)	value of the notAfter field in the certificate.
identifiers	(Not applicable)	(Not applicable)	An array of identifier objects.
>type	(Not applicable)	(Not applicable)	The type of identifier.
>value	(Not applicable)	(Not applicable)	The value of the identifier.
authorizations	(Not applicable)	(Not applicable)	Authorizations resources. If status is pending, all of authorizations shall be completed before issuing.
finalize	(Not applicable)	(Not applicable)	Finalize resource to proceed the process.

Table 5.5.3a.3-2 describes ACME Certificate Issuance response.

Table 5.5.3a.3-2: ACME Certificate Issuance response for finalize

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
status	(Not applicable)	(Not applicable)	The status of the order resource to describe client next action.
expires	(Not applicable)	(Not applicable)	Time shown in response for new order.
notBefore	(Not applicable)	(Not applicable)	value of the notBefore field in the certificate.
notAfter	(Not applicable)	(Not applicable)	value of the notAfter field in the certificate.
identifiers	(Not applicable)	(Not applicable)	An array of identifier objects.
>type	(Not applicable)	(Not applicable)	The type of identifier.
>value	(Not applicable)	(Not applicable)	The value of the identifier.
authorizations	(Not applicable)	(Not applicable)	URL to the completed authorizations resource.
finalize	(Not applicable)	(Not applicable)	URL to this specific finalize resource.
certificate	(Not applicable)	(Not applicable)	URL to the issued certificate to download.

Table 5.5.3a.3-3 describes ACME Certificate Issuance response.

Table 5.5.3a.3-3: ACME Certificate Issuance response for certificate

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
certificate	certificate (ETSI GS NFV-IFA 033[2], clause 11.2.3.3-1)	certificateContent (ETSI GS NFV-SOL 002 [3], clause 5.5.3.44)	Newly issued X.509 certificate.

5.5.3a.4 ACME Account Deactivation

Table 5.5.3a.4-1 describes ACME Account Deactivation response.

Table 5.5.3a.4-1: ACME Account Deactivation by sending post method on "account" resource

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
account	(Not applicable)	(Not applicable)	The current contents of the account object.

5.5.3a.5 ACME Certificate Revocation

Table 5.5.3a.5-1 describes ACME Certificate Revocation response.

Table 5.5.3a.5-1: ACME Certificate Revocation response

Parameter	Mapped IFA033 parameter	Mapped NFV data element/attribute	Description
None	(Not applicable)	(Not applicable)	-

5.6 Additional features

5.6.1 Description

This clause provides additional NFV specification based on ETSI NFV-SOL 013 [4] on top of the profiled solutions against CMP as specified in IETF RFC 9810 [13] and IETF RFC 9811 [14].

5.6.2 Version

For the Certificate Management interface version as specified in the present document, the MAJOR version field shall be 1, the MINOR version field shall be 0 and the PATCH version field shall be 0 (see clause 9.1 of ETSI GS NFV-SOL 013 [4] for a definition of the version fields). Consequently, the {apiMajorVersion} URI variable shall be set to "v1".

5.6.3 Resources

5.6.3.1 Introduction

5.6.3.1.1 Overview

Clause 5.6.3 defines all the resources and methods provided by the Certificate management interface.

5.6.3.1.2 Task resources that trigger Certificate Management operations

A number of resources are defined as task resources to trigger Certificate Management operations.

5.6.3.2 Resource: API versions

The "API versions" resources as defined in clause 9.3.3 of ETSI GS NFV-SOL 013 [4] are part of the Certificate management interface.

5.6.3.3 Resource: Subject

5.6.3.3.1 Description

This resource represents the subject as end entity. The API consumer can use this resource to create individual subject identifier.

5.6.3.3.2 Resource definition

The resource URI is:

{apiRoot}/nfv-cert/{apiMajorVersion}/subjects

This resource shall support the resource URI variables defined in table 5.6.3.3.2-1.

Table 5.6.3.3.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See clause 4.1 of ETSI GS NFV-SOL 013 [4].
apiMajorVersion	See clause 5.6.2.

5.6.3.3.3 Resource methods

5.6.3.3.3.1 POST

The POST method creates a new subject resource.

This method shall follow the provisions specified in tables 5.6.3.3.3.1-1 and 5.6.3.3.3.1-2 for URI query parameters, request and response data structures, and response codes.

As the result of successfully executing this method, a new "Individual Subject" resource as defined in clause 5.6.3.4 shall have been created.

Table 5.6.3.3.3.1-1: URI query parameters supported by the POST method on this resource

Name	Cardinality	Description
none supported		

Table 5.6.3.3.3.1-2: Details of the POST request/response on this resource

Request body	Data type	Cardinality	Description	
	RegistrationRequest	1	Parameters for the Register, as defined in clause 5.6.4.2.3	
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	SubjectInstance	1	201 Created	Shall be returned when a new "Individual Subject instance" resource and the associated Subject instance identifier has been created successfully. The response body shall contain a representation of the created Subject instance, as defined in clause 5.6.4.2.2. The HTTP response shall include a "Location" HTTP header that contains the resource URI of the created Subject instance.
	ProblemDetails	1	409 Conflict	Shall be returned upon the following error: The operation cannot be executed currently, due to a conflict with the state of the resource. The response body shall contain a ProblemDetails structure, in which the "detail" attribute shall convey more information about the error.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

5.6.3.3.3.2 GET

The GET method queries information about multiple subject instances.

This method shall follow the provisions specified in tables 5.6.3.3.3.2-1 and 5.6.3.3.3.2-2 for URI query parameters, request and response data structures, and response codes.

Table 5.6.3.3.3.2-1: URI query parameters supported by the GET method on this resource

Name	Cardinality	Description
Filter	0..1	Attribute-based filtering expression according to clause 5.2 of ETSI GS NFV-SOL 013 [4]. The CMF shall support receiving this parameter as part of the URI query string. The VNFM may supply this parameter. All attribute names that appear in the SubjectInstance and in data types referenced from it shall be supported by the CMF in the filter expression.
all_fields	0..1	Include all complex attributes in the response. See clause 5.3 of ETSI GS NFV-SOL 013 [4] for details. The CMF shall support this parameter.
Fields	0..1	Complex attributes to be included into the response. See clause 5.3 of ETSI GS NFV-SOL 013 [4] for details. The CMF should support this parameter.
exclude_fields	0..1	Complex attributes to be excluded from the response. See clause 5.3 of ETSI GS NFV-SOL 013 [4] for details. The CMF should support this parameter.
exclude_default	0..1	Indicates to exclude the following complex attributes from the response. See clause 5.3 of ETSI GS NFV-SOL 013 [4] for details. The CMF shall support this parameter. The following attributes shall be excluded from the SubjectInstance structure in the response body if this parameter is provided, or none of the parameters "all_fields", "fields", "exclude_fields", "exclude_default" are provided: • subjectId.
nextpage_opaque_marker	0..1	Marker to obtain the next page of a paged response. Shall be supported by the CMF if the CMF supports alternative 2 (paging) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource.

Table 5.6.3.3.3.2-2: Details of the GET request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	SubjectInstance	0..N	200 OK	Shall be returned when information about zero or more subject instances has been queried successfully. The response body shall contain in an array the representations of zero or more subject instances, as defined in clause 5.6.4.2.2. If the "filter" URI parameter or one of the "all_fields", "fields" (if supported), "exclude_fields" (if supported) or "exclude_default" URI parameters was supplied in the request, the data in the response body shall have been transformed according to the rules specified in clauses 5.2.2 and 5.3.2 of ETSI GS NFV-SOL 013 [4], respectively. If the CMF supports alternative 2 (paging) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource, inclusion of the Link HTTP header in this response shall follow the provisions in clause 5.4.2.3 of ETSI GS NFV-SOL 013 [4].
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute-based filtering expression. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute selector. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Response too big. If the CMF supports alternative 1 (error) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource, this error response shall follow the provisions in clause 5.4.2.2 of ETSI GS NFV-SOL 013 [4].
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

5.6.3.3.3 PUT

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.3.4 PATCH

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.3.5 DELETE

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.4 Resource: Individual Subject

5.6.3.4.1 Description

This resource represents an individual Subject instance. The API consumer can use this resource to modify and delete the underlying Subject instance, and to read information about the Subject instance.

5.6.3.4.2 Resource definition

The resource URI is:

{apiRoot}/nfv-cert/{apiMajorVersion}/subjects/{subjectId}

This resource shall support the resource URI variables defined in table 5.6.3.4.2-1.

Table 5.6.3.4.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See clause 4.1 of ETSI GS NFV-SOL 013 [4].
apiMajorVersion	See clause 5.6.2.
subjectId	Identifier of the Subject instance. See note.
NOTE: This identifier can be retrieved from the resource referenced by the "Location" HTTP header in the response to a POST request creating a new "Individual Subject instance" resource. It can also be retrieved from the "id" attribute in the message content of that response.	

5.6.3.4.3 Resource methods

5.6.3.4.3.1 POST

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.4.3.2 GET

The GET method retrieves information about a Subject instance by reading an "Individual Subject instance" resource.

This method shall follow the provisions specified in tables 5.6.3.4.3.2-1 and 5.6.3.4.3.2-2 for URI query parameters, request and response data structures, and response codes.

Table 5.6.3.4.3.2-1: URI query parameters supported by the GET method on this resource

Name	Cardinality	Description
none supported		

Table 5.6.3.4.3.2-2: Details of the GET request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response codes**	**Description**
	SubjectInstance	1	200 OK	Shall be returned when information about an individual Subject instance has been read successfully. The response body shall contain a representation of the Subject instance, as defined in clause 5.6.4.2.2.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

5.6.3.4.3.3 PUT

This method is not supported. When this method is requested on this resource, the VNFM shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.4.3.4 PATCH

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

5.6.3.4.3.5 DELETE

This method deletes an "Individual Subject instance" resource.

This method shall follow the provisions specified in tables 5.6.3.4.3.5-1 and 5.6.3.4.3.5-2 for URI query parameters, request and response data structures, and response codes.

As the result of successfully executing this method, the "Individual Subject instance" resource shall not exist any longer.

Table 5.6.3.4.3.5-1: URI query parameters supported by the DELETE method on this resource

Name	Cardinality	Description
none supported		

Table 5.6.3.4.3.5-2: Details of the DELETE request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	n/a		204 No Content	Shall be returned when the "Individual Subject instance" resource and the associated Subject identifier were deleted successfully. The response body shall be empty.
	ProblemDetails	1	409 Conflict	Shall be returned upon the following error: The operation cannot be executed currently, due to a conflict with the state of the resource. Typically, this is due to the fact that not all certificates under the "Individual Subject instance" are either expired or have been revoked. The response body shall contain a ProblemDetails structure, in which the "detail" attribute shall convey more information about the error.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

5.6.4 Data model

5.6.4.1 Introduction

This clause defines the request and response data structures of the Certificate management interface. If a request or response contains attributes not defined in the present document, a receiving functional block that does not understand these attributes shall not treat their presence as an error and may choose to ignore them.

5.6.4.2 Resource and notification data types

5.6.4.2.1 Introduction

This clause defines the data structures to be used in resource representations and notifications.

5.6.4.2.2 Type: SubjectInstance

This type represents a subject instance. It shall comply with the provisions defined in table 5.6.4.2.2-1.

