ETSI TS 104 000 V1.2.1 (2025-05)

Lawful Interception (LI);
Internal Network Interface X0

Reference
RTS/LI-00283

Keywords
configuration, interface, lawful interception,
security, security requirements

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 Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

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.

Executive summary

The present document specifies the X0 interface as part of a Lawful Interception (LI) system using the ETSI LI architecture. The purpose of the X0 interface is to provide the functions needed to further setup the interfaces for LI functions in the networks like X1, X2 and X3. The X0 interface also contains the functions to bootstrap the trust relations as required by the LI architecture. As part of the present document the provisioning and configuration of the certificates needed for the HTTPS connections are detailed. Also, a mechanism to provision a decryption key for encrypted payloads is specified.

The present document focusses on the functions for X0. The additional configuration of the X1, X2 and X3 interfaces that is facilitated through the X0 connection is specified in the specifications of these interfaces (ETSI TS 103 221-1 [3] and ETSI TS 103 221-2 [16]).

1 Scope

The present document defines an electronic interface for the exchange of information relating to the establishment and management of Lawful Interception. Typically, this interface would be used between a central LI administration function and the network internal interception points.

Typical reference models for LI define an interface between Law Enforcement Agencies (LEAs) and Communication Service Providers (CSPs), called the handover interface. They also define an internal network interface within the CSP domain between administration and mediation functions for lawful interception and network internal functions, which facilitates the interception of communication. This internal network interface typically consists of sub-interfaces; initial configuration of the network internal elements of lawful interception (X0), administration (called X1), transmission of intercept related information (X2), transmission of content of communication (X3).

The present document specifies the X0 interface for configuration of the network elements of lawful interception.

It also covers the needs of the virtualized environments and specifies the initial trust establishment of the LI interfaces to secure that LI functions get identities (certificates) for LI only after being verified (e.g. using attestation) and endorsed for LI use.

The present document is tightly related to the ETSI Lawful Interception Architecture, ETSI TS 104 007 [2]. ETSI TS 104 007 [2] describes the architecture for the LI system and the new X0 interface used for building trust and setup of the X1/2/3 interfaces, the present document specifies the role and detailed definition of interface X0 and how it couples with interfaces X1/2/3. The present document and ETSI TS 104 007 [2] plug together and give a complete model of the LI system.

X0 is characterized in standard documents ETSI GR NFV SEC-011 [i.1] and 3GPP TS 33.127 [i.3] through descriptions and requirements.

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] Void.

[2] ETSI TS 104 007: "Lawful Interception (LI); Lawful Interception Architecture".

[3] ETSI TS 103 221-1: "Lawful Interception (LI); Internal Network Interfaces; Part 1: X1".

[4] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architecture enhancement for Security Management Specification".

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

[6] IETF RFC 9112: "HTTP/1.1".

[7] IETF RFC 9113: "HTTP/2".

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

[9] ETSI TS 133 210 (V10.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[10] W3C® Recommendation 28 October 2004: "XML Schema Part 2: Datatypes Second Edition".

[11] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

[12] IETF RFC 4122: "A Universally Unique Identifier (UUID) URN Namespace".

[13] ETSI TS 103 280: "Lawful Interception (LI); Dictionary for common parameters".

[14] Void.

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

[16] ETSI TS 103 221-2: "Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3".

[17] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[18] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

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-SEC 011: "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[i.2] ETSI GR NFV-EVE 022: "Network Functions Virtualisation (NFV) Release 5;Architectural Framework; Report on VNF configuration".

[i.3] ETSI TS 133 127: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Lawful Interception (LI) architecture and functions (3GPP TS 33.127)".

[i.4] ETSI GS NFV-SOL 002: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; RESTful protocols specification for the Ve-Vnfm Reference Point".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

attestation: action of a component to respond to an attestation request of a (remote) verifier with a response (also called a quote) that via a digitally signature links the response data to an identity coupled to the component with a predetermined (or indicated in the request) selection of the state variables of the component

Attestation Verifier Service (AVS): collection of functions and components that are involved in the attestation of an LI component in the Network Function

Certificate Authority (CA): system that is responsible to manage a Public Key Infrastructure (PKI) and which offers services to register end-entities and to perform certificate management functions for these end-entities such as enrolment, certificate renewal

Certificate Management Function (CMF): ETSI function that mediates between a CA (the LICA) and the ADMF to register the LI required end-entities for LI certificates in the CA as the ADMF establishes the LI interface instances for X0, X1, X2 and X3

day-0: initial configuration of a component like a network entity or LI component when it is deployed and instantiated

end-entity (certificate): leaf certificate in a PKI being either a client or server certificate

LI component: function and equipment involved in handling the Lawful Interception functionality in the CSP's network

LI Security Engine (**LISE):** manages the network-wide security primitives (keys, nonces, salts, etc.) needed by the LI network functions

LI system: collection of all LI components involved in handling the Lawful Interception functionality in the CSP's network

Network Element (NE): element performing the LI operations such as interception, or mediation and delivery. The NE may be embedded in a NF or standalone

Network Function (NF): function performing network operation such as 3GPP network functions

provisioning: action taken by the CSP to provide its Lawful Interception functions information that identifies the target and the specific communication services of interest to the LEA, sourced from the LEA provided warrant

triggering: action taken by a dedicated function (Triggering Function) to provide another dedicated function (triggered POI), that direct provisioning from the LIPF could not directly be applied to, with information that identifies the specific target communication to be intercepted

X1: LI interfaces internal to the CSP for management tasking

X2: LI interfaces internal to the CSP for xIRI delivery

X3: LI interfaces internal to the CSP for xCC delivery

X*n*: collective name for the interfaces other than X0, for which X0 can be used to establish trust, provision and retrieve configuration information i.e. X1, X2 and X3

3.2 Symbols

Void.

3.3 Abbreviations

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

5G	3GPP fifth generation cellular network
ADMF	ADMinistration Function
API	Application Programming Interface
ARP	Attestation Relying Party
AVS	Attest Verifier Service
CA	Certificate Authority
CC	Content of Communication
CISM	Container Infrastructure Service Management
CMF	Certificate Management Function
CMP	Certificate Management Protocol

CSP	Communication Service Provider
CSR	Certificate Signing Request
ELI	Element of Lawful Interception
ELIID	ELI IDentifier
ELIReference	ELI Reference
FQDN	Fully Qualified Domain Name
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over TLS
IAK	Initial Authentication Key
IMK	IMage Key
IP	Internet Protocol
IPR	Intellectual Property Rights
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LI	Lawful Interception
LICA	Lawful Interception Certificate Authority
LICREPF	Lawful Interception Configuration REPository Function
LIPF	Lawful Interception Provisioning Function
LISE	Lawful Interception Security Engine
MANO	NFV MANagement and Orchestration
MDF	Mediation and Delivery Function
mTLS	TLS with client authentication
NE	Network Element
NF	Network Function
NFIID	Network Function Instance IDentifier
NFReference	Network Function Reference
NFV	Network Functions Virtualisation
OSS/BSS	Operations Support System and Business Support System
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POI	Point Of Interception
SAN	Subject Alternative Name
SDO	Standards Development Organizations
SW	SoftWare
TF	Triggering Function
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universal Unique IDentifier
VNF	Virtual Network Function
X0ID	X0 IDentifier
X0PUB	X0 PUBlic key
XML	eXtended Markup Language
XSD	XML Schema Definition

4 Reference model

4.1 Overview

X0 provides a means of establishing trust between an LI Administration Function (ADMF) and an Element of LI (ELI) created in a network and allows configuration of the ELI for other LI interfaces ("X*n*").

This involves a sequence of phases, described in table 4.1-1 below.

Table 4.1-1: Phases of the X0 reference model

#	Phase	Description
0	Pre-configuration	Deals with initial day-0 configuration of both the ELI and ADMF.
1	NF Discovery	Deals with the ADMF discovering that an NF has been deployed and is starting and checking against configured information about this NF.
2	Attestation	Remote attestation of a newly created ELI by the ADMF (interfaces X0_a and X0_v).
3	Trust bootstrap finalization	The initial trust establishment process of an attested identifier and asymmetric key in the ELI for use in the initial trust relation between ADMF and ELI (interface X0_r).
4	Registration and X0 Certificate Enrolment	The ELI and ADMF establish direct trust between each other (interfaces X0_cert and X0_cmf).
5	X0 and X*n* Configuration	The ELI acquires any remaining configuration information required by the X0 procedures as well as configuration information required for operation of the X*n* interfaces (interface X0_c).
6	X*n* Certificate Provisioning	The ELI acquires certificates for use by X*n* interfaces (X0_c).
7	Image key insertion and decryption (optional)	The ADMF provisions the ELI with an image decryption key for decryption of encrypted SW image and configuration blobs (interface X0_c).

The reference model in which these phases occur is given in figure 4.1-1 below. It forms part of the wider LI architecture defined in ETSI TS 104 007 [2].

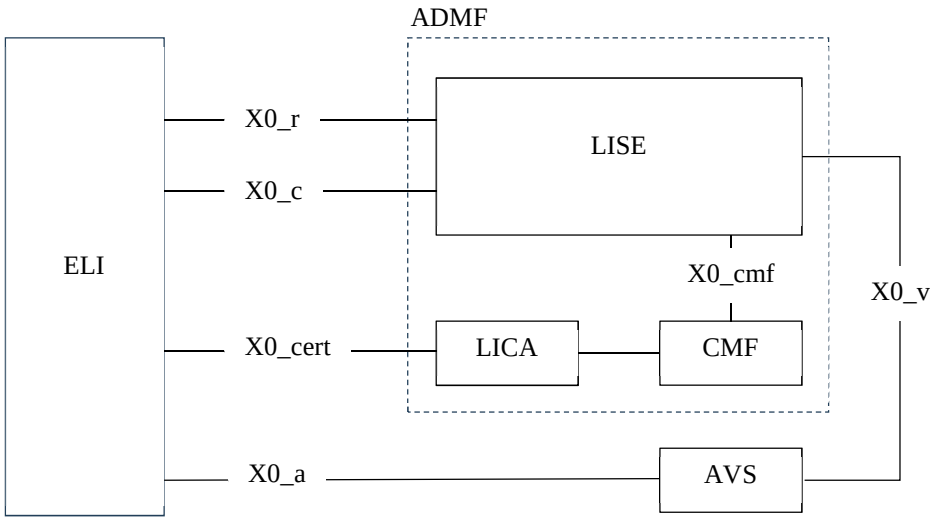

Figure 4.1-1: X0 Reference model

The logical components of this model are described in table 4.1-2 below.

Table 4.1-2: Components of the X0 reference model

Component	Name	Description
ELI	Element of Lawful Interception	Functional element responsible for some aspects of interception (e.g. a POI or MDF), which therefore requires configuration by the ADMF via X0. An ELI is defined as a set of X*n* interfaces (see clause 4.2) configured and controlled via a single X0 interface.
LISE	LI Security Engine	Element of the ADMF responsible for configuration of ELIs via X0. Contains the LICREPF (LI Configuration Repository Function) and the Attestation Relying Party that interacts with the AVS. See ETSI TS 104 007 [2], clause 6.6.2.
LICA	LI Certificate Authority	Certificate Authority used to sign LI-related X.509 [11] certificates. See ETSI TS 104 007 [2], clause 6.6.2.
CMF	Certificate Management Function	Responsible for configuring certificate enrolment of ELIs. ETSI TS 104 007 [2], clause 6.6.2.
AVS	Attestation Verifier Service	Responsible for providing attestation services towards both the ELI (as an attesting party) and the ARP in LISE (as a verifying party). See ETSI TS 104 007 [2], annex B.

The interfaces in this model are described in table 4.1-3 below.

Table 4.1-3: Interfaces in the X0 reference model

Interface	Description
X0_r	Used to build initial trust between a newly started ELI and the ADMF during the Registration phase (see clause 5.6). The protocol used to realize this interface is defined through the messages defined in clause 5.6 and associated parameters defined in clause 6.
X0_c	Used to exchange configuration-related information in the X0 and X*n* Configuration phases (see clauses 5.6 and 5.7). The protocol used to realize this interface is defined in clause 6.
X0_cert	Used to perform certificate enrolment by the ELI via the LICA as part of the Registration and Certificate Enrolment phase (see clauses 5.6 and 5.8). The present document supports the use of CMP (see annex C), but other protocols which meet the functional requirements of X0_cert may be chosen as an implementation option.
X0_a	Used to attest the ELI to the AVS during the Attestation phase (see clause 5.4). The protocol used to realize this interface is out of scope of the present document but shall be able to support the information elements required by the present document.
X0_cmf	Used by the LISE to manage certificate enrolment via the CMF for both X0 and X*n* certificate enrolment (see clauses 5.6 and 5.8). The protocol used to realize this interface is out of scope of the present document but shall be able to support the information elements required by the present document.
X0_v	Used by the LISE to verify the attestation results of an ELI during the Attestation phase (see clause 5.4). The protocol used to realize this interface is out of scope of the present document but shall be able to support the information elements required by the present document.

While this specification of X0 is designed to make use of attestation for trust bootstrapping between the ELI and the ADMF, this trust bootstrap can be provided through configuration of ELI credentials that otherwise would have been obtained through attestation, see clause 5.5.2 for more details. X0 Phase 0 (pre-configuration, see table 4.1-1) requires the ADMF to be provided configuration information that describes the set of interfaces for the type of ELI that may be instantiated. Table 4.1-4 gives the minimum set of information that is required to be provided. The means by which this information is provided is out of scope of the present document.

