

LuxTrust Qualified SelfSigned CAs Certificate Profiles

Version number: 2.3

Publication Date: 15.05.2026

Effective Date: 01.06.2026



Copyright © 2026 – All rights reserved

Document title:	LuxTrust Qualified SelfSigned CAs Certificate Profile
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Specification
Document Distribution List	Any
Document Classification	Public
Document Owner	CSP Board

Version	Who	Date	Reason of modification
1.0	YNU	27/11/2023	Initial Version
2.0	YNU	21/10/2024 28/02/2025	Add LTGQCA4 Certificates Profiles and policy Update colour for critical extension Align short description EC/RSA EE
2.1	YNU/VMI	23/05/2025	Updated version with typo corrections
2.2	CSP Board	10/03/2026	Added ECDSA_P256 - 1.2.840.10045.3.1.7
2.3	CSP Board	30/03/2026	<ul style="list-style-type: none"> • Retire 1.3.171.1.1.1.13.5 / 1.3.171.1.1.1.14.5 • 1.3.171.1.1.1.13.6 / 1.3.171.1.1.1.14.6 – Validity Changes

Table of Contents

Introduction.....	5
1. The LuxTrust project.....	5
2. Goal of the LuxTrust PKI	5
3. LuxTrust PKI Hierarchy	5
4. Certificate Policy	6
LuxTrust Certification Authorities	7
1. CA hierarchy	7
1.1 LuxTrust Qualified TimeStamping CAs	7
1.2 LuxTrust Global Qualified Self Signed CAs	8
CERTIFICATE AND CRL PROFILES	10
1. Certificate types	10
1.1 Certificate extensions	13
1.2 Algorithm object identifiers	13
1.3 Name forms.....	13
1.4 Name constraints.....	13
1.5 Certificate policy object identifier	13
1.6 Usage of Policy Constraints extension.....	13
1.7 Policy qualifiers syntax and semantics.....	13
2. Certification Authorities – Certificates profiles	14
2.1 LuxTrust Qualified TimeStamping CA-RSA.....	14
2.2 LuxTrust Qualified TimeStamping CA-EC	15
2.3 LuxTrust Global Qualified CA-EC.....	16
2.4 LuxTrust Global Qualified CA-RSA.....	17
3. End Entity – Certificates profiles	18
3.1 Certificate profiles	18
3.2 Version number(s).....	18
3.3 Certificate Policy for LT Qualified Timestamping	18

3.3.1	NCP+ Certificate Policy for LT Qualified Timestamping	19
3.4	Certificate Policy for LT Global Qualified CA	21
3.4.1	Smartcard eSeal QCP-I-qscd	21
3.4.2	Smartcard eSeal NCP+	22
3.4.3	Smartcard QCP-n-qscd	24
3.4.4	Smartcard NCP+.....	26
3.4.5	Smartcard eID NCP+	27
3.4.6	Signing Server QCP-n-qscd	29
3.4.7	Signing Server QCP-I-qscd	30
3.4.8	eSeal QCP-I	32
3.4.9	Signing Server eID BE Delegated Sign QCP-n-qscd	34
3.4.10	Signing Server LuxTrust PRI/PRO Delegated Sign QCP-n-qscd	35
3.4.11	Signing Server eID LU Delegated Sign QCP-n-qscd	37
3.4.12	Smartcard QCP – Integration.....	39
3.4.13	Smartcard NCP+ - Integration	40
3.4.14	Signing Server Itsme Delegated Sign QCP-n-qscd	42
3.4.15	Smartcard Integration Delegated Sign QCP	44
4.	LuxTrust CRL / OCSP – Certificates profiles	47
4.1	CRL profile	47
4.2	OCSP profile	49

Introduction

1. The LuxTrust project

The LuxTrust project was created in the form of a Trusted Third Party (hereafter also “TTP”), with an international reach, aiming to establish a national expertise center for Luxembourg. LuxTrust as TTP especially focuses on providing support for any existing business needs in terms of security and promotes new “e-business” and “e-government” opportunities, making the best possible use of existing legal and commercial assets that are unique to Luxembourg.

Established in November 2005 through a partnership between the Luxembourg government and the major private financial actors in Luxembourg, LuxTrust S.A. was created to become a Trust Service Provider (“TSP”) as defined in the Luxembourg Law of 14/08/2000 on electronic commerce as amended itself derived from the European Regulation N° 910/2014 as amended. Before mentioned law and regulation set out the legal framework for electronic signatures in the Grand Duchy of Luxembourg as well as for LuxTrust activities as TSP.

LuxTrust S.A. acts as Financial Sector Professional (“PFS”) providing Public Key Infrastructure (PKI) services for the whole economic marketplace in Luxembourg, for both private and public organisations.

LuxTrust services are in line with the regulation 910/2014 EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS) as amended.

2. Goal of the LuxTrust PKI

The Goal of LuxTrust PKI is to provide to each end-user, in Luxembourg but also outside its national borders, one single shared platform to secure both Government and Private e-applications. Security services supported and provided by the LuxTrust PKI will primarily cover the following services for all applications:

- Strong Authentication;
- Electronic Signatures & seals;
- Encryption facilities;
- Trusted Time Stamping;

LuxTrust will also promote these services towards application service providers in order to facilitate the emergence of e-applications.