Table 5.6.4.2.2-1: Definition of the SubjectInstance data type

Attribute name	Data type	Cardinality	Description
Id	Identifier	1	Identifier of the Subject instance.
certType	Enum	1	Indicate the type of target certificate. The possible values are (see note 1): • MANO_certificate • VNFCI_certificate • VNF_OAM_certificate
subjectId	Structure (inlined)	1..N	Data about subjects and their certificates that need to be registered. This attribute shall be present only if certType is VNFCI certificate or VNF OAM certificate.
>subjectId	Identifier	1	The value of the Identifier of the certificate target VNFCI as subject ID if this operation is used for the VNFCI certificate or VNF OAM certificate.
>certificateData	Structure (inlined)	1..N	Data related to certificates for the target VNFCI.
>>subjectName	CertSubjectData	0..1	Subject data of the of VNFCI certificates, i.e. certificate fields related to common name, organization, country, etc.
>>subjectAlternateName	String	1..N	Subject alternate names of VNFCI certificates.
typeOfVnfcCertHandling	Enum	1	This parameter shall be present only if certType is VNFCI certificate or VNF OAM certificate. It indicates the mode of certificate management for the target entity. The possible values are: • direct_mode; • delegation_mode. See note 2.
_links	Structure (inlined)	1	Links to resources related to this resource.
>self	Link	1	URI of this resource.
NOTE 1: Registration of target certificates of type 'MANO certificate' is not covered in this version of the present document. NOTE 2: At least one overriding attribute shall be present, otherwise shall be absent.			

5.6.4.2.3 Type: RegistrationRequest

This type represents request parameters for the "Register" operation as defined in ETSI GS NFV-IFA 033 [2]. It shall comply with the provisions defined in table 5.6.4.2.3-1.

Table 5.6.4.2.3-1: Definition of the RegistrationRequest data type

Attribute name	Data type	Cardinality	Description
certType	Enum	1	Indicate the type of target certificate. The possible values are (see note 1): • MANO_certificate • VNFCI_certificate • VNF_OAM_certificate
subjectId	Structure (inlined)	1..N	Data about subjects and their certificates that need to be registered. This attribute shall be present only if certType is VNFCI certificate or VNF OAM certificate.
>subjectId	Identifier	1	The value of the Identifier of the certificate target VNFCI as subject ID if this operation is used for the VNFCI certificate or VNF OAM certificate.

Attribute name	Data type	Cardinality	Description
>certificateData	Structure (inlined)	1..N	Data related to certificates for the target VNFCI.
>>subjectName	CertSubjectData	0..1	Subject data of the of VNFCI certificates, i.e. certificate fields related to common name, organization, country, etc.
>>subjectAlternateName	String	1..N	Subject alternate names of VNFCI certificates.
typeOfVnfcCertHandling	Enum	1	This parameter shall be present only if certType is VNFCI certificate or VNF OAM certificate. It indicates the mode of certificate management for the target entity. The possible values are: • direct_mode; • delegation_mode. See note 2.
NOTE 1: Registration of target certificates of type 'MANO certificate' is not covered in this version of the present document. NOTE 2: Only the value "delegation mode" is allowed for this version of the present document.			

5.6.4.3 Referenced structured data types

5.6.4.3.1 Introduction

This clause defines data structures that can be referenced from data structures defined in the previous clauses.

5.6.4.3.2 Type: CertSubjectData

This type provides input information related to subject of certificate. It shall comply with the provisions defined in table 5.6.4.3.2-1.

Table 5.6.4.3.2-1: Definition of the CertSubjectData data type

Attribute name	Data type	Cardinality	Description
commonName	String	0..1	Information of certification target subject FQDN. Can be set empty when this certificate is used for encrypted communication using IP address. See note.
organization	String	0..1	Information of certification target subject Organization. See note.
country	String	0..1	Information of certification target subject Country. See note.
state	String	0..1	Information of certification target subject State. See note.
locality	String	0..1	Information of certification target subject Locality. See note.
emailAddress	String	0..1	Information of certification contact email address. See note.
NOTE: At least one overriding attributes shall be present, otherwise shall be absent.			

5.6.4.4 Referenced simple data types and enumerations

5.6.4.4.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

5.6.4.4.2 Simple data types

The simple data types defined in clause 7.2.2 of ETSI GS NFV-SOL 013 [4] shall apply.

5.6.4.4.3 Enumerations

The enumerations defined in clause 7.2.3 of ETSI GS NFV-SOL 013 [4] shall apply.

5.7 OID consideration

5.7.1 Introduction

The following clauses define OID in "InfoType" and "InfoValue" attributes of "PkiHeader" as defined in clause 5.5.2.3. For each "InfoType" attribute, a standardized value for "InfoValue" attribute is defined.

5.7.2 Conventions for info type attribute

This clause defines namespaces and conventions for the values of the "InfoType" and "InfoValue". The following naming conventions for defining coordination action name strings apply:

1) The name of a public coordination action (i.e. one that is defined in a public document) shall be represented by a URN (see IETF RFC 8141 [7]) where the Namespace Identifier (NID) of the URN is registered to the organization that issues the public document and where the Namespace Specific String (NSS) indicates the name of the type of info unique within the scope defined by the NID.

2) Only alphanumeric characters and ".", "-", "_" should be used in the part of type of info following the NID or prefix.

3) An info type defined by ETSI shall be prefixed by "urn:etsi:", followed by an NSS-root registered in https://portal.etsi.org/PNNS/Generic-Allocation/ETSI-URN-Namespace, followed by a string documented in an ETSI specification.

4) A coordination action name string defined by ETSI NFV shall be prefixed by "urn:etsi:nfv:cert-type:" for certificate type and "urn:etsi:nfv:cert-type:handling:" for type of certificate handling, followed by a string documented in an ETSI NFV specification.

5.7.3 Certificate type

5.7.3.1 Introduction

This clause defines OID for each certificate types.

5.7.3.2 VNFCI Certificate

This certificate type allows the VNFM to request VNFCI certificate to CMF. The certificate type shall follow the provisions defined in table 5.7.3.2-1.

Table 5.7.3.2-1: Definition of values

Attribute name	Definition
InfoType	"urn:etsi:nfv:cert-type".
InfoValue	"urn:etsi:nfv:cert-type:vnfci-certificate" shall be the only allowed value.

5.7.3.3 VNF OAM Certificate

This certificate type allows the VNFM to request VNF OAM certificate to CMF. The certificate type shall follow the provisions defined in table 5.7.3.3-1.

Table 5.7.3.3-1: Definition of values

Attribute name	Definition
InfoType	"urn:etsi:nfv:cert-type".
InfoValue	"urn:etsi:nfv:cert-type:vnfoam-certificate" shall be the only allowed value.

5.7.4 Type of certificate handling

5.7.4.1 Introduction

This clause defines OID for each type of certificate handling.

5.7.4.2 Direct mode

This type of certificate handling allows the VNF to request certificate to CA directly. The type shall follow the provisions defined in table 5.7.4.2-1.

Table 5.7.4.2-1: Definition of values

Attribute name	Definition
InfoType	"urn:etsi:nfv:cert-type:handling".
InfoValue	"urn:etsi:nfv:cert-type:handling:direct" shall be the only allowed value.

5.7.4.3 Delegation mode

This type of certificate handling allows the VNFM to request certificate to CMF as delegate. The type shall follow the provisions defined in table 5.7.4.3-1.

Table 5.7.4.3-1: Definition of values

Attribute name	Definition
InfoType	"urn:etsi:nfv:cert-type:handling".
InfoValue	"urn:etsi:nfv:cert-type:handling:delegation " shall be the only allowed value.

5.8 Profiled solution specific features

5.8.1 ACME for MANO certification management

ACME is profiled for the MANO certification management as described in clauses 4.2.2 and 5. The present clause describes the ACME features which are required for ACME itself, but have no direct relationship with the requirements specified in ETSI GS NFV-IFA 033 [2].

"Identifier authorization" and "Identifier validation challenge" as specified in IETF RFC 8555 [15] are required for "Certificate Issuance" operation, which is mapped against "Certificate Signing Request" in clause 5.2.1.a. For "Identifier validation challenge", authentication method shall support both TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension specified in IETF RFC 8737 [16] and ACME Authority Token Challenge specified in IETF RFC 9447 [17], and the most appropriate method shall be selected based on the service provider's policies.

6 VNF Lifecycle Management interface

This interface allows the CMF to invoke VNF lifecycle management operations of VNF instances towards the VNFM, and to subscribe to notifications regarding VNF lifecycle changes provided by the VNFM.

The interface shall follow the provisions specified in clause 5 of ETSI GS NFV-SOL 002 [3] for the VNF Lifecycle Management interface, except the case that the producer is VNFM and the consumer is CMF.

Only the following operations as defined in clause 5 of ETSI GS NFV-SOL 002 [3] are supported on the CMF - NFV-MANO reference point, and the API producer shall return a "405 Method Not Allowed" response for other methods requested as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4]:

- Query VNF.
- Get Operation Status.
- Subscribe.
- Query Subscription Information.
- Terminate Subscription.
- Notify.

7 Certificate Notification interface

7.1 Description

This interface allows the CMF to invoke Certificate Notification.

The operations provided through this interface are:

- Subscribe.
- Notify.
- Terminate subscription.

See more details of the operations defined in clause 11.4 of ETSI GS NFV-IFA 033 [2].

7.2 Version

For the Certificate Notification interface version as specified in the present document, the MAJOR version field shall be 1, the MINOR version field shall be 0 and the PATCH version field shall be 0 (see clause 9.1 of ETSI GS NFV-SOL 013 [4] for a definition of the version fields). Consequently, the {apiMajorVersion} URI variable shall be set to "v1".

7.3 Sequence diagrams

7.3.1 Flow of managing subscriptions

The present clause describes the procedure for creating, querying/reading and terminating subscriptions to notifications related to Certificate.