Table 4.1-4: ELI configuration information

Name	Description	Format
ELIReference	Identifier that uniquely identifies the configuration information for an ELI. Matches that provided by the ELI during registration (see clause 6.2.3.1).	UUID, (ETSI TS 103 280 [13], clause 6.27).
NFReference	Identifier that uniquely identifies the NF that contains the ELI. Matches that provided by the ELI during registration (see clause 6.2.3.1). May be omitted for ELIs that are not part of an NF (e.g. an MDF).	UUID, (ETSI TS 103 280 [13], clause 6.27).
Interfaces	See table 4.1-5.	List of interface configuration information (see table 4.1-5).

Table 4.1-5: ELI interface configuration information

Name	Description	Format
InterfaceReference	Identifier that uniquely identifies a specific interface within a given ELI. Used by the ELI and ADMF to identify he relevant interface during certificate enrolment (see clauses 6.2.3.2 and 6.2.4).	ShortString, (see ETSI TS 103 280 [13], clause 6.29).
InterfaceType	Identifies the type of interface and the role of the ELI within that interface.	CertificateProfileInterfaceType (see clause 6.2.4).

NOTE: Multiple ELI can be instantiated with the same ELIReference.

4.2 Relationship with X*n* interfaces (X1, X2 and X3)

Since there can be several X*n* interfaces coupled to the ELI, the client certificate associated with the X0 interface is used as the ELI identity, and the client certificates for X1, X2, X3, etc. are logically linked to the X0 client certificate by requiring that the certificate signing requests go over the mTLS connection between ELI and LISE. LISE may use this mechanism to explicitly link an X0 instance to the certificates for the other X interfaces.

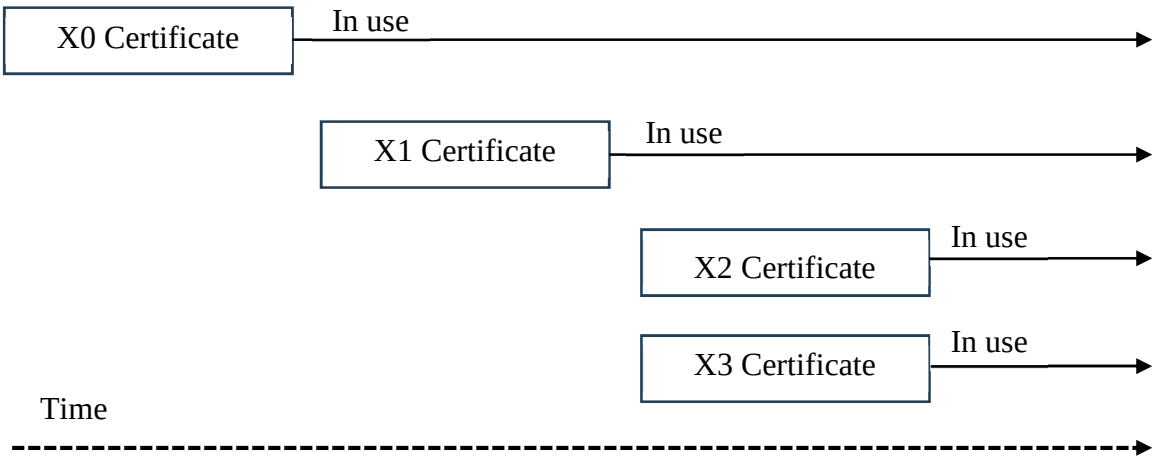

Figure 4.2-1: Stepwise provisioning of ELIs X*n* certificates

It is a deployment choice if the certificates in figure 4.2-1 are distinct. Since the X0 interface serves an infrastructural setup purpose rather than an LI operational purpose, it is good security practice to distinguish between an X0 certificate and X1, X2, X3 certificates.

5 Procedures

5.1 Phases

When the network function is instantiated, the X0 interface shall be configured. To achieve this, the instantiation process shall use mechanisms beyond the X0 interface itself. On the other hand, to have as much as possible of the configuration of X0 to use the X0 interface itself, the instantiation is performed in phases as described below. The phases are the ones summarized in table 4.1-1:

- Phase 0 deals with the configuration of the URIs of the ADMF, the AVS and the trust anchor certificates (e.g. root certificates) for the TLS connection from the X0 instance in ELI to the LISE X0 resource. This configuration is a day-0 configuration of the ELI X0 interface. See also annex D.
- Phase 1 deals with the ADMF discovering the deployed NF by using notifications from the MANO/CISM and checking if this NF is one of the NFs that has been configured as having ELI functions.
- Phase 2 deals with the remote attestation of the ELI/X0 instance. This phase is embedded in the launch process of the X0 instance in the ELI. It leaves the result of the attestation in the AVS that was pointed at in the day-0 configuration that the ARP in the LISE collects for LI.
- Phase 3 deals with the ADMF correlating the attestation to the discovered NF and if attestation and discovery aligns creates an active X0 context in the ADMF for LISE. It finalizes the trust bootstrap of the ELI X0 instance.
- In phase 4 the X0 interface in the ELI connects to LISE via HTTPS using a self-signed certificate as client certificate. Note that at this point this client certificate is not issued by the LICA PKI that the ELI can use for authentication. The ELI X0 instance pulls the required additional configuration data from the LICREPF repository to create a private-key pair for a client certificate that the ELI can subsequently use and performs the necessary steps with the ADMF and the LICA to achieve certificate enrolment. From this point onwards the repository will only expose configuration data via the mutually authenticated X0 connection.
- Phase 5 starts with the ELI X0 instance switching the special client certificate for HTTPS to one issued from the LICA PKI in phase 4 for the HTTPS connection to LISE and pulls the last missing configuration data. The LISE shall enforce that any further communication is done via HTTPS using LICA PKI signed certificates. Note that because phase 5 encompasses a trusted client certificate, from the LICA PKI this situation can also be leveraged to authorize the LISE to expose more specific ELI configuration information. During this phase configuration data for X0 and subsequently for X*n* interfaces are provided.
- In phase 6 the certificates for the X*n* interfaces certificates are enrolled and delivered.
- Phase 7 addresses the case where LEAs may require to hold back the start of an entire ELI before the LEA has received assertions that the ELI can be trusted to run the LI code securely or the LEA does require the LI code to be not visible to anyone in the operator or 3rd party support estate, where many non-LI actors have access to the software catalogues. To support an increased security, implementations of an ELI may distribute the core ELI functionality as an encrypted image (e.g. VM or container image) for which the ADMF possess the key. The ELI is encrypted by the ELI vendor prior to loading into the software catalogues. Such encrypted image or encrypted configuration data may be decrypted by an ELI base component or loading component that is started first in the NF through the procedures previously described. The decryption requires the ADMF to provide an image decryption key to the ELI. Through the use of the X0 interface, LEAs have a secure mechanism to assess if they trust the ELI to receive the key. In phase 7, an image decryption key can be provisioned into the ELI by the ADMF.

ELIs are usually part of an NF but may also exist on their own. An NF can include one or more ELIs. An ELI contains one or more LI Functions (e.g. IRI-POI, CC-POI, CC-TF, MDF). For example, an NF can include a single ELI where the single ELI can include an IRI-POI and a CC-POI. As another example, an NF can include two ELIs where one ELI contains an IRI-POI, and another ELI contains a CC-TF. Each ELI in an NF will have its own unique X0 interface instance. Therefore, if for example an NF has 3 ELIs it will have 3 different X0 interface instances, one per ELI. This can be summarized as:

1) An NF may contain zero or more ELIs.

2) An ELI has a single X0 interface.

3) An ELI has zero or more X1, X2, X3 interfaces in either direction.

4) An ELI may exist outside of an NF.

Clause 5 flows consider the case of a single ELI in the NF. In case of multiple ELIs in one NF, at the NF instantiation the flow described per single ELI applies and is repeated for each ELI present in the NF.

5.2 Pre-configuration (Phase 0)

Prior to the creation of an X0 interface between the ADMF and the X0 interface instance in an ELI, several configurations shall take place at both ends of the X0 connection. Since this configuration takes place before the NF with the associated ELI function is instantiated, these configurations are referred to as X0 pre-configuration.

The network function and its ELI shall be configured with information that the ELI in the NF can use to connect securely to the target LISE in the ADMF and the X*n* interfaces. This information will be:

- The URIs of the relevant X0 and X1 resources in the ADMF (or interface therein), see note 1.
- The trust anchor certificates to be used when setting up a secure connection to the LISE, see note 2.
- The NFReference to reference to the LI related NF configuration at the ADMF.
- The ELIReference for the ELI which shall be scoped through the NFReference.
- The NFIID being the identifier of the deployed NF instance as recognized by the ADMF. The NFIID, and NFReference shall be unique identifiers, also in multivendor deployments. For NFIID see ETSI TS 104 007 [2] and note 3.
- The configuration of the ELI required X*n* interfaces, see table 4.1-5.

NOTE 1: The X0 and X1 resources are typically a list of ADMFs, for redundancy and improved availability, containing their addresses in form of IP addresses and ports or URLs.

NOTE 2: The trust anchors are not only used for LISE but also to the LICA enrolment server(s) and the ADMF for other *Xn* interfaces. Trust anchors are provided for the X0, X1, X2, X3 connections as well as to the LICA enrolment server(s). It is up to the discretion of the LI operations to use the same trust anchors for all these interfaces or to use different ones. Trust anchors are configured using trust anchor lists or trust stores that contain one or more trust anchors.

NOTE 3: The NFIID is an identifier given to the NF instance, e.g. by the orchestration and deployment layer.

The present document requires the possibility to configure the NFIID and NFReference into the NF by OSS/BSS. Deployments can, when possible, reuse existing identifiers, such as 3GPP nfInstanceID. See annex D for more information on Phase 0 and the NFReference.

The required configuration of the AVS with its ground-truth parameters is out of scope of the present document. Nevertheless, the AVS should be informed of the deployment of the NFIID that is given to the NF.

The present document assumes that the ELIReference, see clause 6.2.3, is carried by the ELI itself (e.g. hard-coded or (pre)configured), and does not need to be configured via the X0 interface.

Furthermore, TIME1X0 and TIME2X0 as defined in clause 6.1.3 shall be pre-configured.

The pre-configuration of the NF is done via so-called day-0 configuration of the NF on NFV configuration, see ETSI GR NFV-EVE 022 [i.2].

The URI for LISE is the LISE resource in the ADMF: e.g. https://ADMF-FQDN/X0/ADMF/LISE/.

5.3 NF Discovery (Phase 1)

When the NF is instantiated through orchestration via MANO/CISM the ADMF will receive notifications containing information of the new instance. It is assumed that in phase 0 ADMF has subscribed to MANO/CSIM to receive such notifications and the LIPF in the ADMF will handle the notifications, see ETSI TS 104 007 [2].

NOTE: Compliance on this interface to the present document and the architecture defined in ETSI TS 104 007 [2], can be based on using the interface Ve-Vnfm-em interface in ETSI NFV-SOL 002 [i.4].

The LIPF controller performs several checks to see whether there is a match in the controller information that the NF contains ELIs. If this is the case, there shall be an X0 instance state as well as an X0 context defined in LISE, and these shall be configured with X0 configuration data. The LIPF will update the X0 context with the MANO/CISM provided information.