3. LuxTrust PKI Hierarchy

LuxTrust S.A., acting as “TSP” as described in the Luxembourg Law of 14/08/2000 on electronic commerce as amended, is using several Certification Authorities (CAs).

In all (CA-) certificates issued to these CAs, LuxTrust S.A. is referred to as the legal entity being the certificate issuing authority, assuming final responsibility and liability for all LuxTrust CAs and services used by LuxTrust S.A. for provision of LuxTrust certifications services through any one of its CAs.

This responsibility and liability is still valid when LuxTrust S.A. acting as TSP through any of its CAs is sub-contracting services or part of services process to third parties. Sub-contracting agreements shall include back-to-back provisions to ensure that sub-contractors shall support the liability and responsibility for the sub-contracted provisioned services.

4. Certificate Policy

This document constitutes the certificate policy, taking into account the LuxTrust Qualified TS (TimeStamping) CA CPS and LuxTrust Global Qualified Self Signed CA CPS documents.

LuxTrust Certification Authorities

As described in section 1.3, LuxTrust S.A. acting as TSP is using several Certification Authorities (CAs) to issue LuxTrust Certificates.

These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2018/8/001 by the national registry of Accredited Certification Service Providers.

1. CA hierarchy

The legal person (organisation) responsible for these CAs is LuxTrust S.A. acting as TSP.

The Qualified LuxTrust PKI consists in a one-level CA hierarchy which is described in this document

1.1 LuxTrust Qualified TimeStamping CAs

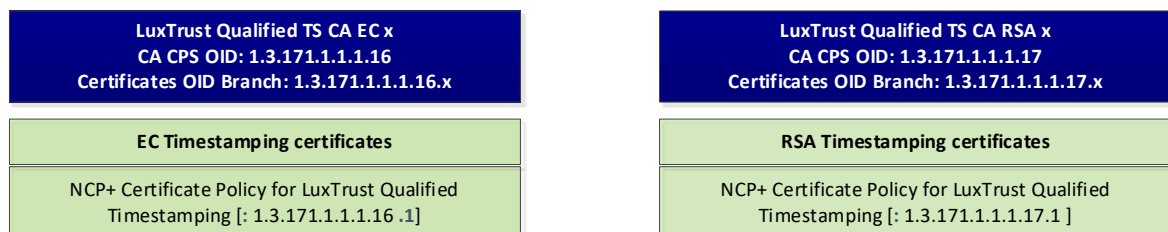


Figure 1 - LuxTrust Qualified TS CA SelfSigned Hierarchy

1.2 LuxTrust Global Qualified Self Signed CAs

LuxTrust Global Qualified CA EC x CA CPS OID: 1.3.171.1.1.1.13 Certificates OID Branch: 1.3.171.1.1.1.13.x	
Smartcard eSeal QCP-I-qscd EC	1.3.171.1.1.1.13.1
Smartcard eSeal NCP+ EC	1.3.171.1.1.1.13.2
Smartcard QCP-n-qscd EC	1.3.171.1.1.1.13.3
Smartcard NCP+ EC	1.3.171.1.1.1.13.4
Smartcard eID QCP-n-qscd EC	1.3.171.1.1.1.13.5
Smartcard eID NCP+ EC	1.3.171.1.1.1.13.6
Signing Server QCP-n-qscd EC	1.3.171.1.1.1.13.7
Signing Server QCP-I-qscd EC	1.3.171.1.1.1.13.8
eSeal QCP-I EC	1.3.171.1.1.1.13.9
Signing Server eID BE DelegatedSign QCP-n-qscd EC	1.3.171.1.1.1.13.10
Signing Server LuxTrust PRI/PRO DelegatedSign QCP-n-qscd EC	1.3.171.1.1.1.13.11
Signing Server eID LU DelegatedSign QCP-n-qscd EC	1.3.171.1.1.1.13.12
Smartcard QCP - Integration EC	1.3.171.1.1.1.13.13
Smartcard NCP+ - Integration EC	1.3.171.1.1.1.13.14
Signing Server Itsme DelegatedSign QCP-n-qscd EC	1.3.171.1.1.1.13.15
Smartcard Integration DelegatedSign QCP EC	1.3.171.1.1.1.13.16