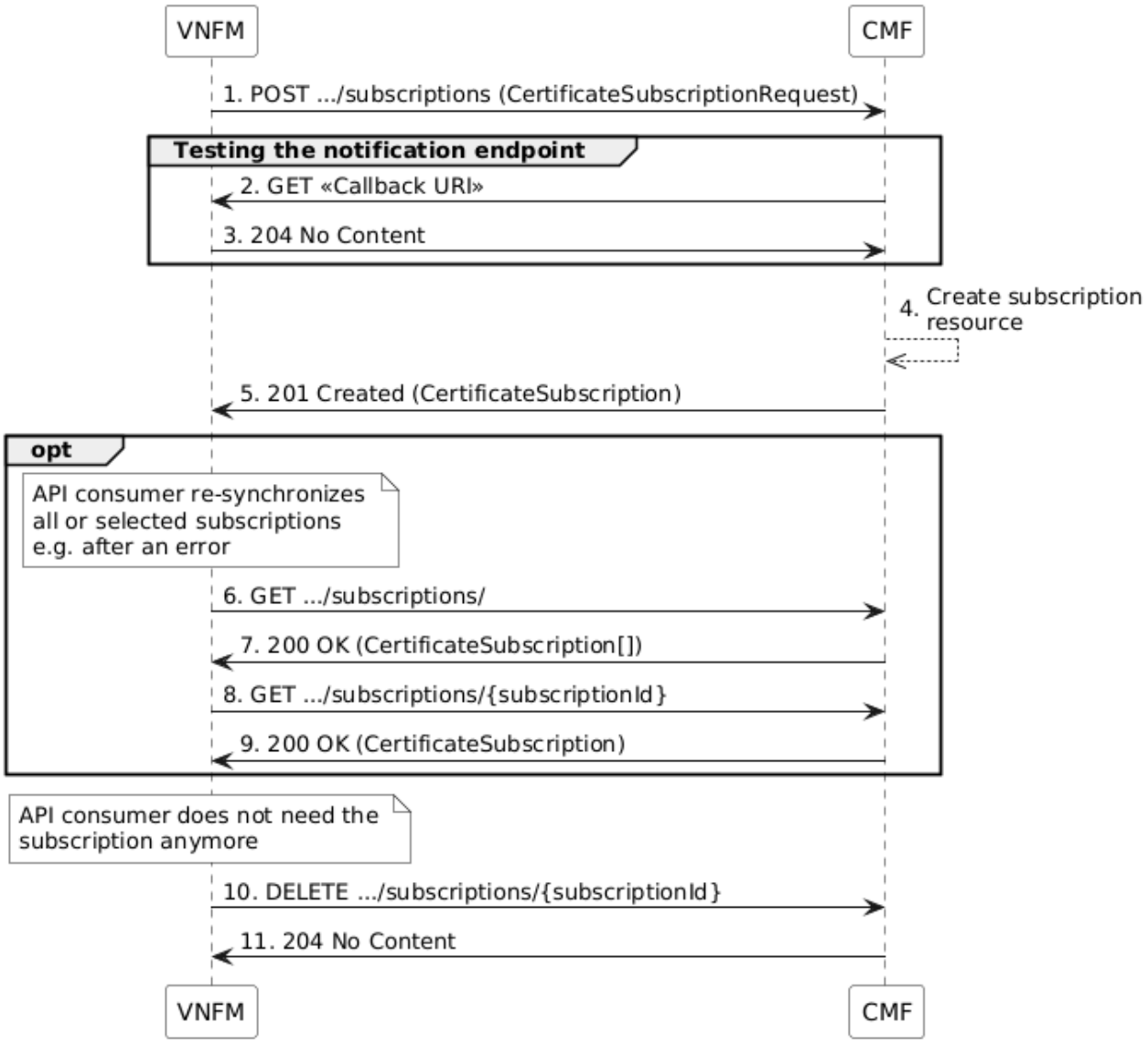

Figure 7.3.1-1: Flow of managing subscriptions

The procedure consists of the following steps as illustrated in figure 7.3.1-1:

1) The VNFM sends a POST request to the "Subscriptions" resource including in the message content a data structure of type "CertificateSubscriptionRequest". That data structure contains filtering criteria and a callback URI to which the CMF subsequently sends notifications about events that match the filter.

2) To test the notification endpoint that has been registered by the VNFM as part of the subscription, the CMF sends a GET request to the notification endpoint URI.

3) The VNFM returns a "204 No Content" response to indicate success.

4) The CMF creates a new subscription to notifications related to Certificate changes, and an "Individual subscription" resource that represents this subscription.

5) The CMF returns a 201 Created response containing a data structure of type "CertificateSubscription" representing the "Individual subscription" resource just created by the CMF and provides the URI of the newly-created resource in the "Location" HTTP header.

6) If desired, e.g. to recover from an error situation, the VNFM can query information about its subscriptions by sending a GET request to the resource representing the subscriptions.

7) In that case, the CMF returns a "200 OK" response that contains zero or more representations of all existing subscriptions that were created by the VNFM.

8) If desired, e.g. to recover from an error situation, the VNFM can read information about a particular subscription by sending a GET request to the resource representing that individual subscription.

9) In that case, the CMF returns a "200 OK" response that contains a representation of that individual subscription.

10) If the VNFM does not need the subscription anymore, it terminates the subscription by sending a DELETE request to the resource that represents the individual subscription to remove.

11) The CMF acknowledges the successful termination of the subscription by returning a "204 No Content" response.

Error handling: The CMF rejects a subscription if the subscription information is not valid: endpoint cannot be reached, subscription information is malformed, etc.

7.3.2 Flow of sending notifications

The present clause describes the procedure for sending notifications.

NOTE 1: Notifications merely report to subscribed NFV-MANO entities the state changes of a Certificate instance. They are triggered during the execution of the operation's flow or at its end but have no impact on the course of the procedure that has triggered them or on the state of the Certificate instance. If this flow is invoked as part of another flow, the invoking procedure does not wait for the acknowledgement of the delivery of the notification.

NOTE 2: Race conditions between requests/responses of other interface on one hand and notification delivery requests/responses on the other hand can occur as these are delivered through different HTTP connections.

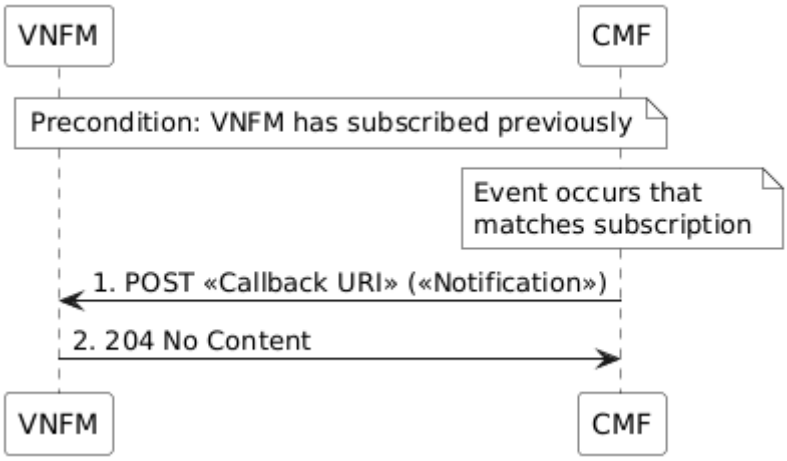

Figure 7.3.2-1: Flow of sending notifications

The procedure consists of the following steps as illustrated in figure 7.3.2-1.

Precondition: The VNFM has subscribed previously to notifications related to Certificate.

1) If an event occurs that matches the filtering criteria which are part of the subscription, the CMF generates a notification that includes information about the event and sends it in the body of a POST request to the URI which the VNFM has registered as part of the subscription request. The variable <<Notification>> in the flow is a placeholder for the different types of notifications that can be sent by this API (see clause 7.6.2.4).

2) The VNFM acknowledges the successful delivery of the notification by returning a "204 No Content" response.

Error handling: If the CMF does not receive the "204 No Content" response from the VNFM, it can retry sending the notification.

7.4 Resource structure and methods

All resource URIs of the API shall use the base URI specification defined in clause 4.1 of ETSI GS NFV-SOL 013 [4]. The string "certnotify" shall be used to represent {apiName}. All resource URIs in clauses below are defined relative to the above base URI.

Figure 7.4-1 shows the overall resource URI structure defined for the Certificate Management interface.

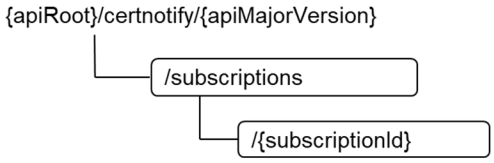

Figure 7.4-1: Resource URI structure of the Certificate Notification interface

Table 7.4-1 lists the individual resources defined, and the applicable HTTP methods.

The CMF shall support responding to requests for all HTTP methods on the resources in table 7.4-1 that are marked as "M" (mandatory) in the "Cat" column. The CMF shall also support the "API versions" resources as specified in clause 9.3.2 of ETSI GS NFV-SOL 013 [4].

Table 7.4-1: Resources and methods overview of the Certificate Notification interface

Resource name	Resource URI	HTTP Method	Cat	Meaning
Subscriptions	/subscriptions	POST	M	Subscribe to Certificate lifecycle status change notifications.
		GET	M	Query multiple subscriptions.
Individual subscription	/subscriptions/{subscriptionId}	GET	M	Read an "Individual subscription" resource.
		DELETE	M	Terminate a subscription.
Notification endpoint	(provided by API consumer)	POST	See note	Notify about VNF lifecycle change.
		GET	See note	Test the notification endpoint.
NOTE: The CMF shall support invoking the HTTP methods defined for the "Notification endpoint" resource exposed by the VNFM. If the VNFM supports invoking the POST method on the "Subscriptions" resource towards the CMF, it shall also support responding to the HTTP requests defined for the "Notification endpoint" resource.				

7.5 Resources

7.5.1 Introduction

Clause 7.5 defines all the resources and methods provided by the Certificate management interface.

7.5.2 Resource: API versions

The "API versions" resources as defined in clause 9.3.3 of ETSI GS NFV-SOL 013 [4] are part of the Certificate management interface.

7.5.3 Resource: Subscriptions

7.5.3.1 Description

This resource represents subscriptions. The API consumer can use this resource to subscribe to notifications related to Certificate, and to query its subscriptions.

7.5.3.2 Resource definition

The resource URI is:

{apiRoot}/certnotify/{apiMajorVersion}/subscriptions

This resource shall support the resource URI variables defined in table 7.5.3.2-1.

Table 7.5.3.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See clause 4.1 of ETSI GS NFV-SOL 013 [4].
apiMajorVersion	See clause 5.1a.

7.5.3.3 Resource methods

7.5.3.3.1 POST

The POST method creates a new subscription.

This method shall follow the provisions specified in tables 7.5.3.3.1-1 and 7.5.3.3.1-2 for URI query parameters, request and response data structures, and response codes.

As the result of successfully executing this method, a new "Individual subscription" resource as defined in clause 7.5.4 shall have been created. This method shall not trigger any notification.

Creation of two "Individual subscription" resources with the same callback URI and the same filter can result in performance degradation and provide duplicates of notifications to the VNFM, and might make sense only in very rare use cases. Consequently, the CMF may either allow creating an "Individual subscription" resource if another "Individual subscription" resource with the same filter and callback URI already exists (in which case it shall return the "201 Created" response code), or may decide to not create a duplicate "Individual subscription" resource (in which case it shall return a "303 See Other" response code referencing the existing "Individual subscription" resource with the same filter and callback URI).

Table 7.5.3.3.1-1: URI query parameters supported by the POST method on this resource

Name	Cardinality	Description
none supported		

Table 7.5.3.3.1-2: Details of the POST request/response on this resource

Request body	**Data type**	**Cardinality**	**Description**	
	CertificateSubscriptionRequest	1	Details of the subscription to be created, as defined in clause 7.6.2.2.	
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	CertificateSubscription	1	201 Created	Shall be returned when the subscription has been created successfully. The response body shall contain a representation of the created "Individual subscription" resource. The HTTP response shall include a "Location" HTTP header that points to the created "Individual subscription" resource.
	n/a		303 See Other	Shall be returned if a subscription with the same callback URI and the same filter already exists and the policy of the CMF is to not create redundant subscriptions. The HTTP response shall include a "Location" HTTP header that contains the resource URI of the existing "Individual subscription" resource. The response body shall be empty.
	ProblemDetails	1	422 Unprocessable Content	Shall be returned upon the following error: The content type of the message content is supported and the message content of a request contains syntactically correct data but the data cannot be processed. The general cause for this error and its handling is specified in clause 6.4 of ETSI GS NFV-SOL 013 [4], including rules for the presence of the response body. Specifically in case of this resource, the response code 422 shall also be returned if the CMF has tested the Notification endpoint as described in clause 7.5.5.3.2 and the test has failed. In this case, the "detail" attribute in the "ProblemDetails" structure shall convey more information about the error.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.3.3.2 GET

The GET method queries the list of active subscriptions of the functional block that invokes the method. It can be used e.g. for resynchronization after error situations.

This method shall follow the provisions specified in tables 7.5.3.3.2-1 and 7.5.3.3.2-2 for URI query parameters, request and response data structures, and response codes.