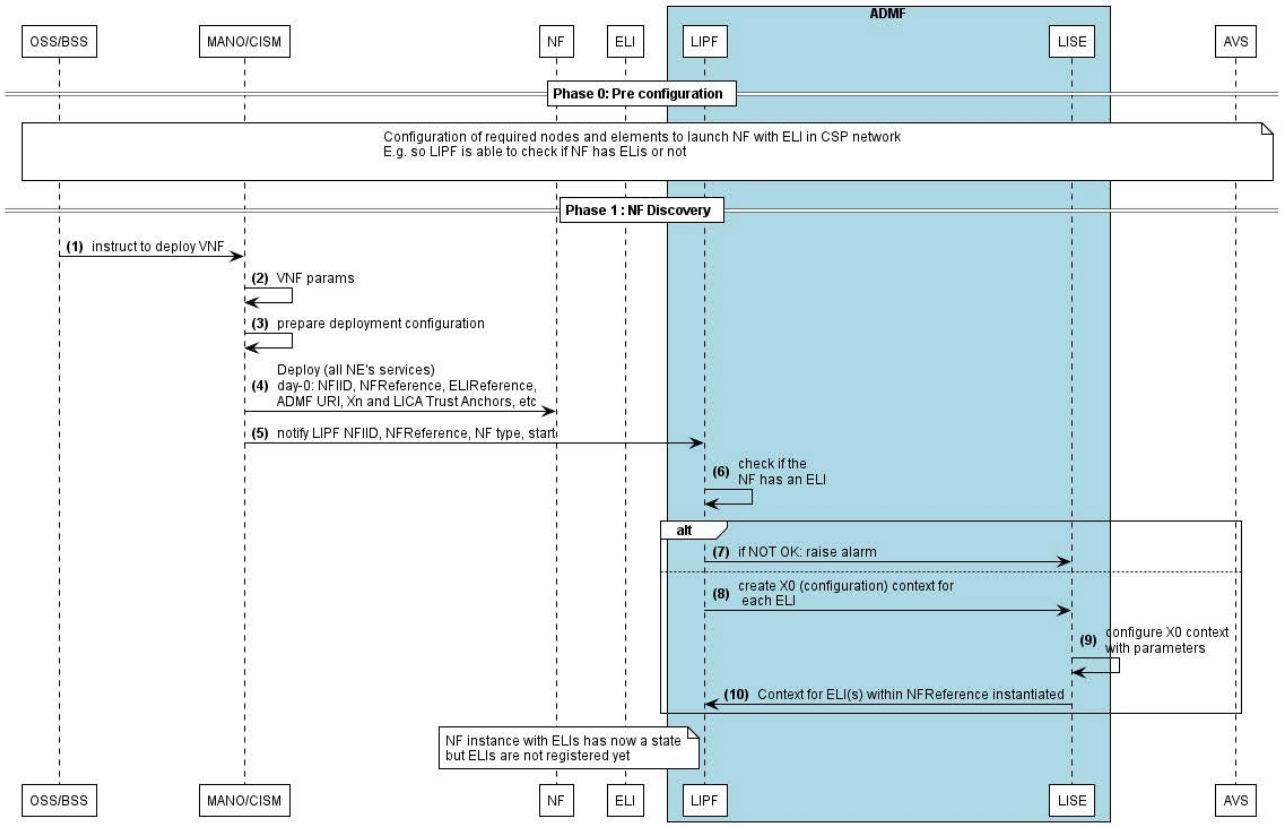

Figure 5.3-1: Phase 0 and NF discovery of phase 1

5.4 Attestation (Phase 2)

The X0 interface instance and ELI will conduct attestation operations. As a result, the AVS will provide the ARP in LISE with:

- The result of attestation (successful or failure, and time of attestation).
- A randomly created identifier associated with the attested interface instance and NFIID.
- A public-key referred as X0PUB, that is associated to the attested instance (ELI/X0 instance).

The association of an attribute, like in the case the attribute is the identifier of a public key, means that the attestation checks the attribute value. E.g. in case the identifier is a hash of the public key, the hash of the value in the attestation report is compared against so-called ground-truth values. See the LI architecture ETSI TS 104 007 [2].

All the required interactions do not involve the X0 interface, but instead use either existing interfaces between MANO and ADMF or interfaces between attester and AVS. For the latter see the LI architecture ETSI TS 104 007 [2].

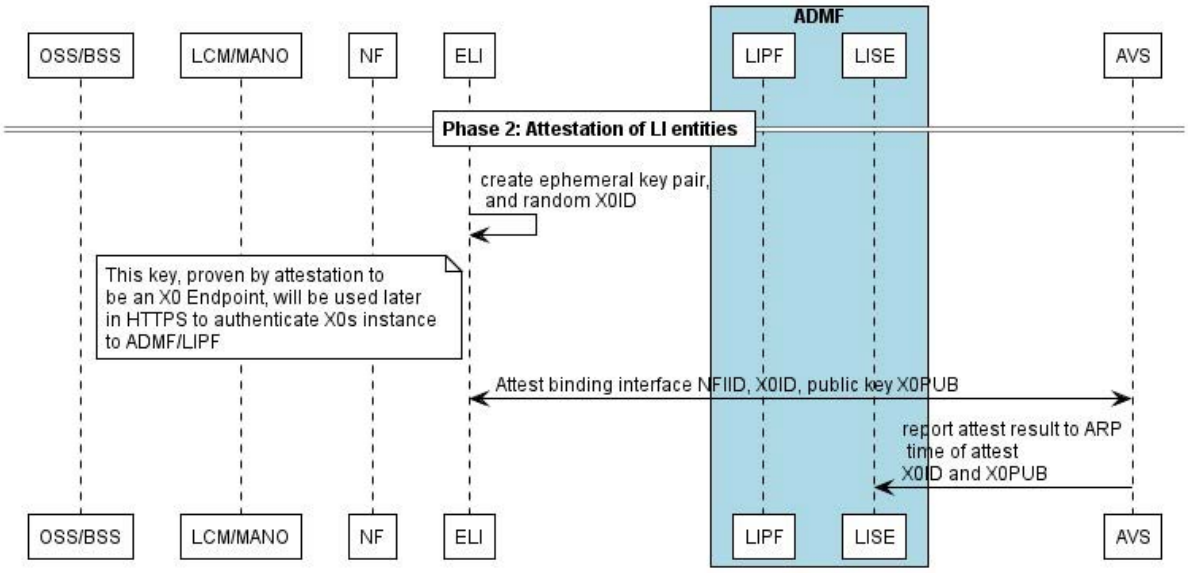

Figure 5.4-1: Attestation during phase 2

5.5 Trust Bootstrap finalization (Phase 3)

5.5.1 Procedure

Having performed the discovery and the attestation having been conducted, the LIPF can check if the attest and the identifiers of the NF line-up, thus indicating that a trusted X0 instance is present in the NF where the X0 has an X0PUB. The X0PUB is a public portion of a public-private key pair supporting authentication. This private-public key pair shall be used to create a self-signed certificate as described in clause 8.4.

The ADMF can create an X0 context for use by LISE to perform the registration of the ELI(s) in the NF.

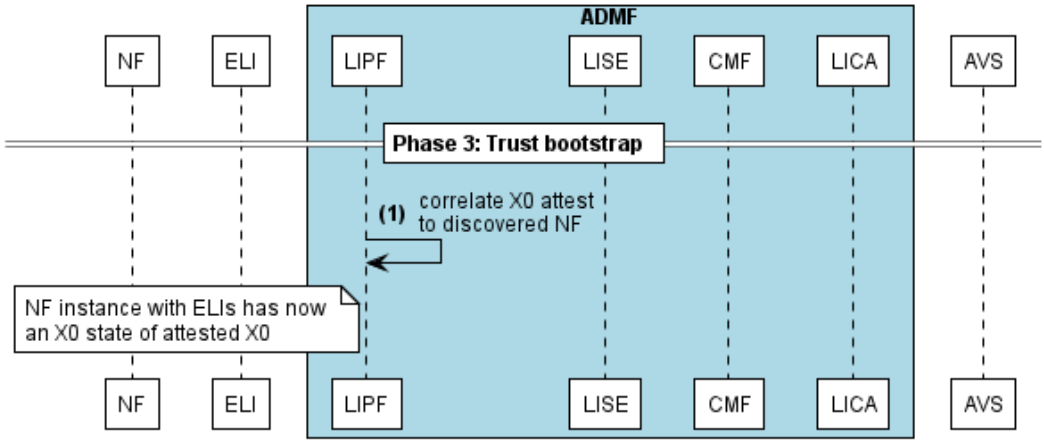

Figure 5.5.1-1: Trust bootstrap of the X0 context

5.5.2 Trust bootstrap without attestation

This clause describes which provisions need to be made to make X0 trust bootstrap work without attestation. The result of the attestation is that the LISE later can consult the AVS to check the identifiers and the X0PUB key. The LISE can perform its task for the X0 trust bootstrap if it is configured with these parameters. The details can be found in figure 5.6.2-1, step 4: NFIID, X0ID and X0PUB.

5.6 Registration and certificate provisioning (Phase 4)

5.6.1 Procedure

After the NF is up and running, the X0 in ELI starts the interactions to obtain a certificate for X0 from the LICA on the basis that the ADMF has attested the ELI X0 interface instance. The interactions are grouped into the following steps:

- First the ELI creates a self-signed X509 certificate using the key pair whose public key has been attested as X0PUB. The self-signed certificate shall comply to the certificate profile in clause 8.4.
- Then the ELI through its X0 interface connects via HTTPS to LISE in the ADMF using the self-signed certificate. This requires the LISE to have an X0 server interface that accepts self-signed certificates as client certificates. LISE can check that the client certificate of ELIs X0 is using X0PUB as public key. The ELI X0 interface also sends the NF and X0 identifiers as well as the supported certificate enrolment protocols.
- The LISE interacts with the CMF to have the LICA prepared for the certificate provisioning.
- LISE configures the ELI X0 certificate parameters such as subject name and Subject Alternative Name (SAN) entries, binding parameters, and shared the certificate enrolment protocol which was selected.
- The ELI X0 creates a new public key pair and uses the provided certificate parameters to create a certificate signing request to be used by the selected certificate enrolment protocol.
- The ELI X0 and the LICA interact using the certificate enrolment protocol to obtain the X0 certificate from the LICA.

Figure 5.6.1-1 provides an overview of the previously mentioned steps.

When the ELI and LISE exchange X0 messages, these X0 messages shall carry the fields as defined in clause 6.2.1:

- ADMF identifier.
- ELI identifier.
- Message Timestamp.
- Version (of the present document used to encode the message).
- X0TransactionID.

In the subsequent flows these fields will not be shown.

The ELI shall check if the provisioned certificates meet the certificate profile for X0 as specified in clause 8 by inspecting if the required attributes are present. If the check is not successful, ELI shall respond with an error indicating that the provisioned data is in error. Similarly, an ELI shall check the provisioned certificates for the X*n* interfaces using, where relevant, the certificate profile for these interfaces. E.g. for X1 the requirements for X1 interface certificates as specified in ETSI TS 103 221-1 [3].

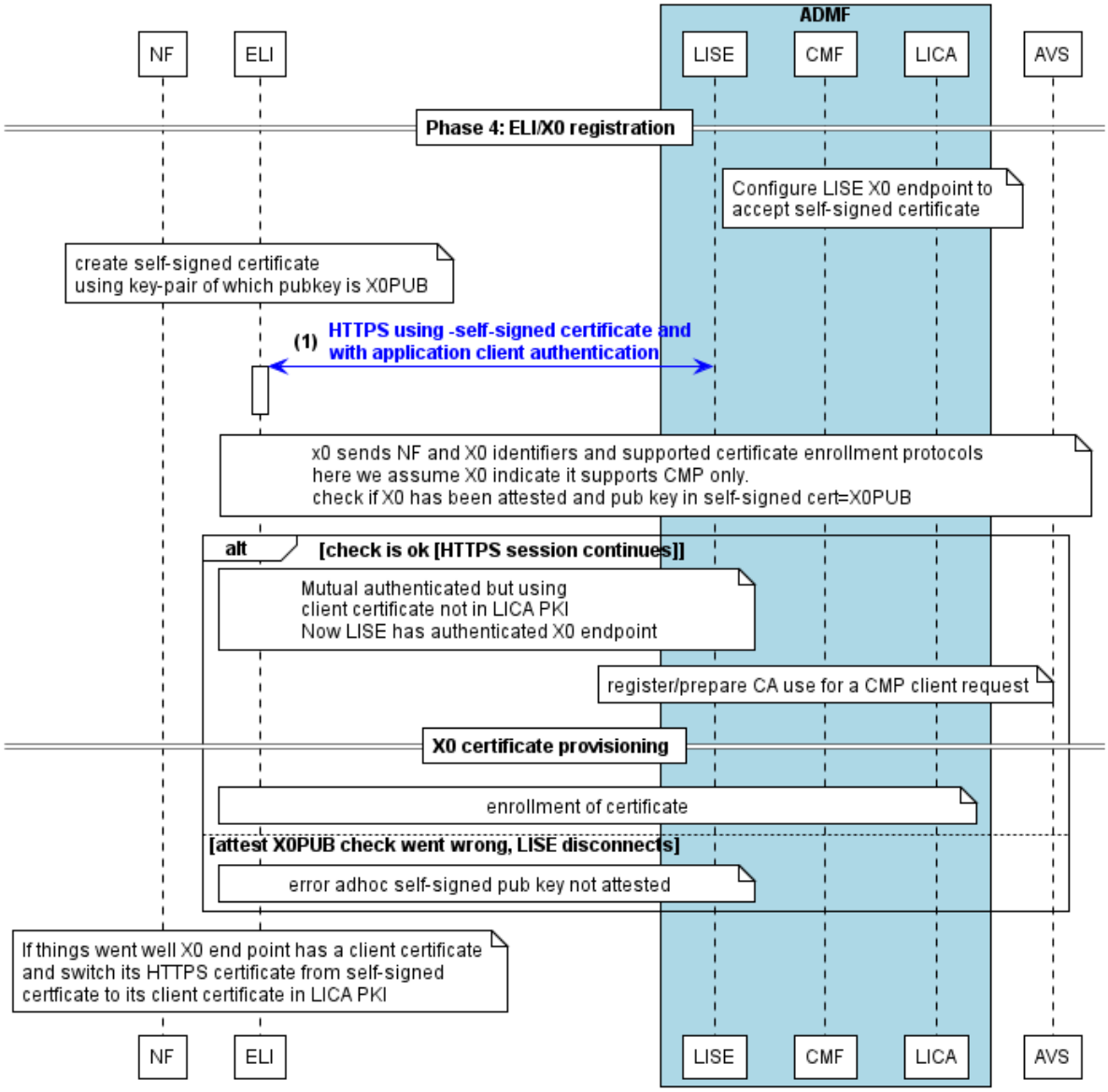

Figure 5.6.1-1: Overview of Interaction steps for getting an X0 certificate from the LICA PKI into the ELI using the X0 channel

Figure 5.6.2-1 shows more details of the steps of figure 5.6.1-1 assuming CMP use. The X0 instance utilizes the temporary X0 client certificate with the public key which was reported in the attest report as X0PUB. This start is step 1 in figure 5.6.2-1.