LuxTrust Global Qualified CA RSA x CA CPS OID: 1.3.171.1.1.1.14 Certificates OID Branch: 1.3.171.1.1.1.14.x	
Smartcard eSeal QCP-I-qscd RSA	1.3.171.1.1.1.14.1
Smartcard eSeal NCP+ RSA	1.3.171.1.1.1.14.2
Smartcard QCP-n-qscd RSA	1.3.171.1.1.1.14.3
Smartcard NCP+ RSA	1.3.171.1.1.1.14.4
Smartcard eID QCP-n-qscd RSA	1.3.171.1.1.1.14.5
Smartcard eID NCP+ RSA	1.3.171.1.1.1.14.6
Signing Server QCP-n-qscd RSA	1.3.171.1.1.1.14.7
Signing Server QCP-I-qscd RSA	1.3.171.1.1.1.14.8
eSeal QCP-I RSA	1.3.171.1.1.1.14.9
Signing Server eID BE DelegatedSign QCP-n-qscd RSA	1.3.171.1.1.1.14.10
Signing Server LuxTrust PRI/PRO DelegatedSign QCP-n-qscd RSA	1.3.171.1.1.1.14.11
Signing Server eID LU DelegatedSign QCP-n-qscd RSA	1.3.171.1.1.1.14.12
Smartcard QCP - Integration RSA	1.3.171.1.1.1.14.13
Smartcard NCP+ - Integration RSA	1.3.171.1.1.1.14.14
Signing Server Itsme DelegatedSign QCP-n-qscd RSA	1.3.171.1.1.1.14.15
Smartcard Integration DelegatedSign QCP RSA	1.3.171.1.1.1.14.16

Or a two-level CA hierarchy which is covered by the document “LuxTrust Global Root CA - Certificate Profiles”

Note 1: Unless explicitly otherwise indicated, “the CA”, refers to the LuxTrust CAs granted to issue Certificates under responsibility of LuxTrust S.A. acting as TSP. “The CA” is thus legally designating LuxTrust S.A. acting as TSP.

LuxTrust S.A. acting as TSP ensures the availability of all services pertaining to the Certificates, including the issuance, suspension/un-suspension/revocation and renewal services as they may become available or required in specific applications.

CERTIFICATE AND CRL PROFILES

1. Certificate types

The following table indicates and shortly describes the various types of certificates that are to be issued by LuxTrust under the two LuxTrust Qualified Timestamping CAs and the two LuxTrust Global Qualified CA:

CP identification	CP OID	CPS OID	Short Description
LuxTrust Qualified TimeStamping Certification Authority			
Timestamping Certificate Profile EC	1.3.171.1.1.1.16.1	1.3.171.1.1.1.16	ETSI EN 319 421 compliant Certificate on HSM with creation of the keys by the TSP, EC : ecdsa-with-SHA512, twelve (12) years validity with two (2) years Private Key Usage.
Timestamping Certificate Profile RSA	1.3.171.1.1.1.17.1	1.3.171.1.1.1.17	ETSI EN 319 421 compliant Certificate on HSM with creation of the keys by the TSP, RSA : rsassaPss SHA512, twelve (12) years validity with two (2) years Private Key Usage.
LuxTrust Global Qualified Certification Authority			
Smartcard eSeal QCP-I-qscd	1.3.171.1.1.1.13.1	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard eSeal QCP-I-qscd	1.3.171.1.1.1.14.1	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard eSeal NCP+	1.3.171.1.1.1.13.2	1.3.171.1.1.1.13	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard eSeal NCP+	1.3.171.1.1.1.14.2	1.3.171.1.1.1.14	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard QCP-n-qscd	1.3.171.1.1.1.13.3	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard QCP-n-qscd	1.3.171.1.1.1.14.3	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard NCP+	1.3.171.1.1.1.13.4	1.3.171.1.1.1.13	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard NCP+	1.3.171.1.1.1.14.4	1.3.171.1.1.1.14	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.

CP identification	CP OID	CPS OID	Short Description
Smartcard eID QCP-n-qscd	1.3.171.1.1.1.13.5	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P384, sixty-one (61) to one hundred and twenty-one (121) months validity. RSA 3072 bit up to 4096 bit, sixty-one (61) months validity.
Smartcard eID QCP-n-qscd	1.3.171.1.1.1.14.5	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P384, sixty-one (61) to one hundred and twenty-one (121) months validity. RSA 3072 bit up to 4096 bit, sixty-one (61) months validity.
Smartcard eID NCP+	1.3.171.1.1.1.13.6	1.3.171.1.1.1.13	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P384, sixty-one (61) to one hundred and twenty-one (121) months validity. RSA 3072 bit up to 4096 bit, sixty-one (61) months validity.
Smartcard eID NCP+	1.3.171.1.1.1.14.6	1.3.171.1.1.1.14	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P384, sixty-one (61) to one hundred and twenty-one (121) months validity. RSA 3072 bit up to 4096 bit, sixty-one (61) months validity.
Signing Server QCP-n-qscd	1.3.171.1.1.1.13.7	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Signing Server QCP-n-qscd	1.3.171.1.1.1.14.7	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Signing Server QCP-l-qscd	1.3.171.1.1.1.13.8	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Signing Server QCP-l-qscd	1.3.171.1.1.1.14.8	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
eSeal QCP-l	1.3.171.1.1.1.13.9	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the Subject, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
eSeal QCP-l	1.3.171.1.1.1.14.9	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the Subject, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Signing Server eID BE DelegatedSign QCP-n-qscd	1.3.171.1.1.1.13.10	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Signing Server eID BE DelegatedSign QCP-n-qscd	1.3.171.1.1.1.14.10	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Signing Server LuxTrust PRI/PRO DelegatedSign QCP-n-qscd	1.3.171.1.1.1.13.11	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.