Table 7.5.3.3.2-1: URI query parameters supported by the GET method on this resource

Name	Cardinality	Description
Filter	0..1	Attribute-based filtering expression according to clause 5.2 of ETSI GS NFV-SOL 013 [4]. The CMF shall support receiving this parameter as part of the URI query string. The VNFM may supply this parameter. All attribute names that appear in the CertificateSubscription and in data types referenced from it shall be supported by the CMF in the filter expression.
nextpage_opaque_marker	0..1	Marker to obtain the next page of a paged response. Shall be supported by the CMF if the CMF supports alternative 2 (paging) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource.

Table 7.5.3.3.2-2: Details of the GET request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	CertificateSubscription	0..N	200 OK	Shall be returned when the list of subscriptions has been queried successfully. The response body shall contain in an array the representations of all active subscriptions of the functional block that invokes the method, i.e. zero or more representations of certificate change notification subscriptions as defined in clause 7.6.2.2. If the "filter" URI parameter was supplied in the request, the data in the response body shall have been transformed according to the rules specified in clause 5.2.2 of ETSI GS NFV-SOL 013 [4]. If the CMF supports alternative 2 (paging) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource, inclusion of the Link HTTP header in this response shall follow the provisions in clause 5.4.2.3 of ETSI GS NFV-SOL 013 [4].
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Invalid attribute-based filtering expression. The response body shall contain a ProblemDetails structure, in which the "detail" attribute should convey more information about the error.
	ProblemDetails	1	400 Bad Request	Shall be returned upon the following error: Response too big. If the CMF supports alternative 1 (error) according to clause 5.4.2.1 of ETSI GS NFV-SOL 013 [4] for this resource, this error response shall follow the provisions in clause 5.4.2.2 of ETSI GS NFV-SOL 013 [4].
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.3.3.3 PUT

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.3.3.4 PATCH

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.3.3.5 DELETE

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.4 Resource: Individual subscription

7.5.4.1 Description

This resource represents an individual subscription. The API consumer can use this resource to read and to terminate a subscription to notifications related to Certificate.

7.5.4.2 Resource definition

The resource URI is:

{apiRoot}/certnotify/{apiMajorVersion}/subscriptions/{subscriptionId}

This resource shall support the resource URI variables defined in table 7.5.4.2-1.

Table 7.5.4.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See clause 4.1 of ETSI GS NFV-SOL 013 [4].
apiMajorVersion	See clause 5.1a.
subscriptionId	Identifier of this subscription. See note.
NOTE: This identifier can be retrieved from the resource referenced by the "Location" HTTP header in the response to a POST request creating a new "Individual subscription" resource. It can also be retrieved from the "id" attribute in the message content of that response.	

7.5.4.3 Resource methods

7.5.4.3.1 POST

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.4.3.2 GET

The GET method retrieves information about a subscription by reading an "Individual subscription" resource.

This method shall follow the provisions specified in tables 7.5.4.3.2-1 and 7.5.4.3.2-2 for URI query parameters, request and response data structures, and response codes.

Table 7.5.4.3.2-1: URI query parameters supported by the GET method on this resource

Name	Cardinality	Description
none supported		

Table 7.5.4.3.2-2: Details of the GET request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	CertificateSubscription	1	200 OK	Shall be returned when information about an individual subscription has been read successfully. The response body shall contain a representation of the "Individual subscription" resource.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.4.3.3 PUT

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.4.3.4 PATCH

This method is not supported. When this method is requested on this resource, the CMF shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.4.3.5 DELETE

The DELETE method terminates an individual subscription.

This method shall follow the provisions specified in tables 7.5.4.3.5-1 and 7.5.4.3.5-2 for URI query parameters, request and response data structures, and response codes.

As the result of successfully executing this method, the "Individual subscription" resource shall not exist any longer. This means that no notifications for that subscription shall be sent to the formerly-subscribed API consumer.

NOTE: Due to race conditions, some notifications might still be received by the formerly-subscribed API consumer for a certain time period after the deletion.

Table 7.5.4.3.5-1: URI query parameters supported by the DELETE method on this resource

Name	Cardinality	Description
none supported		

Table 7.5.4.3.5-2: Details of the DELETE request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	n/a		204 No Content	Shall be returned when the "Individual subscription" resource has been deleted successfully. The response body shall be empty.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.5 Resource: Notification endpoint

7.5.5.1 Description

This resource represents a notification endpoint. The API producer can use this resource to send notifications related to certificate changes to a subscribed API consumer, which has provided the URI of this resource during the subscription process.

7.5.5.2 Resource definition

The resource URI is provided by the API consumer when creating the subscription.

This resource shall support the resource URI variables defined in table 7.5.5.2-1.

Table 7.5.5.2-1: Resource URI variables for this resource

Name	Definition
none supported	

7.5.5.3 Resource methods

7.5.5.3.1 POST

The POST method delivers a notification from the API producer to an API consumer. The API consumer shall have previously created an "Individual subscription" resource with a matching filter.

This method shall follow the provisions specified in tables 7.5.5.3.1-1 and 7.5.5.3.1-2 for URI query parameters, request and response data structures, and response codes.

Table 7.5.5.3.1-1: URI query parameters supported by the POST method on this resource

Name	Cardinality	Description
none supported		

Each notification request body shall include exactly one of the alternatives defined in table 7.5.5.3.1-2.

Table 7.5.5.3.1-2: Details of the POST request/response on this resource

	Data type	Cardinality	Response Codes	Description
Request body	CertificateLifecycleStateChangeNotification	1	A notification about certificate changes triggered by a certificate management operation occurrence.	
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	n/a		204 No Content	Shall be returned when the notification has been delivered successfully.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.5.3.2 GET

The GET method allows the API producer to test the notification endpoint that is provided by the API consumer, e.g. during subscription.

This method shall follow the provisions specified in tables 7.5.5.3.2-1 and 7.5.5.3.2-2 for URI query parameters, request and response data structures, and response codes.

Table 7.5.5.3.2-1: URI query parameters supported by the GET method on this resource

Name	Cardinality	Description
none supported		

Table 7.5.5.3.2-2: Details of the GET request/response on this resource

Request body	Data type	Cardinality	Description	
	n/a			
Response body	**Data type**	**Cardinality**	**Response Codes**	**Description**
	n/a		204 No Content	Shall be returned to indicate that the notification endpoint has been tested successfully. The response body shall be empty.
	ProblemDetails	See clause 6.4 of [4]	4xx/5xx	In addition to the response codes defined above, any common error response code as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4] may be returned.

7.5.5.3.3 PUT

This method is not supported. When this method is requested on this resource, the VNFM shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.5.3.4 PATCH

This method is not supported. When this method is requested on this resource, the VNFM shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.5.5.3.5 DELETE

This method is not supported. When this method is requested on this resource, the VNFM shall return a "405 Method Not Allowed" response as defined in clause 6.4 of ETSI GS NFV-SOL 013 [4].

7.6 Data model

7.6.1 Introduction

Clause 7.6 defines the request and response data structures of the Certificate management interface. If a request or response contains attributes not defined in the present document, a receiving functional block that does not understand these attributes shall not treat their presence as an error and may choose to ignore them.

7.6.2 Resource and notification data types

7.6.2.1 Introduction

This clause defines the data structures to be used in resource representations and notifications.

7.6.2.2 Type: CertificateSubscriptionRequest

This type represents request parameters for the "subscribe" operation as defined in ETSI GS NFV-IFA 033 [2]. It shall comply with the provisions defined in table 7.6.2.2-1.

Table 7.6.2.2-1: Definition of the CertificateSubscriptionRequest data type

Attribute name	Data type	Cardinality	Description
filter	CertificateChangeNotificationsFilter	0..1	Filter settings for this subscription, to define the subset of all notifications this subscription relates to. A particular notification is sent to the subscriber if the filter matches, or if there is no filter.
callbackUri	Uri	1	The URI of the endpoint to send the notification to.
authentication	SubscriptionAuthentication	1	Authentication parameters to configure the use of Authorization when sending notifications corresponding to this subscription, as defined in clause 8.3.4 of ETSI GS NFV-SOL 013 [4].
verbosity	CertificateNotificationVerbosityType	0..1	This attribute signals the requested verbosity of certificate notifications. If it is not present, it shall default to the value "FULL".

7.6.2.3 Type: CertificateSubscription

This type represents a subscription related to notification about Certificate. It shall comply with the provisions defined in table 7.6.2.3-1.

Table 7.6.2.3-1: Definition of the CertificateSubscription data type

Attribute name	Data type	Cardinality	Description
id	Identifier	1	Identifier of this subscription resource.
filter	CertificateChangeNotificationsFilter	0..1	Filter settings for this subscription, to define the subset of all notifications this subscription relates to. A particular notification is sent to the subscriber if the filter matches, or if there is no filter.
callbackUri	Uri	1	The URI of the endpoint to send the notification to.
verbosity	CertificateNotificationVerbosityType	0..1	This attribute signals the requested verbosity of certificate notifications. If it is not present, it shall default to the value "FULL".
_links	Structure (inlined)	1	Links to resources related to this resource.
>self	Link	1	URI of this resource.

7.6.2.4 Type: CertificateLifecycleStateChangeNotification

This type represents a subscription related to notification about Certificate. It shall comply with the provisions defined in table 7.6.2.4-1.

Table 7.6.2.4-1: Definition of the CertificateLifecycleStateChangeNotification data type

Attribute name	Data type	Cardinality	Description
id	Identifier	1	Identifier of this subscription resource.
notificationType	String	1	Discriminator for the different notification types. Shall be set to "CertificateLifecycleStateChangeNotification" for this notification type.
subscriptionId	Identifier	1	Identifier of the subscription that this notification relates to. Shall be set to the value of the "id" attribute of the "CertificateSubscription" representing the associated "Individual subscription" resource.
timeStamp	DateTime	1	Date-time of the generation of the notification.
certificateState	PKIStatusInfoType	1	The state of the Certificate.
certificateId	Identifier	1	The identifier of the Certificate affected.

Attribute name	Data type	Cardinality	Description
verbosity	CertificateNotificationVerbosityType		This attribute signals the verbosity of the notification. If it is not present, it shall default to the value "FULL". If the value is "SHORT", full change details can be obtained by performing a GET request on the "Individual Certificate" resource.
affectedSubject	AffectedSubject	0..1	Information about subject instances that were affected.
affectedCertificate	AffectedCertificate	0..1	Information about certificate instances that were affected.
error	ProblemDetails	0..1	Details of the latest error, if one has occurred during executing the certificate management (see clause 6.3 of ETSI GS NFV-SOL 013 [4]).
_links	Structure (inlined)	1	Links to resources related to this notification. The link URIs in this structure shall be set to point to the resources identified by the corresponding identifier attributes in this notification.
> subscription	NotificationLink	1	Link to the resource representing the subscription that this notification relates to.
> subject	NotificationLink	1	Link to the resource representing the subject instance to which the notified change applies.
> certificate	NotificationLink	1	Links to the resource representing the certificate instance to which the notified change applies.

7.6.3 Referenced structured data types

7.6.3.1 Introduction

This clause defines data structures that can be referenced from data structures defined in the previous clauses.

7.6.3.2 Type: CertificateChangeNotificationsFilter

This type represents a CertificateChangeNotificationsFilter. It shall comply with the provisions defined in table 7.6.3.2-1.