The ELI X0 uses the self-signed certificate as client certificate when connecting via HTTPS to LISE with the purpose to register the ELI in the context of the LICPREF that was prepared earlier. The ELI X0 can verify the LISE server certificate using the root CA certificate pre-configured as described in clause 5.2. By using attestation result the AVS provided to LISEs ARP, LISE can verify that the temporary client certificate indeed is using X0PUB. This check effectively binds the connecting instance to the attestation. Using the encoding and methods described in clause 6, the ELI makes a post request over X0 to the LISE with the RegistrationRequest message using the following parameters (step 4 in figure 5.6.2-1):

- Identifiers of the NF, the NFIID, the ELIReference, and the X0 instance identifier X0ID.
- The supported certificate enrolment protocols.

ELI uses the X0ID as a temporary ELI identifier.

By using the result AVS provided to ARP (step 5 in figure 5.4-1), LISE checks that the incoming request and the public key of the client to the X0 entry that was the result from the X0 trust bootstrap. If no matching data can be found, the LISE shall respond with a failure indication for the service attachment.

NOTE 1: While at this point LISE has authenticated the ELI via X0, it has not done so using an identity(=certificate) of the LICA.

If all checks are satisfactory, LISE proceeds, selects a suitable certificate enrolment protocol and continues with the registration. LISE now binds together the ELIReference, the NFReference and the interface identifier X0ID in the X0 context (step 6). LISE will ask the CMF to prepare a certificate to be issued for the ELI X0 interface. The CMF will then register the ELI X0 end-entity information in the LICA. The specific steps depend on the certificate enrolment protocol that is chosen. Below are the steps for the standardized protocols CMP (IETF RFC 9483 [8]).

The CMF and the LICA agree on an initial credential such as an IAK in form of a password for authentication during the certificate issuing process using CMP.

For CMP, the CMF will pass the password as IAK to the LISE as confirmation that the registration in the LICA was successful. LISE fetches all the additional parameters that are needed at ELI's X0 from the LICREPF ELI's configuration to create a proper Certificate Sign Request (CSR) message. The LISE answers ELI (step 14 in figure 5.6.2-1) with a RegistrationResponse message containing:

- The assigned ELIID, which may be different from the temporary ELIID initially sent by the ELI.
- The certificate enrolment details consisting of:
  - The parameters needed for the certificate request message.
  - The parameters for the CA server including the trusted certificates needed to interact with the LICA service.

NOTE 2: The certificate request message does not need to be a PKCS#10 formatted CSR. The actual formatting of the request is not in the scope of the present document and is defined as part of the certificate enrolment protocol.

The ELI identifier field in the RegistrationResponse message shall carry the X0ID and not the Assigned ELIID value.

5.6.2 Certificate provisioning with CMP

In case of CMP, the ELI creates a public-private key pair for X0, and uses the IAK/password and the provided CSR parameters to create a certificate request message, e.g. for use in CMP.

Then, the ELI uses the certificate management protocol to send the certificate request message to the LICA. The LICA uses the IAK/password to check if the ELI is indeed the correct claimant for the registered end-entity. If so, the LICA issues the X0 end-entity certificate and returns the appropriate certificate chain to the ELI, to be used in the mutually authenticated TLS connection. The chain contains first the ELI X0 end-entity certificate and, optionally, any intermediate subCA certificate up to, but not including the root certificate of the LICA. The chain should not contain the root certificate of the LICA. The latter to adhere to the rule in IETF RFC 5280 [15], section 6.1, that when the trust anchor is provided in the form of a self-signed certificate, this self-signed certificate is not included as part of the prospective certification path to be validated in the handshake.

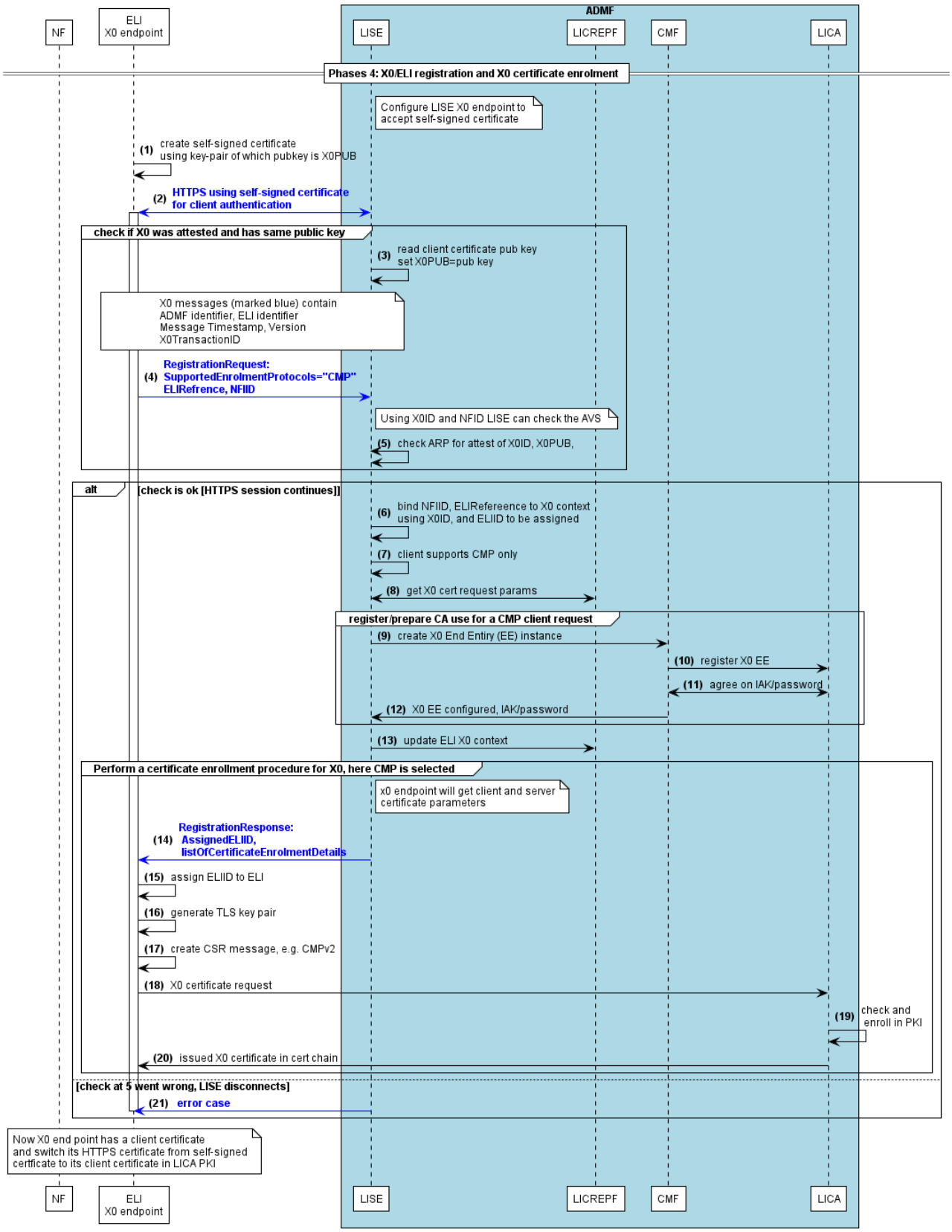

Figure 5.6.2-1: Interactions showing ELI's X0 interface instance using the X0 channel to register itself and the process for provisioning an X0 end-entity client certificate

5.7 X0 and X*n* Configuration (Phase 5)

After ELI has obtained the X0 end-entity certificate from the LICA, it shall henceforth use this certificate for its X0 HTTPS connection to LISE for further configuration of X0 and the other X interfaces.

NOTE: It is assumed that the client certificate used for the HTTPS connection is used in the LICREPF to enforce access control to the LICREPF objects that ELI instance has permissions for.

At this point, the ELI shall do the following (see figure 5.7-1 steps 1 through 4):

- Switch HTTPS client certificate to LICA X0 client certificate to connect to LISE (step 1).
- Send a ConfigurationRequest message, which implicitly requests additional configuration parameters for the X0 interface, such as which other X interfaces shall be setup, see clause 6 (step 2).
- ELI subscribes always to the ADMF to receive configuration change events in the ADMF (step 2).

The details for the X0 parameters are provided in clause 6.2.5.2.

The response will be a ConfigurationResponse message that contains the X0 configuration details as well as the configurations for the X*n* interfaces.

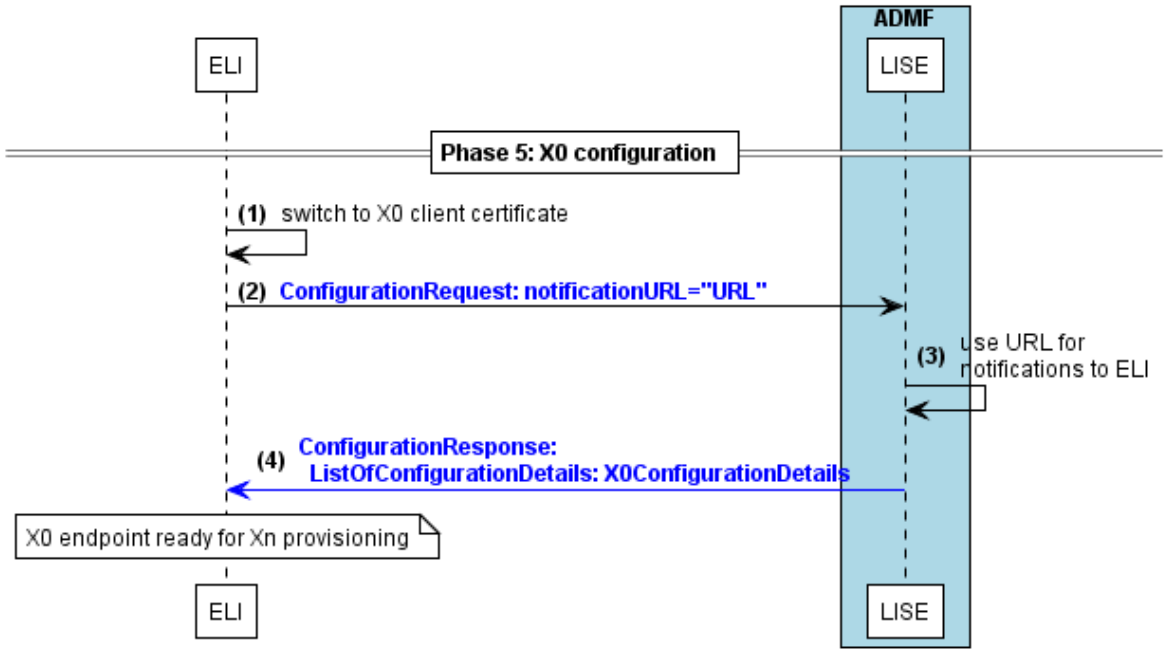

Figure 5.7-1: Interactions for the configuration of the ELI X0 parameters

After X0 configuration has been performed, the configuration of the X*n* interfaces takes place as required by the ELI type. Figure 5.7-2 illustrates the case where an X1 as well as X2 and X3 interfaces are configured. During X1 interface configuration the ELI is configured with the NEID that is later needed during the X1 certificate binding.
Figure 5.7-2, additionally, illustrates the use of the notification mechanism in steps 3 through 7 where LISE changes, for example, the X1 keepalive timer. LISE uses the URL received in step 2 of figure 5.7-1 to send notifications to the ELI. The ELI gets X1 keepalive timer from the X1ConfigurationDetails.