CP identification	CP OID	CPS OID	Short Description
Signing Server LuxTrust PRI/PRO DelegatedSign QCP-n-qscd	1.3.171.1.1.1.14.11	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Signing Server eID LU DelegatedSign QCP-n-qscd	1.3.171.1.1.1.13.12	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Signing Server eID LU DelegatedSign QCP-n-qscd	1.3.171.1.1.1.14.12	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Smartcard QCP - Integration	1.3.171.1.1.1.13.13	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard QCP - Integration	1.3.171.1.1.1.14.13	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard NCP+ - Integration	1.3.171.1.1.1.13.14	1.3.171.1.1.1.13	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity.
Smartcard NCP+ - Integration	1.3.171.1.1.1.14.14	1.3.171.1.1.1.14	ETSI EN 319 411-1 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, thirty-six (36) months validity..
Signing Server Itsme DelegatedSign QCP-n-qscd	1.3.171.1.1.1.13.15	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Signing Server Itsme DelegatedSign QCP-n-qscd	1.3.171.1.1.1.14.15	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the TSP, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Smartcard Integration DelegatedSign QCP	1.3.171.1.1.1.13.16	1.3.171.1.1.1.13	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the Subject, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.
Smartcard Integration DelegatedSign QCP	1.3.171.1.1.1.14.16	1.3.171.1.1.1.14	ETSI EN 319 411-2 compliant Certificate with creation of the keys by the Subject, EC : ECDSA_P256 & ECDSA_P384 / RSA 3072 bit up to 4096 bit, fifteen (15) minutes validity.

Subscriber's Agreement (Purchase Orders and General Terms and Conditions) is made available to customers by LuxTrust S.A. acting as TSP.

In addition to these "external" certificate types, "Internal Certificate Policies" are exclusively reserved by LuxTrust S.A. acting as TSP for issuance of security credentials (and certificates) within the management and operation domains of the LuxTrust PKI. This encompasses but is not limited to PKI component services provider's entities (e.g., RA, SRA, TSAs, devices, components, etc.), specific officers considered as security officers, etc.

Within the present document, Certificates issued by LuxTrust S.A. acting as TSP are collectively called the "Certificates" regardless of their type, unless they are more clearly and specifically identified.

In addition to the above described certifications services, the LuxTrust TSP activities include the LuxTrust Time Stamping Services (TSS). These services consist of the management of the infrastructure, and the provisioning of Time Stamp Tokens according to the LuxTrust Time Stamping Policy.

These services are provided by LuxTrust S.A. acting as LuxTrust Trusted Time Stamping Services Provider (TTSSP) to the Subscribers and are an integral part of the LuxTrust PKI. Hereafter the term TSP includes the activities and provision of trusted time stamping services as expressed in the (eIDAS) regulation). LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy.

The LuxTrust CSP Board acts as Policy Approval Authority for LuxTrust S.A. In particular the CSP board manages the LuxTrust Certification Practice Statement (CPS) and all related CPs, covering the statements of the practices followed by LuxTrust S.A. acting as TSP in issuing CA and end-entities certificates as well as in issuing TSTs through its TSAs.

By means of the CPS and related CPs, LuxTrust S.A. acting as TSP indicates and guarantees that it complies with regulatory and standard texts applicable, and whether or not this guarantee is supported by an accreditation as well as the name and coordinates of the accreditation body

1.1 Certificate extensions

X.509 v3 extensions are supported and used as indicated in the Certificates profiles as described in the present document.

1.2 Algorithm object identifiers

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

1.3 Name forms

Name forms are in the X.500 distinguished name form as implemented in RFC 3739.

1.4 Name constraints

Name constraints are supported as per RFC 5280.

1.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

1.6 Usage of Policy Constraints extension

Usage of Policy Constraints extension is supported as per RFC 5280.

1.7 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 5280 is supported.

2. Certification Authorities – Certificates profiles

LuxTrust certificates are X.509 v3, compliant with RFC 5280.

LuxTrust CAs certificate profiles description is available as follows:

2.1 LuxTrust Qualified TimeStamping CA-RSA

<u>Field</u>	<u>Field OID</u>	.	<u>LuxTrust Qualified TimeStamping CA RSA</u>
		Version	
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified TimeStamping CA RSA
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976988
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	20Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified TimeStamping CA RSA
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976988
		PublicKey	RSA - 1.2.840.113549.1.1.1 4096 bits public exponent: Fermat-4 (=010001).
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.17
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

Text in Red: Critical extension

2.2 LuxTrust Qualified TimeStamping CA-EC

Field	Field OID	-	LuxTrust Qualified TimeStamping CA EC
		Version	
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	ecdsa-with-SHA512
		SignatureValue	
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified TimeStamping CA EC
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976987
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	25Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified TimeStamping CA EC
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976987
		PublicKey	ECC - 1.2.840.10045.2.1 ECDSA_P521 - 1.3.132.0.35
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.16
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

Text in Red: Critical extension

2.3 LuxTrust Global Qualified CA-EC

Field	Field OID	:	LuxTrust Global Qualified CA 4 EC
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	ecdsa-with-SHA512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 EC
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	25Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 EC
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
		PublicKey	ECC - 1.2.840.10045.2.1 ECDSA_P521 - 1.3.132.0.35
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.13
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

Text in Red: Critical extension

2.4 LuxTrust Global Qualified CA-RSA

Field	Field OID	:	LuxTrust Global Qualified CA 4 EC
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 RSA
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	20Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 RSA
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
		PublicKey	RSA - 1.2.840.113549.1.1.1 4096 bits public exponent: Fermat-4 (=010001).
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.14
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

Text in Red: Critical extension

3. End Entity – Certificates profiles

3.1 Certificate profiles

Under the LuxTrust CAs, multiple types of certificates will be issued.