Table 7.6.3.2-1: Definition of the CertificateChangeNotificationsFilter data type

Attribute name	Data type	Cardinality	Description
vnfInstanceSubscriptionFilter	VnfInstanceSubscriptionFilter	0..1	Filter criteria to select VNF instances about which to notify.
cetificateState	PKIStatusInfoType	0..N	Match particular Certificate state values as reported in notifications of type CertificateLifecycleStateChangeNotification. May be present if the "notificationTypes" attribute contains the value " CertificateLifecycleStateChangeNotification" and shall be absent otherwise.
certificationType	Enum (inlined)	0..N	Match particular certificate types. Permitted values: • VNFCI certificate. • VNF OAM certificate.

7.6.3.3 Type: AffectedSubject

This type represents a AffectedSubject. This type provides information about added, deleted and modified subject. It shall comply with the provisions defined in table 7.6.3.3-1.

Table 7.6.3.3-1: Definition of the AffectedSubject data type

Attribute name	Data type	Cardinality	Description
id	Identifier	1	Identifier of the subject instance.
changeType	Enum (inlined)	1	Signals the type of change. Permitted values: • ADDED • REMOVED • MODIFIED
pkiBody	Structure (inlined)	1	Message-specific information. The structure and attributes are defined in IETF RFC 9810 [13] and IETF RFC 9811 [14].
>ip	CertRepMessage	1	Information for Initialization response.

7.6.3.4 Type: AffectedCertificate

This type represents a AffectedCertificate. This type provides information about added, deleted and modified certificate. It shall comply with the provisions defined in table 7.6.3.4-1.

Table 7.6.3.4-1: Definition of the AffectedCertificate data type

Attribute name	Data type	Cardinality	Description
id	Identifier	1	Identifier of the certificate instance.
changeType	Enum (inlined)	1	Signals the type of change. Permitted values: • ADDED • REMOVED • MODIFIED
pkiBody	Structure (inlined)	1	Message-specific information. The structure and attributes are defined in IETF RFC 9810 [13] and IETF RFC 9811 [14].
>cp	CertRepMessage	1	Information for CSR response.

7.6.4 Referenced simple data types and enumerations

7.6.4.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

7.6.4.2 Simple data types

No particular simple data types are defined for this interface, in addition to those defined in clause 5.6.4.4.2.

7.6.4.3 Enumeration: CertificateNotificationVerbosityType

The enumeration CertificateNotificationVerbosityType provides values to control the verbosity of certificate notifications. It shall comply with the provisions defined in table 7.6.4.3-1.

Table 7.6.4.3-1: Enumeration VnfOperationalStateType

Enumeration value	Description
FULL	This signals a full notification which contains all change details.
SHORT	This signals a short notification which omits large-volume change details to reduce the size of data to be sent via the notification mechanism.

Annex A (informative): Analysis on the existing solutions based on the Certificate Management interface requirements

A.1 CMP

A.1.1 Overview

This clause analyses comparison of interface requirements of CMF defined in ETSI GS NFV-IFA 033 [2] and CMP as specified in IETF RFC 2510 [i.2]. CMP supports operation related to certificate management from end entity as follows:

- initial registration operation (ir/ip);
- initial certification operation (cr/cp);
- certificate confirmation (certConf);
- key pair update operation (kur/kup);
- certificate update operation;
- CA key pair update operation;
- certificate discovery operation;
- recovery operation;
- revocation operation (rr/rp);
- PSE (Personal Security Environment) operation;
- End Entity Initialization.

NOTE: CMP is obsoleted by IETF RFC 4210 [i.9]. Therefore, CMPv2 specified in IETF RFC 4210 [i.9], and obsoleted by IETF RFC 9810 [13] and IETF RFC 9811 [14] is analysed in clause A.2 instead of CMP.

A.2 CMPv2

A.2.1 Overview

The present clause analyses comparison of interface requirements of CMF defined in ETSI GS NFV-IFA 033 [2] and CMPv2 as specified in IETF RFC 9810 [13] and IETF RFC 9811 [14]. CMPv2 supports operation related to certificate management as follows:

- initial registration operation (ir/ip);
- initial certification operation (cr/cp);
- certificate confirmation (certConf)key pair update operation (kur/kup);
- certificate update operation;
- CA key pair update operation;
- certificate discovery operation;

- recovery operation;
- revocation operation (rr/rp);
- PSE operation;
- End Entity Initialization.

A.2.2 Comparison of interface requirements of CMF and CMPv2

The present clause shows comparison of interface requirements of CMF defined in clauses 9.3 and 10.3 of ETSI GS NFV-IFA 033 [2] as "Identifier" column and "Requirement" column from table A.2.2-1 and CMPv2 as "Support by solution" and "Related capability of solution" from table A.2.2-1. The legend of "Support by solution" are the following:

- "Yes": fully support the interface requirements of CMF
- "No": not support the interface requirements of CMF
- "Partial": partial support the interface requirements of CMF

NOTE: The text reproduced in tables in clauses A.2, A.3, A.4 and A.5 was extracted from clauses 9.3 and 10.3 of ETSI GS NFV-IFA 033 [2] for readability purposes. Requirements reproduced in these tables are to be considered as quotes as they are not new requirements.

Table A.2.2-1: Comparison of interface requirements of CMF and CMPv2

Identifier	Requirement	Support by solution	Related capability of solution
"CmVnfm.CertMgmt"	*"This interface supports registration and signing request/response of VNFCI/VNF OAM certificates for the VNFCIs managed in delegation mode. It also supports de-registration of the end entities as subjects for certificates and certificate chains."*	Partial	Initial certification, operation and End Entity Initialization, but no deregistration
"CmVnfm.VnfLcmMgmt"	*"This interface supports providing notifications of VNF LCM operation occurrence events and supports querying information about VNF instances (as per clause 7.2 in ETSI GS NFV-IFA 007)."*	No	
"Cm-Vnfm.CertNotification"	*"This interface supports notifications about the VNFCI/VNF OAM certificate lifecycle states."*	No	
"Cm-Oss.CertMgmt"	*"This interface supports registration of NFV MANO certificates."*	Partial	End Entity Initialization but no concrete specification of End Entity Initialization
"Cm-Mano.CertMgmt"	*"This interface supports signing request/response, query, and revoke of NFV MANO certificates."*	Partial	Initial certification, operation, Polling request/response and revocation operation, but no deregistration
"CMF.Certm.Del.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation."*	Partial	End Entity Initialization but no concrete specification of End Entity Initialization
"CMF.Certm.Del.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities."*	Yes	Initial certification operation
"CMF.Certm.Del.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains."*	No	
"CMF.Certm.Del.004"	*Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains."*	No	

Identifier	Requirement	Support by solution	Related capability of solution
"CMF.Certm.Del.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities."*	Yes	Polling request and response
"CMF.Certm.Del.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities."*	Yes	Revocation operation
"CMF.Certm.Mano.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation. This requirement is only applicable to the Cm-Oss reference point."*	Partial	End Entity Initialization but no concrete specification of End Entity Initialization
"CMF.Certm.Mano.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities. This requirement is only applicable to the Cm-Mano reference point."*	Yes	Initial certification operation
"CMF.Certm.Mano.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains. This requirement is only applicable to the Cm-Oss reference point."*	No	
"CMF.Certm.Mano.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	No	
"CMF.Certm.Mano.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	Yes	Polling request and response
"CMF.Certm.Mano.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities. This requirement is only applicable to the Cm-Mano reference point."*	Yes	Revocation operation
"VNFM.LCM.001"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support managing subscriptions to VNF lifecycle management operation occurrence notifications."*	No	
"VNFM.LCM.002"	*The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support querying information about a VNF instance.*	No	
"CMF.CNS.001"	*T"he Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support managing subscriptions to certificate lifecycle state notifications."*	No	
"CMF.CNS.002"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support querying information about VNFCI or VNF OAM certificate states."*	No	

A.2.3 Comparison of Register operation and End Entity Initialization operation

The End Entity Initialization operation of CMPv2 as specified in IETF RFC 2510 [i.2] is specified only concept and is not specified concrete parameter. There is no specification comparable to CMF's Register operation.

A.2.4 Comparison of Certificate Signing Request operation and initial certification operation

Tables A.2.4-1 and A.2.4-2 illustrate a comparison of the attributes in Certificate Signing Request operation as specified in clause 11.2.3 in ETSI GS NFV-IFA 033 [2] and initial certification operation of CMPv2 as specified in IETF RFC 2510 [i.2].

Table A.2.4-1: Comparison of input parameter in Certificate Signing Request operation and initial certification operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters initial certification operation in IETF RFC 2510 [i.2]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
vnfcId	1			No correspondence.
certType	1			No correspondence.
certChainRequest	1			No correspondence.
csr	1	CertReqMessage		

Table A.2.4-2: Comparison of output parameter in Certificate Signing Request operation and initial certification operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters initial certification operation in IETF RFC 2510 [i.2]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
certificate	1	CertOrEncCert		
certificateChain	1	PKIMessage.extraCerts		

A.2.5 Comparison of Revoke operation and Revocation operation

Table A.2.5-1 and table A.2.5-2 illustrate a comparison of the attributes in Revoke operation as specified in clause 11.2.4 in ETSI GS NFV-IFA 033 [2] and Revocation operation of CMPv2 as specified in IETF RFC 9480 [i.10].

Table A.2.5-1: Comparison of input parameter in Revoke operation and Revocation operation

Input Parameters in Revoke operation in ETSI GS NFV-IFA 033 [2]		Parameters Revocation operation in IETF RFC 9480 [i.10]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
certificateId	1	certDetails	1	

Table A.2.5-2: Comparison of output parameter in Revoke operation and Revocation operation

Output Parameters in Revoke operation in ETSI GS NFV-IFA 033 [2]		Parameters Revocation operation in IETF RFC 9480 [i.10]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
None				

A.3 SCEP

A.3.1 Overview

This clause analyses comparison of interface requirements of CMF defined in ETSI GS NFV-IFA 033 [2] and SCEP as specified in IETF RFC 8894 [i.3]. SCEP supports operation related to certificate management from end entity as follows:

- CA public key distribution operation.
- Certificate enrolment and issue operation.
- Certificate renewal operation.
- Certificate query operation.
- CRL query operation.

A.3.2 Comparison of interface requirements of CMF and SCEP

This clause shows comparison of interface requirements of CMF defined in clauses 9.3 and 10.3 of ETSI GS NFV-IFA 033 [2] as "Identifier" column and "Requirement" column from table A.3.2-1 and SCEP as "Support by solution" and "Related capability of solution" from table A.3.2-1. The legend of "Support by solution" are the following:

- "Yes": fully support the interface requirements of CMF.
- "No": not support the interface requirements of CMF.
- "Partial": partial support the interface requirements of CMF.