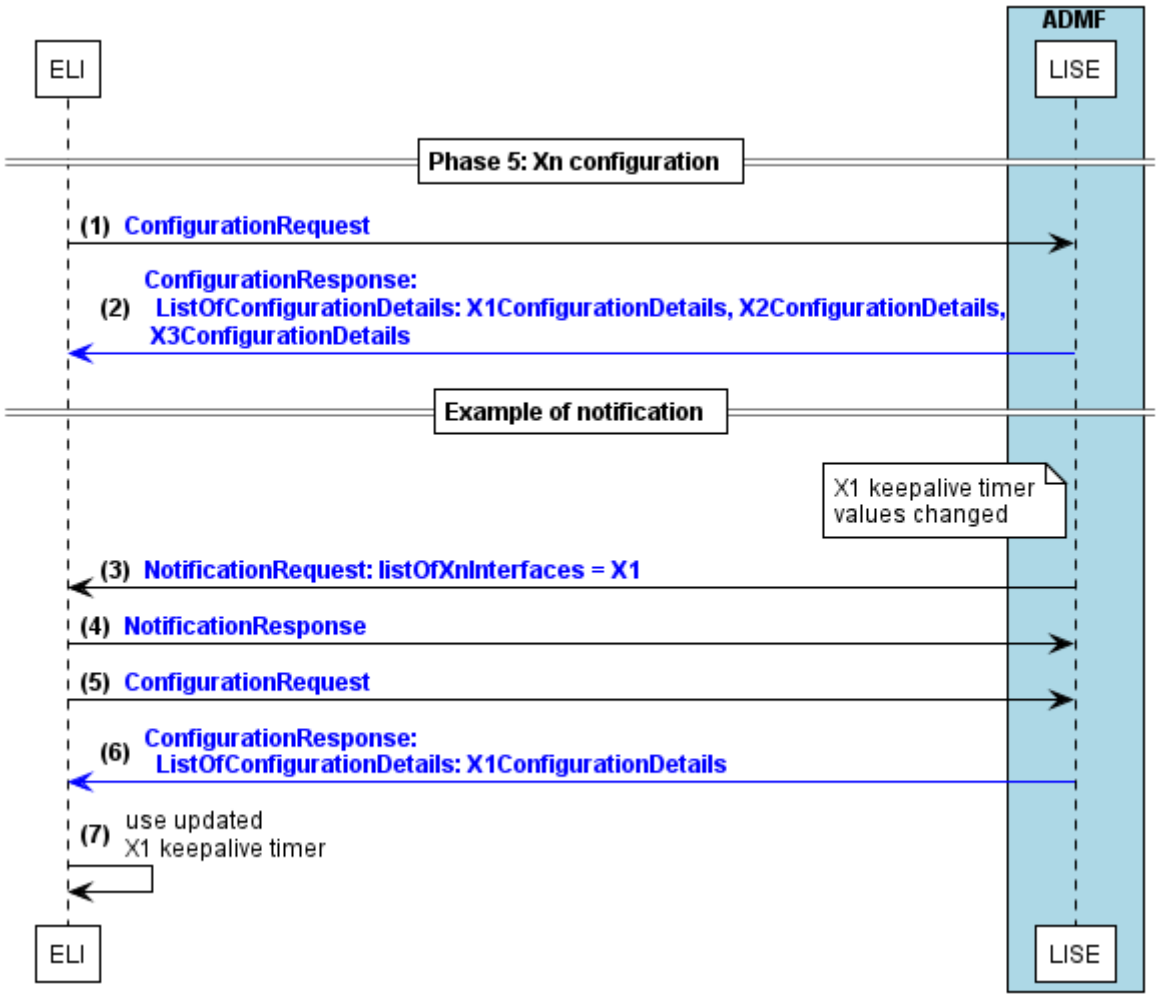

Figure 5.7-2: Example of X*n* configuration where X1 as well as X2 and X3 configuration takes place and handling of configuration update through notification

5.8 Provisioning of certificates for X1, X2 and X3 (Phase 6)

The provisioning of certificates for the X interfaces other than X0 is a prerequisite for further configuration of those X interfaces. In case certificates are shared between distinct interface instances, this implies that the associated private keys shall be shared as well. However, it is recommended not to share certificates and their associate private keys. If certificate provisioning is automated, the additional number of certificates in use should not complicate the certificate management. However, products may support key sharing.

While the certificate enrolment of the X interfaces is basically identical to the one for X0, the preparations differ (the present clause details the steps). In the present clause X*n* stands for any of the X1, X2 or X3 interfaces.

When the X0 interface is configured, through the configuration in clause 5.7 the ELI knows which X*n* interfaces need to be setup, and thus which certificates are required.

In the following text it is assumed that the X*n* certificates are provisioned one by one, the order being irrelevant. The ELI shall create the X*n* interfaces it requires and shall perform for each X*n* a certificate enrolment after it has fetched the certificate details from the LICREPF via the X0 connection. In such context, the ELI will request certificates for all its relevant X*n* interfaces. Figure 5.8-1 illustrates the ELI initiating the request for X*n* in step 1. The certificate provisioning will use the protocol that was selected for the X0 certificate provisioning in clause 5.6.

To secure that the ELI only can enrol certificates that the ADMF has planned for the ELI in the NF, for each X*n* LISE shall approve the creation of the end-entities e.g. by registering the corresponding end-entities in the LICA. Certificate enrolment protocol specific mechanisms are utilized to authenticate the certificate issuing process.

Note that at this point of the configuration process the binding of the X*n* certificates to their respective X*n* instance is implicitly realized via the authenticated and attested X0 connection.

LISE will respond to the request in step 3 with the XnCertificateEnrolmentResponse message (see clause 6.2.4) containing:

- The IAK/password that will be used to authenticate during certificate enrolment.
- The parameters in XnCertificateEnrolmentDetails needed for the certificate request message, see also annex A.

NOTE 1: Since the same LICA is used for the final certificate issuing, there is no need to provide the URI of this CA as it has already been provided by the ADMF earlier during the setup required to get the X0 certificate.

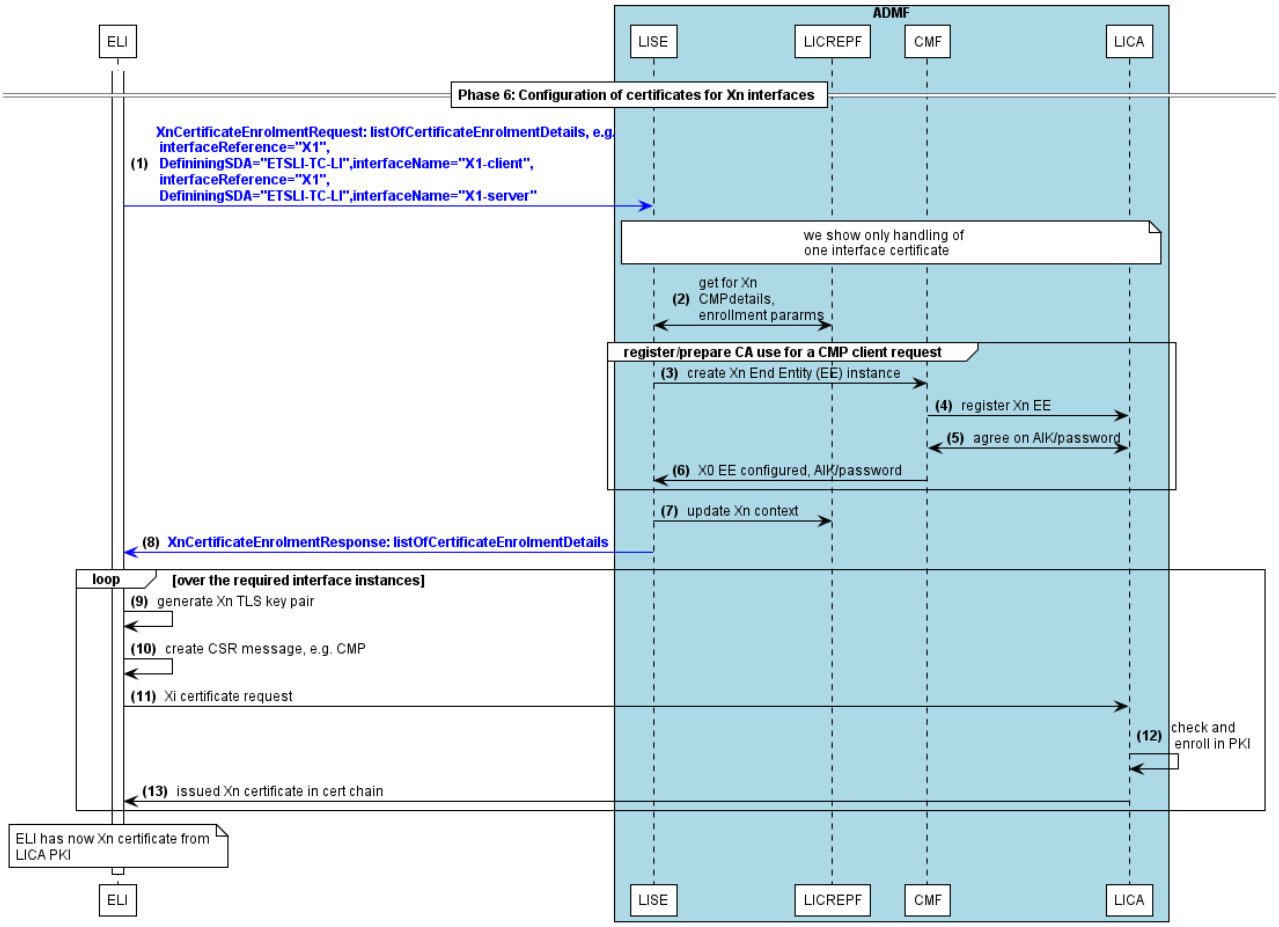

Figure 5.8-1: Interactions for provisioning of each of the X*n* end-entity certificates

NOTE 2: In the XnCertificateEnrolmentRequest message (step 1) the ELI may request the parameters for all the X*n* interfaces at once.

Figure 5.8-2 illustrates the use of the notification mechanism in steps 1 through 2 where LISE changes certificate enrolment parameters related to the X1-client and X1-server. In such context, the ELI will request certificates for the X1-client and X1-server interface type. Figure 5.8-2 illustrates the ELI initiating the request for X1-client and X1-server certificates enrolment parameters in step 3. To secure that the ELI can only enrol certificates for each updated certificate enrolment parameters set, LISE may approve the creation of the end-entities e.g. by registering the corresponding end-entities in the LICA in steps 5 through 8. If successfully registered, LISE shall deregister/revoke the end-entities replaced by the new end-entities.

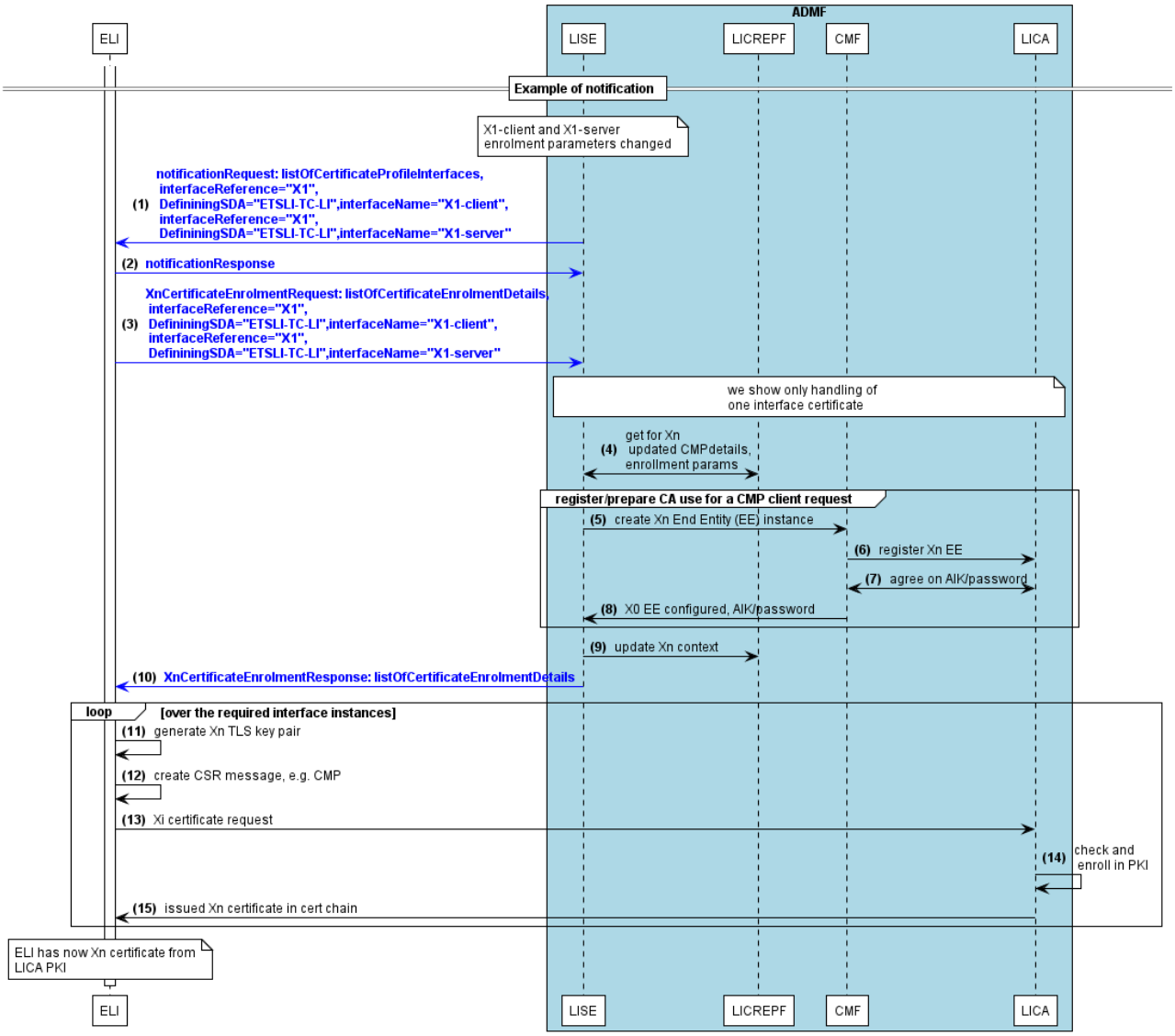

Figure 5.8-2: Handling of certificate parameters update through notification.

5.9 Image key insertion and decryption (Phase 7)

The ADMF can use the X0 interface to send to the ELI an IMK key which can be used for decryption of software images or configuration data, see clause 5.1. The IMK is sent in a key container. The ADMF can use the X0 interface to instruct the ELI about what to do with the key as part of the ImageKeyDetails, see clause 6.2.5.

The image key can be provided by a notification trigger as shown in figure 5.9-1 or via the configuration of X0 in phase 5.