Depending on the device used, the following types of certificates are issued by the LuxTrust Global Qualified CA :

- Device provided by LuxTrust:
 - QSCD Smartcard for signature
 - These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
 - One LuxTrust QCP-n-qscd Certificate Profile for the purpose of creating qualified electronic signature,
 - One LuxTrust NCP+ Certificate Profile for the purpose of data/entity authentication
 - QSCD Smartcard for seal
 - These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
 - One LuxTrust QCP-l-qscd Certificate Profile for the purpose of creating qualified electronic seal,
 - One LuxTrust NCP+ Certificate Profile for the purpose of data/entity authentication
 - QSCD signature server – remote electronic signature
 - These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy
 - One LuxTrust QCP-n-qscd certificate for the purpose of creating qualified electronic signature,
 - QSCD seal server – remote electronic seal
 - These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy
 - One LuxTrust QCP-l-qscd certificate for the purpose of creating qualified electronic seal,
- Device provided by the customer
 - One LuxTrust QCP-l certificate for the purpose of advanced electronic seal

3.2 Version number(s)

X.509 v3 is supported and used.

3.3 Certificate Policy for LT Qualified Timestamping

- LuxTrust Qualified Timestamping CA EC : 1.3.171.1.1.1.16
- LuxTrust Qualified Timestamping CA RSA : 1.3.171.1.1.1.17

The end-entity policy identifier is the concatenation of the OID of the corresponding CA with the value specified in PolicyIdentifier-1

3.3.1 NCP+ Certificate Policy for LT Qualified Timestamping

LuxTrust Timestamping Certificates are issues by the LuxTrust Qualified Timestamping CA with keys located on HSM devices, with generation by LuxTrust TSP according to the processes and procedures described in the applicable CP.

The profiles of the public key certificates used by the LuxTrust QTS CA comply with the RFC 3161 and RFC5816.

This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 2024/1183. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles. This profile complies with the requirements of the standard ETSI EN 319 411-1 describing the Requirements for trust service providers issuing Extended Normalized Certificate Policy.

Field	Field OID		Timestamping
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20977002
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	12Y
Subject			
	2.5.4.3	commonName	LuxTrust Qualified Timestamping
	2.5.4.6	countryName	LU
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.
	2.5.29.16	privateKeyUsagePeriod	24M
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://qtsca.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qtsca.luxtrust.lu/LTQTSCA-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	http://qtsca.crl.luxtrust.lu/LTQTSCA-XX-1.crl
subjectAltName	2.5.29.17		

	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.8	TimeStamping	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.1
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a

Text in Red : Critical extension

3.4 Certificate Policy for LT Global Qualified CA

- LuxTrust Global Qualified CA EC : 1.3.171.1.1.1.13
- LuxTrust Global Qualified CA RSA : 1.3.171.1.1.1.14

The end-entity policy identifier is the concatenation of the OID of the corresponding CA with the value specified in PolicyIdentifier-1

3.4.1 Smartcard eSeal QCP-I-qscd

LuxTrust Certificates for Qualified Seal Signature Services are Qualified Certificates generated on Secure User Device, with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic eSeals as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified eSeals supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.1 || 1.3.171.1.1.1.14.1 >.

Field	Field OID		Smartcard eSeal QCP-I-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	SSN1
	2.5.4.3	commonName	CN2
	2.5.4.42	givenName	n/a
	2.5.4.4	surname	n/a
	2.5.4.6	countryName	C2
	1.2.840.113549.1.9.1	emailAddress	n/a
	2.5.4.12	title	n/a
	2.5.4.10	organizationName	O2
	2.5.4.7	localityName	n/a
	2.5.4.11	organizationalUnitName 1	O03
	2.5.4.11	organizationalUnitName 2	n/a
	2.5.4.97	organizationIdentifier	O11

		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	<a href="http://<LastDigitOID>.qca4.ocsp.luxtrust.lu">http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.1
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.3
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.2

3.4.2 Smartcard eSeal NCP+

LuxTrust Certificates for Advanced Seal Signature Services are Advanced Certificates generated on Secure User Device, with creation of the keys by LuxTrust. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eSeals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate

policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.2 || 1.3.171.1.1.1.14.2>.