Table A.3.2-1: Comparison of interface requirements of CMF and SCEP

Identifier	Requirement	Support by solution	Related capability of solution
"CmVnfm.CertMgmt"	*"This interface supports registration and signing request/response of VNFCI/VNF OAM certificates for the VNFCIs managed in delegation mode. It also supports de-registration of the end entities as subjects for certificates and certificate chains."*	Partial	PKCSreq
"CmVnfm.VnfLcmMgmt"	*"This interface supports providing notifications of VNF LCM operation occurrence events and supports querying information about VNF instances (as per clause 7.2 in ETSI GS NFV-IFA 007 [i.8])."*	No	
"Cm-Vnfm.CertNotification"	*"This interface supports notifications about the VNFCI/VNF OAM certificate lifecycle states."*	No	
"Cm-Oss.CertMgmt"	*"This interface supports registration of NFV MANO certificates. "*	No	
"Cm-Mano.CertMgmt"	*"This interface supports signing request/response, query, and revoke of NFV MANO certificates."*	Partial	PKCSreq
"CMF.Certm.Del.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation."*	No	
"CMF.Certm.Del.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities."*	Yes	PKCSreq
"CMF.Certm.Del.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains."*	No	

Identifier	Requirement	Support by solution	Related capability of solution
"CMF.Certm.Del.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains."*	No	
CMF.Certm.Del.005	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities."*	Yes	CertPoll
"CMF.Certm.Del.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities."*	No	
"CMF.Certm.Mano.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation. This requirement is only applicable to the Cm-Oss reference point."*	No	
"CMF.Certm.Mano.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities. This requirement is only applicable to the Cm-Mano reference point."*	Yes	PKCSreq
"CMF.Certm.Mano.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains. This requirement is only applicable to the Cm-Oss reference point."*	No	
"CMF.Certm.Mano.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	No	
"CMF.Certm.Mano.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	Yes	CertPoll
"CMF.Certm.Mano.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities. This requirement is only applicable to the Cm-Mano reference point."*	No	
"VNFM.LCM.001"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support managing subscriptions to VNF lifecycle management operation occurrence notifications."*	No	
"VNFM.LCM.002"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support querying information about a VNF instance."*	No	
"CMF.CNS.001"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support managing subscriptions to certificate lifecycle state notifications."*	No	
"CMF.CNS.002"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support querying information about VNFCI or VNF OAM certificate states."*	No	

A.3.3 Comparison of Certificate Signing Request operation and PKCSreq operation

Table A.3.3-1 and table A.3.3-2 illustrate a comparison of the attributes in Certificate Signing Request operation as specified in clause 11.2.3 in ETSI GS NFV-IFA 033 [2], and PKCSreq of SCEP that is "Transaction Attribute" is message type 18 and CertRep of SCEP that is "Transaction Attribute" is message type 3 as specified in IETF RFC 8555 [15].

Table A.3.3-1: Comparison of input parameter in Certificate Signing Request operation PKCSreq operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters PKCSreq operation in IETF RFC 8555 [15]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
vnfcId	1			No correspondence.
certType	1			No correspondence.
certChainRequest	1			No correspondence.
Csr	1	PKIDate.reqSequence		

Table A.3.3-2: Comparison of output parameter in Certificate Signing Request operation and CertRep operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters CertRep operation in IETF RFC 8555 [15]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
certificate	1	pkiMessage.certificates		
certificateChain	1	pkiMessage.certificates		

A.4 EST

A.4.1 Overview

Clause A.4 analyses comparison of interface requirements of CMF defined in ETSI GS NFV-IFA 033 [2] and EST as specified in IETF RFC 7030 [i.4]. EST supports operation related to certificate management from end entity as follows:

- Distribution of CA Certificates operation.
- Enrolment of Clients operation.
- Re-enrolment of Clients operation.
- Full CMC operation.
- Server-Side Key Generation operation.
- CSR Attributes operation.

A.4.2 Comparison of interface requirements of CMF and EST

The present clause shows comparison of interface requirements of CMF defined in clauses 9.3 and 10.3 of ETSI GS NFV-IFA 033 [2] as "Identifier" column and "Requirement" column from table A.4.2-1 and EST as "Support by solution" and "Related capability of solution" from table A.4.2-1. The legend of "Support by solution" are the following:

- "Yes": fully support the interface requirements of CMF.

- "No": not support the interface requirements of CMF.
- "Partial": partial support the interface requirements of CMF.

Table A.4.2-1: Comparison of interface requirements of CMF and EST

Identifier	Requirement	Support by solution	Related capability of solution
"CmVnfm.CertMgmt"	*"This interface supports registration and signing request/response of VNFCI/VNF OAM certificates for the VNFCIs managed in delegation mode. It also supports de-registration of the end entities as subjects for certificates and certificate chains."*	Partial	Enrolment of Clients operation
"CmVnfm.VnfLcmMgmt"	*"This interface supports providing notifications of VNF LCM operation occurrence events and supports querying information about VNF instances (as per clause 7.2 in ETSI GS NFV-IFA 007 [i.8])."*	No	
"Cm-Vnfm.CertNotification"	*"This interface supports notifications about the VNFCI/VNF OAM certificate lifecycle states."*	No	
"Cm-Oss.CertMgmt"	*"This interface supports registration of NFV MANO certificates."*	No	
"Cm-Mano.CertMgmt"	*"This interface supports signing request/response, query, and revoke of NFV MANO certificates."*	Partial	Enrolment of Clients operation
"CMF.Certm.Del.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation."*	No	
"CMF.Certm.Del.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities."*	Yes	Enrolment of Clients operation
"CMF.Certm.Del.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains."*	No	
"CMF.Certm.Del.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains."*	No	
"CMF.Certm.Del.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities."*	Yes	CSR Attributes Request
"CMF.Certm.Del.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities."*	No	
"CMF.Certm.Mano.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation. This requirement is only applicable to the Cm-Oss reference point."*	No	
"CMF.Certm.Mano.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities. This requirement is only applicable to the Cm-Mano reference point."*	Yes	Enrolment of Clients operation
"CMF.Certm.Mano.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains. This requirement is only applicable to the Cm-Oss reference point."*	No	

Identifier	Requirement	Support by solution	Related capability of solution
"CMF.Certm.Mano.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	No	
"CMF.Certm.Mano.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	Yes	CSR Attributes Request
"CMF.Certm.Mano.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities. This requirement is only applicable to the Cm-Mano reference point."*	No	
"VNFM.LCM.001"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support managing subscriptions to VNF lifecycle management operation occurrence notifications."*	No	
"VNFM.LCM.002"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support querying information about a VNF instance."*	No	
"CMF.CNS.001"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support managing subscriptions to certificate lifecycle state notifications."*	No	
"CMF.CNS.002"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support querying information about VNFCI or VNF OAM certificate states."*	No	

A.4.3 Comparison of Certificate Signing Request operation and Enrolment of Clients operation

Table A.4.3-1 and table A.4.3-2 illustrate a comparison of the attributes in Certificate Signing Request operation as specified in clause 11.2.3 in ETSI GS NFV-IFA 033 [2] and Enrolment of Clients of EST as specified in [i.6].

Table A.4.3-1: Comparison of input parameter in Certificate Signing Request operation and initial certification operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters initial certification operation in [i.6]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
vnfcId	1			No correspondence.
certType	1			No correspondence.
certChainRequest	1	PKIData.reqSequence		
csr	1	simpleenroll. pkcs10		

Table A.4.3-2: Comparison of output parameter in Certificate Signing Request operation and initial certification operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters initial certification operation in [i.6]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
certificate	1	simpleenroll.pkcs7-mime		
certificateChain	1	simpleenroll.pkcs7-mime		

A.5 ACME

A.5.1 Overview

This clause analyses comparison of interface requirements of CMF defined in ETSI GS NFV-IFA 033 [2] and ACME as specified in IETF RFC 8555 [i.5]. ACME supports operation related to certificate management from end entity as follows:

- Account Creation.
- Ordering a Certificate.
- Identifier Authorization.
- Certificate Issuance.
- Certificate Revocation.
- Account Deactivation.
- Poll for status.
- Download certificate.

NOTE: There are additional technical constraints preventing ACME protocol adoption in the current NFV architecture for the support of VNFC/VNF OAM certificate management in delegation mode. The primary limitation stems from ACME's mandatory domain validation requirements - specifically, the inability to satisfy either the HTTP-01 challenge (web server file placement) or DNS-01 challenge (DNS record modification) to verify FQDN ownership.

A.5.2 Comparison of interface requirements of CMF and ACME

This clause shows comparison of interface requirements of CMF defined in clauses 9.3 and 10.3 of ETSI GS NFV-IFA 033 [2] as "Identifier" column and "Requirement" column from table A.5.2-1 and ACME as "Support by solution" and "Related capability of solution" from table A.5.2-1. The legend of "Support by solution" are the following:

- "Yes": fully support the interface requirements of CMF
- "No": not support the interface requirements of CMF
- "Partial": partial support the interface requirements of CMF

Table A.5.2-1: Comparison of interface requirements of CMF and ACME

Identifier	Requirement	Support by solution	Related capability of solution
"CmVnfm.CertMgmt"	*"This interface supports registration and signing request/response of VNFCI/VNF OAM certificates for the VNFCIs managed in delegation mode. It also supports de-registration of the end entities as subjects for certificates and certificate chains."*	Yes	Account Creation, Ordering a Certificate, and Account deactivation
"CmVnfm.VnfLcmMgmt"	*"This interface supports providing notifications of VNF LCM operation occurrence events and supports querying information about VNF instances (as per clause 7.2 in ETSI GS NFV-IFA 007 [i.8])."*	No	
"Cm-Vnfm.CertNotification"	*"This interface supports notifications about the VNFCI/VNF OAM certificate lifecycle states."*	Partial	Contact supports mailto
"Cm-Oss.CertMgmt"	*"This interface supports registration of NFV MANO certificates."*	Yes	Account Creation, and Account deactivation
"Cm-Mano.CertMgmt"	*"This interface supports signing request/response, query, and revoke of NFV MANO certificates."*	Partial	Ordering a Certificate, Get Account Information, Poll for status, Certificate Revocation
"CMF.Certm.Del.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation."*	Yes	Account Creation
"CMF.Certm.Del.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities."*	Yes	Ordering a Certificate and Certificate Issuance
"CMF.Certm.Del.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains."*	Yes	Account deactivation
"CMF.Certm.Del.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains."*	Partial	Get Account Information
"CMF.Certm.Del.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities."*	Yes	Poll for status
"CMF.Certm.Del.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities."*	Yes	Certificate Revocation
"CMF.Certm.Mano.001"	*"Certificate management interface shall support the registration of the end entities, which are target for certificate enrolment and installation. This requirement is only applicable to the Cm-Oss reference point. "*	Yes	Account Creation
"CMF.Certm.Mano.002"	*"Certificate management interface shall support signing certificates and delivering certificate chains for the registered entities. This requirement is only applicable to the Cm-Mano reference point. "*	Yes	Ordering a Certificate and Certificate Issuance
"CMF.Certm.Mano.003"	*"Certificate management interface shall support the de-registration of the end entities as subjects for certificates and certificate chains. This requirement is only applicable to the Cm-Oss reference point. "*	Yes	Account deactivation
"CMF.Certm.Mano.004"	*"Certificate management interface shall support querying information of the end entities as subjects for certificates and certificate chains. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	Partial	Get Account Information

Identifier	Requirement	Support by solution	Related capability of solution
"CMF.Certm.Mano.005"	*"Certificate management interface shall support querying information of the certificates which are signed and delivered to the end entities. This requirement is applicable to the Cm-Mano reference point and Cm-Oss reference point."*	Yes	Poll for status
"CMF.Certm.Mano.006"	*"Certificate management interface shall support revoking the certificates which are signed and delivered to the end entities. This requirement is only applicable to the Cm-Mano reference point."*	Yes	Certificate Revocation
"VNFM.LCM.001"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support managing subscriptions to VNF lifecycle management operation occurrence notifications."*	No	
"VNFM.LCM.002"	*"The VNF Lifecycle Management interface produced by the VNFM on the Cm-Vnfm reference point shall support querying information about a VNF instance."*	No	
"CMF.CNS.001"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support managing subscriptions to certificate lifecycle state notifications."*	Partial	Contact supports mailto
"CMF.CNS.002"	*"The Certificate Notification Service interface produced by the CMF on the Cm-Vnfm reference point shall support querying information about VNFCI or VNF OAM certificate states."*	Yes	Poll for status

A.5.3 Comparison of Register operation and Account Creation operation

Table A.5.3-1 and table A.5.3-2 illustrate a comparison of the attributes in Register operation as specified in clause 11.2.2 in ETSI GS NFV-IFA 033 [2] and Account Creation operation of ACME as specified in IETF RFC 8555 [15].