NOTE: It is application-dependent how the ELI will use the provided key and what to do with objects that are protected with the image key when, e.g. an image key is deleted. Which objects are associated with key identifiers is application dependent.

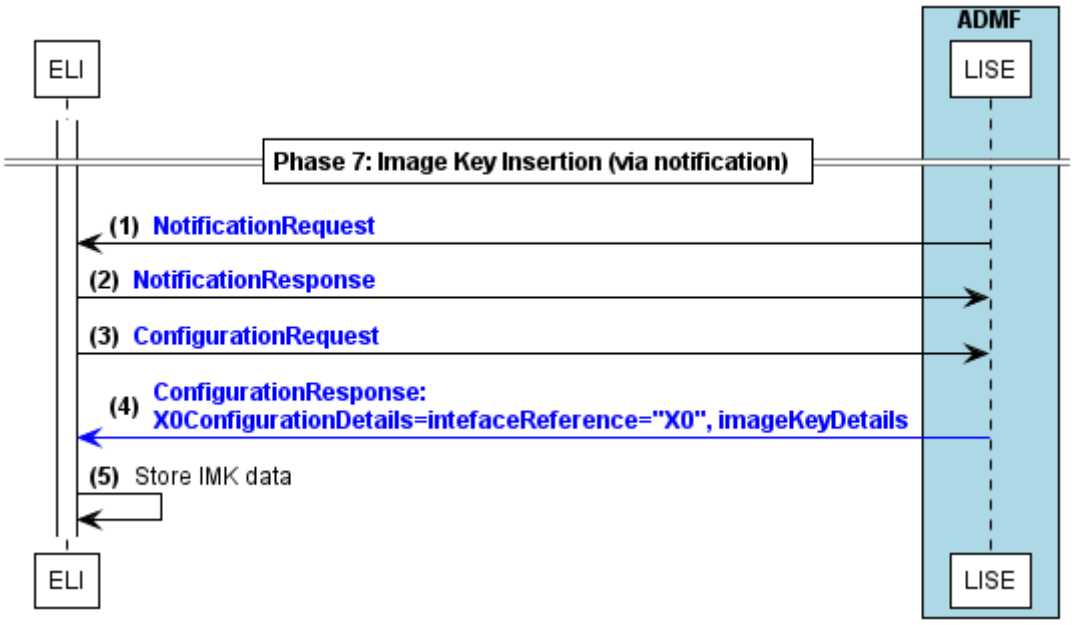

Figure 5.9-1: Interactions for Image Key insertion and decrypt message

6 X0 protocol

6.1 Basic Concepts

6.1.1 Reference model for X0: requesting and responding

X0 transactions consist of a request followed by a response.

Requests may be sent in either direction i.e. with either the ELI or the LISE initiating the request.

Figure 6.1.1-1 shows a response-request model, with the ELI initiating the request and the LISE responding with the requested data.

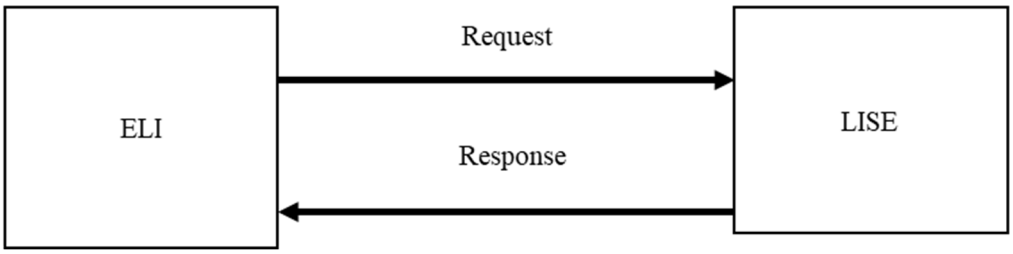

Figure 6.1.1-1: Generic request-response model: ELI as the requester

The above request-response model with ELI as the requester applies to the Read Configuration, ELI Subscription and ELI Registration procedures as specified in clause 6.2.

Figure 6.1.1-2 shows a response-request model, with the LISE sending a request (i.e. notification) and the ELI acknowledging the request.

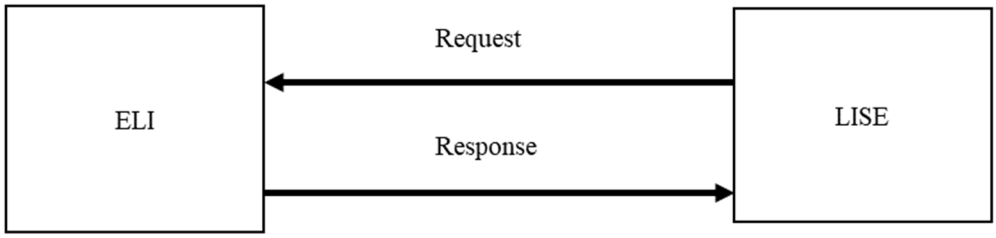

Figure 6.1.1-2: Generic request-response model: LISE as the requester

The above request-response model with LISE as the requester applies for the LISE sending a notification and the ELI acknowledging the notification as specified in clause 6.2.

6.1.2 The lifecycle of an ELI configuration

An ELI configuration is uniquely associated with the X0 interface established between the ELI and the LISE of the ADMF.

Each ELI configuration is uniquely identified by an ELI Identifier (ELIID) assigned by the LISE as part of the Registration phase (see clauses 5.6 and 6.2.3).

When the LISE detects that an ELI has been terminated, it shall remove the ELI configuration associated with that ELI.

6.1.3 The lifecycle of an X0 request/response

Each request and response shall be identified by an X0TransactionID. The requester (LISE or ELI) shall assign an X0TransactionID as a version 4 UUID as per IETF RFC 4122 [12].

The response shall be sent without delay and shall be sent within TIME1X0 of receiving the request. TIME1X0 shall be configurable and by default TIME1X0 shall be five seconds. TIME2X0, the time a requester waits for a response, shall be configurable; it shall be at least twice TIME1X0 and by default shall be fifteen seconds.

An error response (see clause 6.2.2) shall be sent if the request is not compliant syntactically (it does not match the schema) or semantically (it is not compliant or consistent with the existing state of the ELI, e.g. ELIID not existing in LISE).

If the request is compliant, an "OK" response shall be sent once the request has been successfully completed. If the request was a request for information, then all the information shall be delivered together as part of the "OK" response. The ELI and LISE shall be designed so that the information requested is in a data store which is readily available without delay and within TIME1X0.

If the requester has not received a response after TIME2X0, the requester may assume that either the request or the response failed to get through. For example, the requester may re-send the original request (as a new request, with a new X0TransactionID).

6.2 Message Definitions

6.2.1 X0 Message

X0 messages contain information as defined in table 6.2.1-1. The information is Mandatory, Optional or Conditional as shown in the last column.

Table 6.2.1-1: X0 Message

Field	Description	Format	M/C/O
admfIdentifier	Identifies the ADMF uniquely to the ELI. Required to match the details provided by the ADMF's X.509 certificate (see clause 8).	Token as per W3C Recommendation [10], section 3.3.2.	M
eliIdentifier	Uniquely identifies the ELI to the LISE for the duration of the ELI lifecycle. Shall be set to the ELI X0 instance ID (X0ID) for Registration messages (see clause 5.2), and to the Assigned ELI Identifier (ELIID) for all other messages. Required to match the details provided by the ELI's X.509 certificate (see clause 8).	Token as per W3C Recommendation [10], section 3.3.2.	M
messageTimestamp	Timestamp indicating the time the message was generated.	QualifiedMicrosecondDateTime (see ETSI TS 103 280 [13], clause 6.5).	M
version	Version of the present document used for encoding the message.	x.y.z with x,y,z integer.	M
x0TransactionID	Used to correlate Request and Response. See clause 6.1.3.	UUIDv4 as per IETF RFC 4122 [12].	M

In addition to the information in table 6.2.1-1, the X0 Request shall contain additional information specific to the type of message. The type of the message being sent will be identified in an xsi attribute in the XSD, for example a NotificationRequest message would have an xsi:type="NotificationRequest" attribute. See the following clauses within clause 6.2 for the information elements in each specific type of message.

If a new message does not carry an optional parameter for which a previous message provided a value, the previous value shall be retained.

6.2.2 Error responses

If the Responder is unable to parse an X0 Request, or cannot fulfil the X0 Request, then it shall respond with an ErrorResponse.

If the Responder is unable to determine the correct ADMF or ELIID values (e.g. because the original Request cannot be parsed), it shall use the values provided in the client certificate (see clause 8) if possible. If this is not possible, the Responder shall use the value "UNKNOWN" for the corresponding fields in the ErrorResponse message.

If the Responder is unable to determine the X0TransactionID from the original Request, it shall use a randomly generated X0TransactionID in the ErrorResponse message.

In addition to the details in clause 6.2.1, the ErrorResponse shall contain the following information.

Table 6.2.2-1: ErrorResponse

Field	Description	Format	M/C/O
errorCode	Integer code indicating the type of error (see table B.1-1).	Integer	M
errorDescription	Free text field giving further details of the error. Implementers are encouraged to avoid placing sensitive information (such as personally identifiably information or sensitive details of the network) in error messages.	UTF-8 string	M

6.2.3 Registration message definitions

6.2.3.1 RegistrationRequest

The RegistrationRequest message is sent by ELI to the LISE to perform initial registration and obtain the necessary information to perform X0 certificate enrolment (see clause 5.6). In addition to the details in clause 6.2.1, it shall contain the following information.

Table 6.2.3.1-1: RegistrationRequest

Field	Description	Format	M/C/O
supportedEnrolmentProtocols	List of enrolment protocols that the ELI supports.	List of SupportedEnrolmentProtocol values. Currently only "CMP" is supported. See IETF RFC 9483 [8] for details of the CMP protocol.	M
eLIReference	ELIReference that identifies the appropriate configuration of the ELI, see table 4.1-4. During phase 0 the ADMF is configured with the ELIs in the NF and the reference of the ELI The ELIReference value that the ELI presents should match the configured value, so that LISE can determine the ELI instance sending the request in combination with the NFIID.	UUID, (ETSI TS 103 280 [13], clause 6.27).	M
nFIID	The identifier of the network function instance that contains the ELI and data of interest to LI. See ETSI TS 104 007 [2]. The NFIID is the value assigned to the NF instance by the orchestration layer.	ShortString, (see clause 6.29 of ETSI TS 103 280 [13]).	M

6.2.3.2 RegistrationResponse

The RegistrationResponse message is sent by the LISE to the ELI as a response to a RegistrationRequest to signal that registration has been successfully completed (see clause 5.6.1) and that the ELI shall now proceed with certificate enrolment (see clauses 5.6.2 and 5.8). If the registration procedure is not successful, the LISE shall respond with an ErrorResponse message instead (see clause 6.2.2).

In addition to the details in clause 6.2.1, the RegistrationResponse shall contain the following information.

Table 6.2.3.2-1: RegistrationResponse

Field	Description	Format	M/C/O
assignedELIID	ELIID value that is assigned by the LISE to the ELI (see clause 5.4) and which identifies the ELI configuration in the LISE (see clause 6.1.2).	UUID, (ETSI TS 103 280 [13], clause 6.27).	M
listOfCertificateEnrolmentDetails	A list of certificate enrolment details with information to be used by the ELI to perform X0 client and server certificate enrolment.	Sequence with at least one CertificateEnrolmentDetails, see table 6.2.4.2-2 with CertificateProfileInterfaceType being "X0-client" or "X0-server", see table 6.2.4.1-3.	M

6.2.4 Xn certificate enrolment message definitions

6.2.4.1 XnCertificateEnrolmentRequest

The XnCertificateEnrolmentRequest message shall be sent by the ELI to the LISE after the ELI has successfully retrieved its configuration information for the first time (see figure 5.7-1 in clause 5.7). If the ELI has not yet retrieved its initial configuration for the first time, the LISE shall respond to the XnCertificateEnrolmentRequest with an Error (see clause 6.2.2).

The present document defines a set of values and their associated meanings in table 6.2.4.1-3. Other SDOs may define additional values.

A XnCertificateEnrolmentRequest may be triggered through notification of a configuration change. Implementers should be aware that changes to certificate enrolment parameters may disrupt active LI operations as this would require the ELI to enrol the new X*n* certificates.

In addition to the details in clause 6.2.1, it shall contain the following information.

Table 6.2.4.1-1: XnCertificateEnrolmentRequest

Field	Description	Format	M/C/O
listOfCertificateEnrolmentRequests	A list of certificate enrolment requests.	List of CertificateEnrolmentRequest (see table 6.2.4.1-2).	M

Table 6.2.4.1-2: CertificateEnrolmentRequest

Field	Description	Format	M/C/O
interfaceReference	Reference to interface in ELI (see table 4.1-4).	ShortString, (see ETSI TS 103 280 [13], clause 6.29).	M
certificateProfileInterfaceType	Specifies for which interface of the ELI the certificate enrolment parameters are requested.	ShortString, (see ETSI TS 103 280 [13], clause 6.29 and table 6.2.4.1-3).	M

Where the certificateProfileInterfaceType is defined by table 6.2.4.1-3.