Field	Field OID		Smartcard eSeal NCP+
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	SSN1
	2.5.4.3	commonName	CN2
	2.5.4.42	givenName	n/a
	2.5.4.4	surname	n/a
	2.5.4.6	countryName	C2
	1.2.840.113549.1.9.1	emailAddress	n/a
	2.5.4.12	title	n/a
	2.5.4.10	organizationName	O2
	2.5.4.7	localityName	n/a
	2.5.4.11	organizationalUnitName 1	OUB3
	2.5.4.11	organizationalUnitName 2	n/a
	2.5.4.97	organizationIdentifier	O11
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	n/a

	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.2
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	n/a
	0.4.0.1862.1.4	QcSSCD	n/a
	0.4.0.1862.1.5	QcPDS	n/a
	0.4.0.1862.1.6	QcType	n/a

3.4.3 Smartcard QCP-n-qscd

LuxTrust Certificates for Qualified Signature Service are Qualified Certificate generated on a Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.3 || 1.3.1717.1.1.1.14.3>.

Field	Field OID		Smartcard QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	SSN1

	2.5.4.3	commonName	CN1
	2.5.4.42	givenName	GN1
	2.5.4.4	surname	SN1
	2.5.4.6	countryName	C1
	1.2.840.113549.1.9.1	emailAddress	E1
	2.5.4.12	title	T1
	2.5.4.10	organizationName	O1
	2.5.4.7	localityName	L1
	2.5.4.11	organizationalUnitName 1	OU1
	2.5.4.11	organizationalUnitName 2	OU2
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.3
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS

	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1
--	----------------	--------	------------------

3.4.4 Smartcard NCP+

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.4 || 1.3.171.1.1.1.14.4>.

Field	Field OID		Smartcard NCP+
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976989
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	SSN1
	2.5.4.3	commonName	CN1
	2.5.4.42	givenName	GN1
	2.5.4.4	surname	SN1
	2.5.4.6	countryName	C1
	1.2.840.113549.1.9.1	emailAddress	E1
	2.5.4.12	title	T1
	2.5.4.10	organizationName	O1
	2.5.4.7	localityName	L1
	2.5.4.11	organizationalUnitName 1	OU1
	2.5.4.11	organizationalUnitName 2	OU2
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		

	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	E2
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.4
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	n/a
	0.4.0.1862.1.4	QcSSCD	n/a
	0.4.0.1862.1.5	QcPDS	n/a
	0.4.0.1862.1.6	QcType	n/a

3.4.5 Smartcard eID NCP+

LuxTrust Certificate for Advanced Authentication Service are Normalized Certificate generated on a Secure User Device (e.g., Luxemburgish eID Smartcard) with creation of the keys by LuxTrust. The usage purpose of these certificate is limited to sole authorized usage of supporting authentication service supported by advanced certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.6 || 1.3.171.1.1.1.14.6 >

Field	Field OID		Smartcard eID NCP+
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU

	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976991
Validity			
	<i>n/a</i>	NotBefore	Certificate generation process date/time.
	<i>n/a</i>	NotAfter = NotBefore + x	12M 24M 60M 120M
Subject			
	2.5.4.5	SerialNumber	<i>SSN1</i>
	2.5.4.3	commonName	<i>CNeID</i>
	2.5.4.42	givenName	<i>GNeID</i>
	2.5.4.4	surname	<i>SNeID</i>
	2.5.4.6	countryName	LU
	1.2.840.113549.1.9.1	emailAddress	<i>E1</i>
	2.5.4.12	title	Private Person
	2.5.4.10	organizationName	<i>n/a</i>
	2.5.4.7	localityName	<i>n/a</i>
	2.5.4.11	organizationalUnitName 1	<i>OU4</i>
	2.5.4.11	organizationalUnitName 2	<i>n/a</i>
	2.5.4.97	organizationIdentifier	<i>n/a</i>
		PublicKey	<p>RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.</p> <p>ECC - 1.2.840.10045.2.1 ECDSA_P384 - ansip384r1 - 1.3.132.0.34</p>
	2.5.29.16	privateKeyUsagePeriod	<i>n/a</i>
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		<i>n/a</i>
subjectAltName	2.5.29.17		
		Rfc822Name	<i>E2</i>
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	<i>n/a</i>	digitalSignature	TRUE
	<i>n/a</i>	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	<i>n/a</i>
	1.3.6.1.5.5.7.3.8	TimeStamping	<i>n/a</i>
certificatePolicies	2.5.29.32		
	<i>n/a</i>	PolicyIdentifier-1	.6
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com

	<i>n/a</i>	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	<i>n/a</i>	CA	FALSE
	<i>n/a</i>	pathLenConstraint	<i>n/a</i>
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	<i>n/a</i>
	0.4.0.1862.1.4	QcSSCD	<i>n/a</i>
	0.4.0.1862.1.5	QcPDS	<i>n/a</i>
	0.4.0.1862.1.6	QcType	<i>n/a</i>

3.4.6 Signing Server QCP-n-qscd

LuxTrust Certificates for Qualified Signature Service are Qualified Certificate generated on a Remote Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.7 || 1.3.1717.1.1.1.14.7>.