Table A.5.3-1: Comparison of input parameter in Register operation and Account Creation operation

Input Parameters in Register operation in ETSI GS NFV-IFA 033 [2]		Parameters Account Creation operation in IETF RFC 8555 [15]		Comments
Parameter	**Cardinality**	**Parameter**	**Cardinality**	
certType	1			No correspondence.
subjectId	1..N			No correspondence.
> subjectId	1	JWK	1	
> certificateData	1..N			No correspondence.
>> subjectName	0..1			No correspondence.
>> subjectAlternate Name	1..N			No correspondence.
typeOfVnfcCertH andling	1			No correspondence.

Table A.5.3-2: Comparison of output parameter in Register operation and Account Creation operation

Output Parameters in Register operation in ETSI GS NFV-IFA 033 [2]		Parameters Account Creation operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
None				

A.5.4 Comparison of Certificate Signing Request operation and Certificate Issuance operation

Table A.5.4-1 and table A.5.4-2 illustrate a comparison of the attributes in Certificate Signing Request operation as specified in clause 11.2.3 in ETSI GS NFV-IFA 033 [2], and Certificate Issuance operation and Download Certificate of ACME as specified in IETF RFC 8555 [15].

Table A.5.4-1: Comparison of input parameter in Certificate Signing Request operation and Certificate Issuance operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters Certificate Issuance operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
vnfcId	1	value		
certType	1			No correspondence.
certChainRequest	1			No correspondence.
Csr	1	csr		

Table A.5.4-2: Comparison of output parameter in Certificate Signing Request operation and Download Certificate operation

Output Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Parameters Certificate Issuance operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
Certificate	1	end-entity certificate contents		
certificateChain	1	issuer certificate contents		

A.5.5 Comparison of Deregister operation and Account Deactivation operation

Table A.5.5-1 and table A.5.5-2 illustrate a comparison of the attributes in Deregister operation as specified in clause 11.2.4 in ETSI GS NFV-IFA 033 [2] and Account Deactivation operation of ACME as specified in IETF RFC 8555 [15].

Table A.5.5-1: Comparison of input parameter in Deregister operation and Account Deactivation operation

Input Parameters in Deregister operation in ETSI GS NFV-IFA 033 [2]		Parameters Account Deactivation operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
subjectId	1	signature		

Table A.5.5-2: Comparison of output parameter in Deregister operation and Account Deactivation operation

Output Parameters in Deregister operation in ETSI GS NFV-IFA 033 [2]		Parameters Account Deactivation operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
None				

A.5.6 Comparison of Revoke operation and Certificate Revocation operation

Table A.5.6-1 and table A.5.6-2 illustrate a comparison of the attributes in Revoke operation as specified in clause 11.2.4 in ETSI GS NFV-IFA 033 [2] and Certificate Revocation operation of ACME as specified in IETF RFC 8555 [15].

Table A.5.6-1: Comparison of input parameter in Revoke operation and Certificate Revocation operation

Input Parameters in Revoke operation in ETSI GS NFV-IFA 033 [2]		Parameters Certificate Revocation operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
certificateId	1	certificate	1	

Table A.5.6-2: Comparison of output parameter in Revoke operation and Certificate Revocation operation

Output Parameters in Revoke operation in ETSI GS NFV-IFA 033 [2]		Parameters Certificate Revocation operation in IETF RFC 8555 [15]		Comments
Parameter	Cardinality	Parameter	Cardinality	
None				

A.6 Analysis of solutions against the interface requirements of CMF

A.6.1 Overview

Clause A.6 analyses comparison of solutions (CMPv2, SCEP, EST and ACME) based on analysis on the solutions described in clauses A.1 to A.5 against requirements of CMF defined in ETSI GS NFV-IFA 033 [2].

A.6.2 Comparison of interface requirements

Table A.6.2-1 shows summary of "Requirement" column from table A.2.2-1 to table A.5.2-1 for the detailed interface requirement of CMF description related to each requirement identifier. The legend of "Support by solution" are the following:

- "Yes": fully support the interface requirements of CMF
- "No": not support the interface requirements of CMF
- "Partial": partial support the interface requirements of CMF

Table A.6.2-1: Comparison of interface requirements of CMF

Identifier	Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
CmVnfm.CertMgmt	Yes	Partial	Partial	Yes
CmVnfm.VnfLcmMgmt	No	No	No	No
Cm-Vnfm.CertNotification	No	No	No	Partial
Cm-Oss.CertMgmt	Yes	Partial	Partial	Yes
Cm-Mano.CertMgmt	Yes	Partial	Partial	Partial
CMF.Certm.Del.001	Partial	No	No	Yes
CMF.Certm.Del.002	Yes	Yes	Yes	Yes
CMF.Certm.Del.003	No	No	No	Yes
CMF.Certm.Del.004	No	No	No	Partial
CMF.Certm.Del.005	Yes	Yes	Yes	Yes
CMF.Certm.Del.006	Yes	No	No	Yes
CMF.Certm.Mano.001	Partial	No	No	Yes
CMF.Certm.Mano.002	Yes	Yes	Yes	Yes
CMF.Certm.Mano.003	No	No	No	Yes
CMF.Certm.Mano.004	No	No	No	Yes
CMF.Certm.Mano.005	Yes	Yes	Yes	Yes
CMF.Certm.Mano.006	Yes	No	No	Yes
VNFM.LCM.001	No	No	No	No
VNFM.LCM.002	No	No	No	No
CMF.CNS.001	No	No	No	Partial
CMF.CNS.002	No	No	No	Yes

A.6.3 Comparison of attributes of interface

Refer to "Parameter" column from table A.2.4-1 to table A.5.6-2 for the detailed input and output parameter of CMF interface. The legend of "Support by solution" are the following:

- "Yes": fully support the CMF service requirements
- "No": not support the interface requirements of CMF
- "Partial": partial support the interface requirements of CMF

Table A.6.3-1: Comparison of input parameter in Register operation

Input Parameters in Register operation in ETSI GS NFV-IFA 033 [2]		Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
Parameter	Cardinality				
certType	1	No	No	No	No
subjectId	1..N	No	No	No	Partial
typeOfVnfcCertHandling	1	No	No	No	No

Table A.6.3-2: Comparison of input parameter in Certificate Signing Request operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
Parameter	Cardinality				
vnfcId	1	No	No	No	Yes
certType	1	No	No	No	No
certChainRequest	1	No	No	Yes	No
Csr	1	Yes	Yes	Yes	Yes

Table A.6.3-3: Comparison of output parameter in Certificate Signing Request operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
Parameter	Cardinality				
Certificate	1	Yes	Yes	Yes	Yes
certificateChain	1	Yes	Yes	Yes	Yes

Table A.6.3-4: Comparison of input parameter in Deregister operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
Parameter	Cardinality				
subjectId	1	No	No	No	Yes

Table A.6.3-5: Comparison of input parameter in Revoke operation

Input Parameters in Certificate Signing Request operation in ETSI GS NFV-IFA 033 [2]		Support by CMPv2	Support by SCEP	Support by EST	Support by ACME
Parameter	Cardinality				
certificateId	1	Yes	No	No	Yes

A.6.4 Conclusion

For the VNFC/VNF OAM certificate management consideration with delegation mode, based on analysis of clauses A.6.2 and A.6.3, any solution does not meet interface requirements of CMF. In particular, Registration and Deregistration as CMF.Certm.Del.001 and CMF.Certm.Del.003 while ACME is the only one solution which supports Registration and Deregistration that is not yet profiled for NFV architecture due to ownership of identifiers issues in present document. Since VNF lifecycle management operation occurrence notifications as VNFM.LCM.001 and query VNF instance as VNFM.LCM.002 are not covered by the IETF protocols, existing ETSI specifications such as ETSI GS NFV-SOL 002 [3] is recommended to be reused. It is recommended for NFV to create new solutions Registration/Deregistration, and it is recommended to reuse CMPv2 for Certificate Signing Request and Revoke as CMF.Certm.Del.002 and CMF.Certm.Del.006.

For the MANO certificate management consideration with indirect mode, based on analysis of clauses A.6.2 and A.6.3, ACME is the solution which supports Registration and Deregistration as CMF.Certm.Mano.001 and CMF.Certm.Mano.003. Since VNF lifecycle management operation occurrence notifications as VNFM.LCM.001 and query VNF instance as VNFM.LCM.002 are not covered by the IETF protocols, existing ETSI specifications such as ETSI GS NFV-SOL 002 [3] is recommended to be reused. It is recommended for NFV to create new solutions Registration/Deregistration, and it is recommended to reuse ACME for Registration, Deregistration, Certificate Signing Request and Revoke as CMF.Certm.Mano.001, CMF.Certm.Mano.003, CMF.Certm.Mano.002 and CMF.Certm.Mano.006.

NOTE: There are additional technical constraints preventing ACME protocol (clause A.5) adoption in the current NFV architecture for the VNFC/VNF OAM certificate management. The primary limitation stems from ACME's mandatory domain validation requirements - specifically, the inability to satisfy either the HTTP-01 challenge (web server file placement) or DNS-01 challenge (DNS record modification) to verify FQDN ownership.

Annex B (informative): Mapping operations to protocol elements

B.1 Overview

The present annex provides the mapping between operations as defined in ETSI GS NFV-IFA 033 [2] and the corresponding resources and HTTP methods defined in the present document.

B.2 Certificate Management interface

Table B.2-1: Mapping for the Certificate Management interface

ETSI GS NFV-IFA 033 [2] operation	HTTP method	Resource	Direction
Register	POST	/nfv-cert/{name}/subjects	VNFM → CMF
Deregister	DELETE	/nfv-cert/{name}/subjects/{subjectId}	VNFM → CMF
Query Subject Info	GET	/nfv-cert/{name}/subjects	VNFM → CMF
	GET	/nfv-cert/{name}/subjects/{subjectId}	VNFM → CMF
Certificate Signing Request	POST	/.wellknown/cmp/p/{name}/pkcs10	VNFM → CMF
Revoke	POST	/.wellknown/cmp/p/{name}/revocation	VNFM → CMF
Query Certificate Info	POST	/.wellknown/cmp/p/{name}/pkcs10	VNFM → CMF

B.3 VNF Lifecycle Management interface

Table B.3-1: Mapping for the VNF Lifecycle management interface

ETSI GS NFV-IFA 033 [2] operation	HTTP method	Resource	Direction
Query VNF	GET	/vnf_instances/{vnfInstanceId}	CMF → VNFM
	GET	/vnf_instances	CMF → VNFM
Subscribe	POST	/subscriptions	CMF → VNFM
Query Subscription Information	GET	/subscriptions	CMF → VNFM
	GET	/subscriptions/{subscriptionId}	CMF → VNFM
Terminate Subscription	DELETE	/subscriptions/{subscriptionId}	CMF → VNFM
Notify	POST	(provided by API consumer)	VNFM → CMF

B.4 Certificate Notification interface

Table B.4-1: Mapping for the Certificate Notification interface

ETSI GS NFV-IFA 033 [2] operation	HTTP method	Resource	Direction
Subscribe	POST	/subscriptions	VNFM → CMF
Terminate Subscription	DELETE	/subscriptions/{subscriptionId}	VNFM → CMF
Notify	POST	(provided by API consumer)	CMF → VNFM

Annex C (normative): Authorization scope values

C.1 Overview

The present annex specifies authorization scope values for selected APIs defined in the present document as defined in clause 8.3.7 of ETSI GS NFV-SOL 013 [4]. Each authorization scope value is defined recursively as the union of a set of permitted resource URIs with associated permitted methods, and a set of permitted referenced authorization scope values, where one of these sets can be empty.