Table 6.2.4.1-3: CertificateProfileInterfaceType

Field	Description	Format	M/C/O
definingSDO	Indicates which SDO defines the interfaceName value	ShortString, (see ETSI TS 103 280 [13], clause 6.29). The ETSI TC-LI values shall use here "ETSI-TC-LI".	M
interfaceName	Name of the interface type	ShortString, (see ETSI TS 103 280 [13], clause 6.29 and table 6.2.4.1-4).	M

Table 6.2.4.1-4 defines the interfaceName values when the definingSDO="ETSI-TC-LI". The quotes for the values in table 6.2.4.1-4 are used to indicate that the values are strings. These quotes are not to be used in the interfaceName values.

Table 6.2.4.1-4: String values of ETSI TC-LI interfaceName

interfaceName value	Description
"X0-client"	Indicates the request concerns a client certificate to be used in the ELI for an X0 interface.
"X0-server"	Indicates the request concerns a server certificate to be used in the ELI for an X0 interface.
"X1-client"	Indicates the request concerns a client certificate to be used in the ELI for an X1 interface.
"X1-server"	Indicates the request concerns a server certificate to be used in the ELI for an X1 interface.
"X2-client"	Indicates the request concerns a client certificate to be used in the ELI for an X2 interface.
"X2-server"	Indicates the request concerns a server certificate to be used in the ELI for an X2 interface.
"X3-client"	Indicates the request concerns a client certificate to be used in the ELI for an X3 interface.
"X3-server"	Indicates the request concerns a server certificate to be used in the ELI for an X3 interface.

6.2.4.2 XnCertificateEnrolmentResponse

The XnCertificateEnrolmentResponse message shall be sent by the LISE to the ELI as a response to a XnCertificateEnrolmentRequest if the LISE is able to enter the ELI into enrolment for all of the interfaces requested (see table 6.2.4.2-1). If enrolment fails for any of the requested interfaces, then the LISE shall terminate all enrolment requests for the ELI and return an error.

In addition to the details in clause 6.2.1, it shall contain the following information.

Table 6.2.4.2-1: XnCertificateEnrolmentResponse

Field	Description	Format	M/C/O
listOfCertificateEnrolmentDetails	A list of certificate enrolment details.	List of CertificateEnrolmentDetails (see table 6.2.4.2-2).	M

Table 6.2.4.2-2: CertificateEnrolmentDetails

Field	Description	Format	M/C/O
interfaceReference	Reference to interface in ELI (see table 4.1-4).	ShortString, (see ETSI TS 103 280 [13], clause 6.29).	M
certificateProfileInterfaceType	Specifies which interface of the ELI the enrolment will provide a certificate is for.	See table 6.2.4.1-3.	M
enrolmentProtocolDetails	Details necessary for the ELI to perform enrolment via the LISE's chosen enrolment protocol.	Currently only: CMPEnrolmentDetails (see table A.2-1).	M

6.2.5 Configuration message definitions

6.2.5.1 ConfigurationRequest

The ELI may send a ConfigurationRequest to the LISE at any time after X0 enrolment to request configuration information for the ELI's X*n* interfaces.

The ELI shall send a ConfigurationRequest to the LISE immediately after successful X0 certificate enrolment (see clause 5.7). This request shall provide a notification URL (see table 6.2.5.1-1). If it does not, the LISE shall respond with an Error message (see clause 6.2.2) instead of a ConfigurationResponse message.

A ConfigurationRequest may be triggered through notification of a configuration change. The ConfigurationResponse message may result in parameter changes. Implementers should be aware that changes to configuration may disrupt active LI operations.

In addition to the details in clause 6.2.1, the ConfigurationRequest shall contain the following information.

Table 6.2.5.1-1: ConfigurationRequest

Field	Description	Format	M/C/O
notificationURL	URL to which the LISE should send any Notification messages (see clause 6.2.6). Shall be provided in the first ConfigurationRequest sent by the ELI to the LISE. May be sent in any subsequent requests.	any URI (see W3C Recommendation [10], clause 3.2.17) containing a valid URL.	C

6.2.5.2 ConfigurationResponse

The ConfigurationResponse message is sent by the LISE to the ELI as a response to a successful ConfigurationRequest message. In addition to the details in clause 6.2.1, it shall contain the following information.

Table 6.2.5.2-1: ConfigurationResponse

Field	Description	Format	M/C/O
listOfConfigurationDetails	List of configuration details associated with a given interface.	List of ConfigurationDetails (see table 6.2.5.2-2).	C

The present document provides an abstract ConfigurationDetails type (see table 6.2.5.2-2) from which concrete configuration detail structures may be derived. The present document defines one concrete ConfigurationDetails type (X0ConfigurationDetails, see table 6.2.5.2-3). X1 configuration details are defined by ETSI TS 103 221-1 [3]. X2 and X3 configuration details are defined by ETSI TS 103 221-2 [16]. Other specifications may derive other types of configuration details from the ConfigurationDetails definition.

The LISE shall provide all the configuration details it has associated with the ELI configuration.

In addition to the details in clause 6.2.1, it shall contain the following information:

Table 6.2.5.2-2: ConfigurationDetails

Field	Description	Format	M/C/O
interfaceReference	See table 4.1-5.	ShortString (see ETSI TS 103 280 [13], clause 6.29).	M
Other parameters	One or more additional parameters may be included and whose details are to be specified by owner indicated by the InterfaceReference value.	To be specified by owner indicated by the interfaceReference value.	C

Table 6.2.5.2-3: X0ConfigurationDetails

Field	Description	Format	M/C/O
interfaceReference	See table 4.1-5.	Shall be given as the value "X0".	M
imageKeyDetails	Details for the image key that is provided in the response.	See table 6.2.5.2-4.	O

Table 6.2.5.2-4: ImageKeyDetails

Field	Description	Format	M/C/O
iMKidentifier	Reference value of the image key used by LISE and which ELI shall use.	UUID (ETSI TS 103 280 [13], clause 6.27).	M
iMKformat	Format of the key. Base64 formatted PKCS12 container or as base64 encoding of a raw binary byte array.	Enumerated value, one of: • "PKCS12BASE64" • "RAWBASE64"	M
iMKvalue	The key value, base64 encoded.	String	M
instruction	Optional parameter indication of what the ELI should do with the returned image key. The default is that the ELI should store the key, "roll-over" means that an existing key shall be replaced and existing material shall be re-protected using that new key. "Delete" means that the referred key shall be deleted. Absence of this parameter shall be interpreted that the ELI shall store the received key.	Enumerated value, one of: • "store" • "delete" • "roll-over"	O

6.2.6 Notification message definitions

6.2.6.1 NotificationRequest

Whenever the configuration of the ELI is required to change because the ADMFs has changed the ELI configuration in the repository the LISE shall send a NotificationRequest message to the ELI The ELI shall respond with a NotificationResponse message (see clause 6.2.6.2) and then issue ConfigurationRequest message (see clause 6.2.5.1) and/or XnCertificateEnrolmentRequest (see clause 6.2.4.1) to the LISE without delay.

NOTE: A notification request may result in changes due to parameter changes of even changes in certificates. Implementers should be aware that changes to configuration or certificates may disrupt active LI operations.

In addition to the details in clause 6.2.1, the NotificationRequest shall contain the information as described in table 6.2.6.1-1.

Table 6.2.6.1-1: ParametersUpdateIndications

Field	Description	Format	M/C/O
listOfCertificateProfileInterfaces	It shall include a list of the certificate profile type for which the certificate enrolment parameters have been updated If there are no updates to the certificate enrolment parameters, an empty list is returned - this is not an error.	List of CertificateEnrolmentRequest structures (see table 6.2.4.1-2) that indicate the relevant interfaces which require re-enrolment.	C
listOfXnInterfaces	It shall include a list of the updated X*n* configuration interfaces. If there are no updates to the X*n* configuration interface, an empty list is returned - this is not an error.	List of interfaceReferences (see table 4.1-5).	C

6.2.6.2 NotificationResponse

The ELI shall respond to a NotificationRequest message from the LISE with a NotificationResponse message.

The NotificationResponse has no additional parameters beyond those given in clause 6.2.1.

7 Transport and encoding

7.1 Overview

The present document defines a single profile for transport and encoding of X0 messages ("profile A").

7.2 Profile A

7.2.1 Encoding

Samples, which provide an informative example for implementations of the present document, are available together with the normative XSD at https://forge.etsi.org/rep/li/schemas-definitions/-/tree/spec/104000/1.2.1/104000?ref_type=tags which accompanies the present document. In the event of a discrepancy between the XSD and encoding requirements that are stated in the present document, the XSD shall be considered authoritative. The samples do not form part of the normative specification.

Implementers on both the sending and receiving end shall validate the XML they generate against the XSD. Both ELI and LISE shall only send messages which conform to the XSD.

7.2.2 Transport

HTTPS shall be used as per IETF RFC 9110 [5]. The details relating to HTTP are given in this clause and the details relating to TLS are specified in clause 8.2.

In this clause, the term HTTP is used (it is implicit that it is in fact HTTPS, i.e. that the HTTP is used over TLS).

The LISE and ELI shall run HTTP clients and servers for communication over X0:

- For messages where the LISE is the requester, the LISE shall use its HTTP client, and the ELI shall use the X0 interface as their HTTP servers.
- For messages where the ELI is the requester, then ELI shall use its HTTP client in the X0 interface and the LISE shall use its HTTP server.

Details in the request:

- Each X0 request message shall be sent as a HTTP request. It shall be a "POST" message (regardless of which type of X0 request it is).

Details in the response:

- Each X0 response message shall be sent as a HTTP response.
- The response shall indicate HTTP level errors within the range of HTTP error codes. If the HTTP level transaction is successful, then the response shall be a 200 OK message, with the X0 message contained within the message body.

HTTP error codes shall only be used to indicate HTTP-level errors and shall not be used to indicate errors with the X0 responses themselves. X0-level errors shall be indicated by correct use of the appropriate X0 ErrorResponse, encoded and returned within a HTTP 200 OK response.

7.2.3 HTTP configuration

HTTP version 1.1 or HTTP/2 shall be used. LISE and ELI implementations shall support both.

Where used, HTTP version 1.1 shall be used as per IETF RFC 9110 [5], IETF RFC 9112 [6] and related specifications.

NOTE: HTTP/1.1 defaults to the use of "persistent connections" (see IETF RFC 9112 [6], section 9.3). Implementers are encouraged to support the use of persistent connections.

Where used, HTTP/2 shall be used as per IETF RFC 9113 [7] and related specifications.

HTTP/1.1 Pipelining shall not be used.

A Requester may issue multiple HTTP requests in parallel over multiple HTTP connections or multiplexed HTTP/2 requests. However, such implementations should be aware that there is no guarantee of the order in which these requests are processed by the Responder. If such ordering is important to the Requester, the Requester is responsible for ensuring the requests are sent out in the correct order and is responsible for waiting for the response to each request before issuing the next one. Transfer Coding shall not be applied to the HTTP Request or Response (see IETF RFC 9112 [6], section 7).

By default, port 443 shall be used. If this is already in use, then the X0 interface instance in ELI and LISE shall be able to be configured with a port number, which shall be agreed prior to use of the standard.

By default, the LISE shall send the HTTP requests with the path set to "/X0" and the ELI shall send the HTTP requests with the path set to "/X0/ADMF/LISE".

8 Certificate profiles for X0

8.1 Overview

The X0 interface uses certificates from the LICA for the X0 channel that is utilized for the configuration of X1, X2 and X3. In addition, the X0 interface uses a self-signed client certificate during the ELI registration (see clause 5.6). The public key of this certificate is the same as the X0PUB key that the attested procedure left into the AVS. Clause 8 of the present document specifies the certificate profiles for these two types of certificates and the certificate binding for X0.

The certificate binding can be realized through the mandatory presence of a URN in the certificate's subjectAltName. The URN provides a value used to bind a client or server certificate to a specific identifier and role (ELI or ADMF), and to ensure that a certificate is intended to be used for X0.

For the X0 certificates the binding value is always the URN value. New implementation shall use the URN in the subjectAltName. Older implementations may use the URN as the UID value.

The certificate binding URN is a URN value under the ETSI TC LI namespace root `urn:etsi:li`.

X0 Certificates shall conform to IETF RFC 6125 [11] and be profiled using the TLS certificate profile in 3GPP TS 33.210 [9] with the additions stipulated in the following clauses within clause 8.

8.2 URN format

A certificate binding URN has the following format, with the placeholders `{role}` and `{identifier}` given as per table 8.2-1.

```
Urn:etsi:li:x0-binding:{role}:{identifier}
```

Table 8.2-1: Certificate binding URN format

Field	Description	Format
Role	String indicating the role of the party presenting the certificate.	One of "ADMF", "X0ID", "ELIID".
Identifier	String giving the relevant identifier of the party presenting the certificate (ADMF Identifier if the role is ADMF, otherwise the NE side ELI identifier.	For ADMF String containing a value as per table 1 in ETSI TS 103 221-1 [3]. For ELI identifier the identifier string containing a value as per table 6.2.1-1 of the present document.

8.3 Certificate Binding Validity

A certificate binding URN presented in a client or server certificate as part of the transmission of an X0 message shall be considered valid if and only if all the following conditions are met:

- It follows the format given in table 8.2-1.
- The Role value correctly matches the expected role of the presenting party (i.e. ADMF, X0ID, ELIID or ELI-REG).
- The Identifier value correctly matches the relevant identifier in the X0 message (i.e. the ADMF identifier if the Role is given as "ADMF", or ELI identifiers (see table 6.2.1-1).