Field	Field OID		Signing Server QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976992
Validity			
	<i>n/a</i>	NotBefore	Certificate generation process date/time.
	<i>n/a</i>	NotAfter = NotBefore + x	Up to 36M
Subject			
	2.5.4.5	SerialNumber	<i>SSN1</i>
	2.5.4.3	commonName	<i>CN1</i>
	2.5.4.42	givenName	<i>GN1</i>
	2.5.4.4	surname	<i>SN1</i>
	2.5.4.6	countryName	<i>C1</i>
	1.2.840.113549.1.9.1	emailAddress	<i>E1</i>
	2.5.4.12	title	<i>T1</i>
	2.5.4.10	organizationName	<i>O1</i>
	2.5.4.7	localityName	<i>L1</i>

	2.5.4.11	organizationalUnitName 1	<i>OUI</i>
	2.5.4.11	organizationalUnitName 2	<i>OUI</i>
	2.5.4.97	organizationIdentifier	<i>n/a</i>
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	<i>n/a</i>
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	<a href="http://<LastDigitOID>.qca4.ocsp.luxtrust.lu">http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		<i>n/a</i>
subjectAltName	2.5.29.17		
		Rfc822Name	<i>E2</i>
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	<i>n/a</i>	digitalSignature	FALSE
	<i>n/a</i>	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	<i>n/a</i>
	1.3.6.1.5.5.7.3.8	TimeStamping	<i>n/a</i>
certificatePolicies	2.5.29.32		
	<i>n/a</i>	PolicyIdentifier-1	.7
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	<i>n/a</i>	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	<i>n/a</i>	CA	FALSE
	<i>n/a</i>	pathLenConstraint	<i>n/a</i>
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	<i>PDS</i>
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1

3.4.7 Signing Server QCP-I-qscd

LuxTrust Certificates for Qualified Seal Signature Services are Qualified Certificates generated on a Remote Secure User Device, with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic eSeals as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified

eSeals supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.8 || 1.3.171.1.1.1.14.8 >.

Field	Field OID		Signing Server QCP-I-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976993
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	60M
Subject			
	2.5.4.5	SerialNumber	SSN1
	2.5.4.3	commonName	CN2
	2.5.4.42	givenName	n/a
	2.5.4.4	surname	n/a
	2.5.4.6	countryName	C2
	1.2.840.113549.1.9.1	emailAddress	n/a
	2.5.4.12	title	n/a
	2.5.4.10	organizationName	O2
	2.5.4.7	localityName	n/a
	2.5.4.11	organizationalUnitName 1	OU3
	2.5.4.11	organizationalUnitName 2	OU3
	2.5.4.97	organizationIdentifier	O11
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a

subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.8
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.3
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.2

3.4.8 eSeal QCP-I

LuxTrust Certificates for Advanced Seal Signature Services are Qualified Certificates generated by LuxTrust, with creation of the keys by the Subject. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eSeals supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.9 || 1.3.171.1.1.1.14.9 >.

Field	Field OID		eSeal QCP-I
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976994
Validity			
	n/a	NotBefore	Certificate generation process date/time.

	<i>n/a</i>	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	<i>SSN1</i>
	2.5.4.3	commonName	<i>CN2</i>
	2.5.4.42	givenName	<i>n/a</i>
	2.5.4.4	surname	<i>n/a</i>
	2.5.4.6	countryName	<i>C2</i>
	1.2.840.113549.1.9.1	emailAddress	<i>n/a</i>
	2.5.4.12	title	<i>n/a</i>
	2.5.4.10	organizationName	<i>O2</i>
	2.5.4.7	localityName	<i>n/a</i>
	2.5.4.11	organizationalUnitName 1	<i>OU3</i>
	2.5.4.11	organizationalUnitName 2	<i>OU3</i>
	2.5.4.97	organizationIdentifier	<i>OI1</i>
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	<i>n/a</i>
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	<a href="http://<LastDigitOID>.qca4.ocsp.luxtrust.lu">http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		<i>n/a</i>
subjectAltName	2.5.29.17		
		Rfc822Name	<i>n/a</i>
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	<i>n/a</i>	digitalSignature	FALSE
	<i>n/a</i>	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	<i>n/a</i>
	1.3.6.1.5.5.7.3.8	TimeStamping	<i>n/a</i>
certificatePolicies	2.5.29.32		
	<i>n/a</i>	PolicyIdentifier-1	.9
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	<i>n/a</i>	PolicyIdentifier-2	0.4.0.194112.1.1
BasicConstraints	2.5.29.19		
	<i>n/a</i>	CA	FALSE
	<i>n/a</i>	pathLenConstraint	<i>n/a</i>
QcStatements	0.4.0.1862.1		

	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	<i>n/a</i>
	0.4.0.1862.1.5	QcPDS	<i>PDS</i>
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.2

3.4.9 Signing Server eID BE Delegated Sign QCP-n-qscd

LuxTrust Certificate for Qualified Signature Service are Qualified Certificate generated on a Remote Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. This profile is only associated with identification performed with a notified eID BE and notified foreign eID BE. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.10 || 1.3.171.1.1.1.14.10 >