C.2 Certificate Management interface

The present clause specifies authorization scope values to consume the Certificate Management interface specified in clause 5. The CMF shall support the authorization scope values specified in table C.2-1 and may support additional authorization scope values, when authorizing an API request from an API consumer as specified in clause 8.3.3 of ETSI GS NFV-SOL 013 [4].

The elements in the authorization scope value definition specified in clause 8.3.7 of ETSI GS NFV-SOL 013 [4] are defined as follows, resulting in the authorization scope values given in table C.2-1:

- {apiName} is set as defined in clause 5.4;
- <vn> shall be set to the value of {apiMajorVersion} as defined in clause 5.2;
- <permissionName> and <qualifier> are set as defined in table C.2-1.

Table C.2-1: Authorization scope values for Certificate Management interface

Authorization scope value	Description
cert:<vn>:subject	Allows to read the "Subject instances" resource, to create and delete its child resources. This permission allows to create an "Individual Subject instance" resource as indicated in clause 5.3.1, delete an "Individual Subject instance" resource as indicated in clause 5.3.2, and query/read information in an "Individual Subject instance" resource as indicated in clause 5.3.6.
cert:<vn>:all	Allows to perform all methods on all resources of the Certificate Management interface.

Table C.2-2 defines the authorization scope values that are applicable to the Certificate Management interface on the CMF-Vnfm reference point.

Table C.2-2: Resource and permission of authorization scope for Certificate Management interface

Authorization scope value	Resources and scopes	Permitted methods
cert:<vn>:subject	/nfv-cert/{name}/subject	GET, POST
	/nfv-cert/{name}/subject/{subjectId}	GET, DELETE
cert:<vn>:all	cert:<vn>:subject	-
	cert:<vn>:certificate_content:readonly	-

C.3 Certificate Notification interface

The present clause specifies authorization scope values to consume the Certificate Notification interface specified in clause 7. The CMF shall support the authorization scope values specified in table C.3-1 and may support additional authorization scope values, when authorizing an API request from an API consumer as specified in clause 8.3.3 in ETSI GS NFV-SOL 013 [4].

The elements in the authorization scope value definition specified in clause 8.3.7 of ETSI GS NFV-SOL 013 [4] are defined as follows, resulting in the authorization scope values given in table C.3-1:

- {apiName} is set as defined in clause 5.4;
- <vn> shall be set to the value of {apiMajorVersion} as defined in clause 5.2;
- <permissionName> and <qualifier> are set as defined in table C.3-1.

Table C.3-1: Authorization scope values for Certificate Notification interface

Authorization scope value	Description
certnotify:<vn>:all	Allows to perform all methods on all resources of the Certificate Notification interface. This permission allows managing subscriptions as indicated in clause 7.3.1.

Table C.3-2 defines the authorization scope values that are applicable to the Certificate Notification interface on the CMF-Vnfm reference point.

Table C.3-2: Resource and permission of authorization scope for Certificate Notification interface

Authorization scope value	Resources and scopes	Permitted methods
certnotify:<vn>:all	certnotify:<vn>:subscription	GET, POST
	certnotify:<vn>:subscription/{subscriptionId}	GET, DELETE

Annex D (informative): Complementary material for API utilization

To complement the definitions of each method, resource, and data type defined in the main body of the present document, the ETSI NFV ISG is providing supplementary description files, compliant to the OpenAPI™ Specification [i.6], for the CMF - NFV-MANO reference point. These supplementary description files, containing the OpenAPI specification for each API defined in the present document, are located at https://forge.etsi.org/rep/nfv/SOL023/.

In case of discrepancies between the supplementary files and the related data structure definitions in the main body of the present document, the data structure definitions take precedence.

The OpenAPI representations referenced above:

1) use the MAJOR.MINOR.PATCH version fields to signal the version of the API as defined in the present document; and

2) use the "impl" version parameter (see clause 9.1.2 of ETSI GS NFV-SOL 013 [4]) to represent changes to the OpenAPI representation without changing the present document.

It is specified in clause 6 of ETSI GS NFV-SOL 015 [i.7] how the OpenAPI specification references the present document and signals the version information.

Annex E (informative): Change history

Date	Version	Information about changes
February 2024	V0.0.1	First version providing the document skeleton and scope.
March 2024	V0.0.2	Contributions incorporated: • NFVSOL(24)000071r1 "SOL023 MegaCR for milestone1"
May 2024	V0.0.3	Contributions incorporated: • NFVSOL(24)000118r1 "SOL023 MegaCR for milestone2"
September 2024	V0.0.4	Contributions incorporated: • NFVSOL(24)000227r2 "SOL023 MegaCR for milestone3"
October 2024	V0.0.5	Contributions incorporated: • NFVSOL(24)000256r1 "Enh01.01 SOL023 Annex Mapping operations to protocol" • NFVSOL(24)000263 "Enh01.01 SOL023 Annex Authorization scope value" • NFVSOL(24)000270r1 "SOL023 MegaCR for milestone4"
October 2024	V0.0.6	Contributions incorporated: • NFVSOL(24)000339 "Enh01.01 SOL023 Query flow" • NFVSOL(24)000340r1 "Enh01.01 SOL023 Query Subject" • NFVSOL(24)000341 "Enh01.01 SOL023 Query Certificate" • NFVSOL(24)000342r1 "Enh01.01 SOL023 Revoke operation" • NFVSOL(24)000343 "Enh01.01 SOL023 Notification interface" • NFVSOL(24)000359r1 "Enh01.01 SOL023 Notification datatype" • NFVSOL(24)000372 "SOL023 – some smaller updates" • NFVSOL(24)000374 "SOL023 miscellaneous editorial fix"
November 2024	V0.0.7	Contributions incorporated: • NFVSOL(24)000394 "SOL023 unsupported update certificate" • NFVSOL(24)000395 "SOL023 refactoring CSRRequest" • NFVSOL(24)000396r1 "SOL023 resolve EN of CMP study" • NFVSOL(24)000398 "SOL023 review contribution - certificate notification interface" • NFVSOL(24)000411 "SOL023 resolve EN of subjectId and certificateId" • NFVSOL(24)000412 "SOL023 resolve EN of OID" • NFVSOL(24)000413 "SOL023 add error-handling" • NFVSOL(24)000414 "SOL023 Milestone 5 SEC contributions" • NFVSOL(24)000423 "SOL023 resolve EN of Authenticated Scheme" • NFVSOL(24)000428 "SOL023 review contribution - certificate management interface" • NFVSOL(24)000435 "SOL023 SEC Changes from NFVSEC#275"
March 2025	V0.0.8	Contributions incorporated: • NFVSOL(25)000049 "SOL023 refactoring to the profiling CMPv2" • NFVSOL(25)000056 "SOL023 URIs structure" • NFVSOL(25)000066 "SOL023 5.5.2.2 PKIMessage structure" • NFVSOL(25)000067r1 "SOL023 5.5.2.3 PKIHeader structure" • NFVSOL(25)000069r1 "SOL023 5.5.2.4 PKIBody structure" • NFVSOL(25)000070r1 "SOL023 5.5.2.5 Certification Request structure"
April 2025	V0.0.9	Contributions incorporated: • NFVSOL(25)000098 "SOL023 comparison of CMF interface and ACME" • NFVSOL(25)000099 "SOL023 comparison of ACME operation" • NFVSOL(25)000100 "SOL023 update comparison for IFA033ed521" • NFVSOL(25)000111r1 "SOL023 Update Resource structure" • NFVSOL(25)000112 "SOL023 Update profile of CMPv2 message structure" • NFVSOL(25)000113 "SOL023 Refactor registration"
May 2025	V0.0.10	Contributions incorporated: • NFVSOL(25)000119 "SOL023 Refactor flow" • NFVSOL(25)000120 "SOL023 Update Annex" • NFVSOL(25)000128 "SOL023 Clause 4.1 Introduction" • NFVSOL(25)000129 "SOL023 Clause 5.5.1 Introduction" • NFVSOL(25)000130 "SOL023 Clause 5.5.2.3 Update PKIHeader" • NFVSOL(25)000131r1 "SOL023 editorial change of reference and clause number"
May 2025	V0.0.11	Contributions incorporated: • NFVSOL(25)000139r1 "SOL023 Clause A.6 Update analysis and conclusion for ACME" • NFVSOL(25)000141 "SOL023 ACME analysis clarification note"

Date	Version	Information about changes
June 2025	V0.0.12	Contributions incorporated: • NFVSOL(25)000182 "SOL023 Clause 5.6.3.3.3.2 Resolve Editor's Note" • NFVSOL(25)000183 "SOL023 Clause 5.6.4.2.2 Resolve Editor's Note" • NFVSOL(25)000184 "SOL023 update reference" • NFVSOL(25)000185r1 "SOL023 improve scope and add OpenAPI" • NFVSOL(25)000186 "SOL023 bulk editorial changes"
July 2025	V0.0.13	Editorial changes: • adding "_" in clause 5.6.2.2 • change title in clause 5.6.2.2 • change clause number in clause 5.6.2.2 • typo in clause A.5.2, 5.6.3.3, 5.6.3.4, 7.6.3.3 and 7.6.3.4
September 2025	V5.3.1	Version update for publication
November 2025	V5.3.2	Contributions incorporated: • BWC:NFVSOL(25)000322 "SOL023 Update reference IETF RFC for CMP" • BWC:NFVSOL(25)000362 "SOL023ed541 Add clarifying note to Annex A" • BWC:NFVSOL(25)000365r1 "SOL023 AnnexA ACME Profiling" • BWC:NFVSOL(25)000366r1 "SOL023 4.2.2 ACME Summary" • BWC:NFVSOL(25)000367 "SOL023 5.2 ACME Operation Mapping" • BWC:NFVSOL(25)000407 " SOL023 5.2 ACME Operation Mapping QuerySubjectInfo_QueryCertInfo" • BWC:NFVSOL(25)000408 "SOL023 AnnexA MANO certificate consideration for SCEP/EST" • BWC:NFVSOL(25)000409 "SOL023 Update reference IETF RFC for CMP"
December 2025	V5.3.3	Contributions incorporated: • BWC:NFVSOL(25)000403 "SOL023 5.3 Add Sequence diagrams for MANO certificate " • BWC:NFVSOL(25)000441 "SOL023ed541 5.3 Add Query Sequence diagrams for MANO certificate" • BWC:NFVSOL(25)000451 "SOL023 4.2.1.4/4.2.2.4 CMP/ACME entities mapping" • BWC:NFVSOL(25)000453 "SOL023 5.5.x ACME input parameter Mapping" • BWC:NFVSOL(25)000454 "SOL023 5.5.x ACME output parameter Mapping" • BWC:NFVSOL(25)000455 "SOL023 Annex A MANO certificate consideration for CMP" • BWC:NFVSOL(25)000462r1 "SOL023 Challenge aspects as ACME specific feature"
February 2026	V5.3.4	ETSI Technical Officer review

History

Version	Date	Status
V5.3.1	September 2025	Publication
V5.4.1	April 2026	Publication