8.4 ELI client certificate for registration

The procedure in clause 5.6 where the ELI registers at LISE in ADMF shall use a self-signed certificate with a profile complying to the requirements in clause 8.1 and details of table 8.4-1.

Table 8.4-1: Client certificate profile for ELI registration

Field	Description	Value
Basic Constraints	Certificate shall function also as trust anchor.	CA:true.
URN in subjectAltName	String indicating the role and identifier for X0 interface in ELI during registration, see clause 5.6.	Role="X0ID", Identifier=X0ID.
extendedKeyUsage	Limit certificate for client authentication only.	id-kp-clientAuth TLS clients.

8.5 X0 client and server certificates

Certificates issued by the LICA and used on the X0 channel shall, in addition to profile requirement in clause 8.1, be profiled as indicated in table 8.5-1.

Table 8.5-1: Client and Server end-entity certificate profile for X0 channel

Field (attribute)	Description	Value
Subject commonName	Use is not recommended.	If present, it shall contain a value present as dnsName in the subjectAltName extension.
Basic Constraints	Certificate is an end-entity certificate.	CA:false.
URN in subjectAltName	String indicating the role and identifier for X0 interface in ELI configuration via X0, see clauses 5.6 and 5.7.	For ELI side of X0 channel Role="ELI" Identifier=ELIID. For ADMF/LISE side of X0 channel Role="ADMF" Identifier=ADMF identifier.
extendedKeyUsage	Limit certificate for client authentication or server authentication only.	id-kp-clientAuth TLS clients. id-kp-serverAuth TLS server.

8.6 Authentication and binding verification

Implementations shall perform mutual authentication using X.509 certificates following IETF RFC 6125 [11] with the additional provisions for X0 as detailed in clauses 8.1 through 8.4. Implementations shall ensure that it is possible to configure which certificates are used. Implementations shall also perform a verification of the validity of the binding as described in clause 8.3.

Annex A (normative): Certificate Enrolment Details

A.1 Introduction

Annex A provides definitions for certificate enrolment messages content (see clause 6.2.4) and consists of two main structures: CMPServerDetails and CMPCertificateOnlineEnrolment.

A.2 CMP details

Table A.2-1: CMPEnrolmentDetails

Field	Description	Format	M/C/O
listOfCMPServerDetails	List of CMP servers. It is possible that several CMP servers are configured. At least one CMP server shall be configured. If a list is configured, they are configured in order of priority.	ListOfCMPServerDetails, sequence of,CMPServer, see table A.2-2.	M
cMPCertificateOnlineEnrolment	Defines the parameters to start the CMP-based online enrolment.	CMPCertificateOnlineEnrolment, see table A.2-3.	M

Table A.2-2: CMPServer

Field	Description	Format	M/C/O
name	A human friendly name of the CMP enrolment server.	ShortString, (see ETSI TS 103 280 [13], clause 6.29).	M
certificateAuthority	Indicates the Certificate Authority CN in the certificate used to authenticate a CMP server.	String. FQDN denoting the common name (host domain name) of the CMP server.	M
uRL	Provides the full URL to the CMP-based online enrolment endpoint of the CMP server.	anyURI (see W3C Recommendation [10], clause 3.2.17) containing a valid URL.	M

Table A.2-3: CMPCertificateOnlineEnrolment

Field	Description	Format	M/C/O
algorithm	The algorithm to be used when generating the asymmetric key.	Algorithm, see table A.2-4.	M
keyIdentifier	A reference value to use as fallback sender KID. This is used to inform the CMP server which shared secret to use for verification if sender name cannot be determined from subject. To be provided if mandatory for the CMP LICA.	String with KeyIdentifier, see CMP IETF RFC 9483 [8].	C
password	The CMP challenge password configured in the CMP server.	String.	M
subject	The X.501 DN to be used in the subject field of the requested certificate, for instance: "O=Company,C=US,L=Boston, UID= epg357-1-pgw". NOTE: In case UID is used for X1 binding, The UID for the X1 interface shall be present in the subject.	String with X.501 DN.	M
subjectAlternativeName	The subjectAltName containing IP addresses, FQDNs or URIs. For X0 certificates, see clause 8.	String. The string content has to comply to the format for the subjectAltName as stipulated in IETF RFC 5280 [15].	O
renewalThreshold	The threshold specifies the number of days prior to certificate expiry that the ELI should commence certificate renewal procedures. When the validity period of the certificate falls below the expiration threshold, the ELI shall raise an alarm and shall start the CMP renewal of the asymmetric key and certificate. The alarm is terminated when the certificate renewal has been successfully executed and the new validity period is equal or larger than the threshold.	Integer.	M

Table A.2-4: Algorithm

Field	Description	Format	M/C/O
algorithmOID	Contains a string encoding of the OID identifying the algorithm, e.g. 1.2.840.113549.1.1.1 for RSA keys, see IETF RFC 3279 [17] and 1.2.840.10045.2.1 for ECC keys, see IETF RFC 5480 [18].	OIDValue	M
curveOID	Contains a string encoding of the relevant ECC curve. Supplied if needed by the identified algorithmOID (i.e. ECC), see section 2.1.1.1 of IETF RFC 5480 [18].	OIDValue	O
algorithmBitSize	Specifies the bit length of the algorithm. Supplied if needed when neither the algorithmOID nor curveOID is specifying the bit size (i.e. when using RSA keys).	Integer	O

Annex B (normative): Error codes

B.1 Error codes

Table B.1-1 below gives the set of error codes to be used in the ErrorInformation structure (see clause 6.2.2).

Table B.1-1: Error codes

Error Code	Error Description	Suggested information element
General message error		
1000	Generic error.	Details of the error.
1010	Syntax/schema error.	Details of the schema or syntax error.
1020	Unsupported version.	Version supported by the issuing system.
1030	Certificate binding URN in ADMF certificate not valid or missing.	None.
1040	Unexpected ADMF Identifier.	None.
1050	Certificate binding URN in ELI certificate not valid or missing.	None.
1060	Unexpected ELI identifier.	None.
Identifier errors		
2000	ELIID unknown to ADMF.	ELIID in question.
2010	ELIReference unknown.	ELIReference in question.
2020	NFReference unknown to ADMF.	NFReference in question.
2030	NFIID unknown to ADMF.	NFIID in question during registration.
2040	ADMF identifier unknown.	None.
Configuration request failures		
3000	Generic Configuration Request failure.	Details the configuration request failure.
Registration request failures		
4000	Generic registration request failure.	Details of why the registration request failure.
4010	Attestation check failure.	None.
XnCertificateEnrolment request failures		
5000	Generic XnCertificateEnrolment request failure.	Details of the XnCertificateEnrolment request failure.
5010	ConfigurationRequest with notificationURL not sent.	None.
Notification request errors		
6000	Generic Notification request failure.	Details of why the notification request failure.

Annex C (informative): Rationale and background

C.1 Background

As described in the LI Architecture, ETSI TS 104 007 [2], the AVS will check the attest report of the ELI/X0 instance and ELI(s) in the network function when these services are instantiated. After their instantiation, these services cannot go into LI service operation since they lack the identities (in the form of valid certificates), hence such services need to interact with the LI systems in the ADMF. The purpose of the verification is to assess if the ELI and its X0 instance can be trusted to be given the certificate (identity) that will make it possible to use the ADMF configuration services for the X interfaces. The verification proofs to the AVS that the ELI can hold the key associated with the certificate in a secure manner, and that the ELI is of the correct type and uses the approved software. In such context, the AVS is configured by trusted operators with the so-called ground truth being effectively allowed-listed data and policies used during the verification. If an attest fails, further setup of the ELI X0 instance and the X0 interface will not happen, and the failure is logged. In case of successful attestation, the AVS has a record of the attestation result together with an identifier associated with the attested instance, and a public key value that, through the successful attestation, is known to be the public key of a private key that is securely kept in the ELI. For more details see ETSI TS 104 007 [2] and ETSI GR NFV-SEC 011 [i.1], clause 8.1.3 "LI Instantiation".

The LICA operates and keeps the PKI (e.g. as a database) holding certificates for the X interfaces including the X0 interface. However, since CA systems usually have proprietary APIs for registration and management, it is proposed to use a Certificate Management Function (CMF) in combination with the LICA in the same way as in ETSI GS NFV-IFA 026 [4]. The CMF instructs the LICA to perform its certificate management operations (e.g. enrolment, renewal, and revocation).

The attest operations and certificate management functions do not involve the use of the X0 interface between the ELI X0 and LISE. The attestation and certificate management use existing standardized or industry practices procedures, and the relevant interfaces(s) are not in scope of the present document. However, attestation needs to support the information elements required by the present document and the present document supports the use of CMP enrolment protocol.

C.2 X0 reference model rationale

ELI interacts via its X0 with the LICREPF to get configuration data. This is done via pulling information from the repository. It is a preferred pattern in virtual/cloud native systems to have the functions to configure themselves by pulling the configuration and state from a central repository. This makes scaling a much simpler task than developing ways to distribute and synchronize configuration and state to replicas. Consequently, only the bare minimum data is configured into the ELI at deployment (e.g. using day-0 procedures on NFV configuration as in ETSI GR NFV-EVE 022 [i.2]) such as the URL and credentials of the ADMF and repository to use.

As the ELI X0 instance cannot authenticate itself directly towards the repository, it is necessary to take into account that additional care is needed in the context of the X0 interface initialization. This is an additional reason why the X0 specified in the present document also considers the initial trust establishment process that is referred to as the trust bootstrap.

Having the initial trust establishment handled via out-of-band methods, *albeit* being possible, implies the following:

- It will cause vendor interoperability problems when trying to automate this step, even more so considering that automation is highly desired in container-based system implementations.
- It is highly desirable to be able to abstract different (hardware) based technologies that support trust establishment via attestation, so that the controlling function can use a technology neutral API.
- Part of the trust bootstrap is to bring verification after LI instance (ELI/X0 instance in the controlled function), i.e. the certificates need to be in place for the X interfaces which require interactions with a certificate management function and a CA for LI.

For the reasons above, the X0 support system is part of the present document.

Annex D (informative): Phase 0 and identities

D.1 Background

The configuration in phase 0 related to X0 is out-of-scope of the present document. However, it is useful to understand the background of what information is configured and how the flow of configuration is supposed to take place. In reality, the process of configuration may be realized in different ways, hence annex D is for information and to help to better understand the role of the identifiers used in the present document.

An important consideration or assumption is that when a CSP network is planned, this process involves the detailing of which NFs are to be deployed in the network, the planning of their network names, FQDNs, the configuration of support systems for operational management, monitoring and logging and, where applicable, the configuration and use of ELIs in certain NFs. As part of this process the responsible actor/operator for LI will configure the ADMF so the ADMF is aware of the topology of NFs (with its ELIs) in the network.

In the present document it is assumed that OSS/BSS, while operationally responsible for the NF, learns little if anything about the ELI functions in the NFs it manages. In addition to this separation, the mechanisms to establish an X0 connection in an NF does not depend on specific technologies, hence does not depend on how NFs are implemented. This implies that, for example, MANO/CISM specific identifiers used for NFs are abstracted away at the ADMF control level. Finally, the X0 interface should also be able to support NFs that are not 5G, thus 3GPP 5G specific identifiers such as nfInstanceID cannot be reused to generically identify NFs from the ADMF point of view.

Another important assumption in the above-described approach is that vertical scaling, i.e. adding more, new, instances of an NF with ELIs into a telco network, happens as a managed change in the deployment. Thus, the ADMF can be configured in such manner to stay aware of any new NFs added to the network. This type of scaling by adding new independent NFs is the current practice for NF management in an OSS/BSS system and will be supported by the X0 design of the present document but will rely on the implementation of LISE being able to handle ELIs with same ELIReference.

D.2 ADMF awareness and NFReference

When the ADMF is configured with information about the NF that will be in the network, this configuration may happen well before the actual NF is deployed. To make it possible for the ADMF to become aware/discover the planned NF, the ADMF uses the NFReference and ELIReference as tools to link a starting NF with its ELI configurations in the ADMF. In such context, the OSS/BSS system needs to be told which NFReference to attach to an NF that is to be deployed. Note that the OSS/BSS system does not need to know more information, e.g. the ELIIDs or ELI types in the NF. That knowledge can stay private for the NF and ADMF. In the present document the OSS/BSS is not being told about the ELIs and ELI identifiers even if the OSS/BSS may know which types of ELIs there will be in an NF by awareness of the 3GPP and ETSI specifications.

From the architectural point of view, the NFReference is controlled by the responsible actor for LI. The present document does not exclude the use of, for example MANO/CISM VNFid if that is possible for a network setup. The choice of the specific NFReference values is at discretion of the responsible actor for LI.

Annex E (informative): Change history

Status of Technical Specification ETSI TS 104 000 Lawful Interception Architecture		
TC LI approval date	**Version**	**Remarks**
October 2024	1.1.1	First publication of the TS after approval at ETSI TC LI#67 (22-24 October 2024, Vancouver)
February 2025	1.2.1	Included Change Request: CR001 (Cat C), LI(25)P68011r2 Modification of NotificationRequest This CR was approved by TC LI#68 in Dublin (25-27 February 2025)

History

Document history		
V1.1.1	November 2024	Publication
V1.2.1	May 2025	Publication