Field	Field OID		Signing Server eID BE Delegated Sign QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976995
Validity			
	<i>n/a</i>	NotBefore	Certificate generation process date/time.
	<i>n/a</i>	NotAfter = NotBefore + x	15m
Subject			
	2.5.4.5	SerialNumber	<i>V1</i>
	2.5.4.3	commonName	<i>V1</i>
	2.5.4.42	givenName	<i>V1</i>
	2.5.4.4	surname	<i>V1</i>
	2.5.4.6	countryName	<i>V1</i>
	1.2.840.113549.1.9.1	emailAddress	<i>n/a</i>
	2.5.4.12	title	<i>n/a</i>
	2.5.4.10	organizationName	<i>n/a</i>
	2.5.4.7	localityName	<i>n/a</i>
	2.5.4.11	organizationalUnitName 1	<i>n/a</i>
	2.5.4.11	organizationalUnitName 2	<i>n/a</i>
	2.5.4.97	organizationIdentifier	<i>n/a</i>

		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	n/a
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	n/a
cRLDistributionPoints	2.5.29.31		
		cdp-url	n/a
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		TRUE
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.10
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1

3.4.10 Signing Server LuxTrust PRI/PRO Delegated Sign QCP-n-qscd

LuxTrust Certificate for Qualified Signature Service are Qualified Certificate generated on a Remote Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. This profile is only associated with identification performed with a qualified LuxTrust PRI/PRO certificate. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.11 || 1.3.171.1.1.1.14.11 >

Field	Field OID		Signing Server LuxTrust PRI/PRO Delegated Sign QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976996
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	15m
Subject			
	2.5.4.5	SerialNumber	V2
	2.5.4.3	commonName	V2
	2.5.4.42	givenName	V2
	2.5.4.4	surname	V2
	2.5.4.6	countryName	V2
	1.2.840.113549.1.9.1	emailAddress	V2
	2.5.4.12	title	V2
	2.5.4.10	organizationName	V2
	2.5.4.7	localityName	V2
	2.5.4.11	organizationalUnitName 1	V2
	2.5.4.11	organizationalUnitName 2	V2
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	n/a
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	n/a
cRLDistributionPoints	2.5.29.31		
		cdp-url	n/a
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		TRUE
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits

keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.11
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1

3.4.11 Signing Server eID LU Delegated Sign QCP-n-qscd

LuxTrust Certificate for Qualified Signature Service are Qualified Certificate generated on a Remote Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. This profile is only associated with identification performed with identification performed with a notified eID LU. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.12 || 1.3.171.1.1.1.14.12 >

Field	Field OID		Signing Server eID LU Delegated Sign QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976997
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	15m
Subject			

	2.5.4.5	SerialNumber	V3
	2.5.4.3	commonName	V3
	2.5.4.42	givenName	V3
	2.5.4.4	surname	V3
	2.5.4.6	countryName	V3
	1.2.840.113549.1.9.1	emailAddress	V3
	2.5.4.12	title	V3
	2.5.4.10	organizationName	n/a
	2.5.4.7	localityName	n/a
	2.5.4.11	organizationalUnitName 1	V3
	2.5.4.11	organizationalUnitName 2	n/a
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	n/a
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	n/a
cRLDistributionPoints	2.5.29.31		
		cdp-url	n/a
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		TRUE
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.12
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE

	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1

3.4.12 Smartcard QCP – Integration

LuxTrust Certificate for Signature Service are Qualified Certificate with creation of the keys by the subject and subscriber LuxTrust. This profile aims at issuing advanced electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of testing and monitoring the signature service. It is only associated with an internal LuxTrust identification carried out in accordance with LuxTrust's internal procedures. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.13 || 1.3.171.1.1.1.14.13>

Field	Field OID		Smartcard QCP - Integration
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976998
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	SSN2
	2.5.4.3	commonName	CN3
	2.5.4.42	givenName	GN3
	2.5.4.4	surname	SN3
	2.5.4.6	countryName	LU
	1.2.840.113549.1.9.1	emailAddress	n/a
	2.5.4.12	title	T1
	2.5.4.10	organizationName	O1
	2.5.4.7	localityName	L1
	2.5.4.11	organizationalUnitName 1	OU1
	2.5.4.11	organizationalUnitName 2	OU2
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34

	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.13
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.0
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	n/a
	0.4.0.1862.1.4	QcSSCD	n/a
	0.4.0.1862.1.5	QcPDS	n/a
	0.4.0.1862.1.6	QcType	n/a

3.4.13 Smartcard NCP+ - Integration

LuxTrust Certificate for Authentication Service are Certificate with creation of the keys by the subject and subscriber LuxTrust. This profile aims at issuing advanced electronic authentication. The usage purpose of these Certificates is limited to sole authorised usage of testing and monitoring of the signature service. It is only associated with an internal LuxTrust identification carried out in accordance with LuxTrust's internal procedures. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.14 || 1.3.171.1.1.1.14.14>

Field	Field OID		Smartcard NCP+ - Integration
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy

		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976999
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	36M
Subject			
	2.5.4.5	SerialNumber	
	2.5.4.3	commonName	
	2.5.4.42	givenName	
	2.5.4.4	surname	
	2.5.4.6	countryName	
	1.2.840.113549.1.9.1	emailAddress	
	2.5.4.12	title	
	2.5.4.10	organizationName	
	2.5.4.7	localityName	
	2.5.4.11	organizationalUnitName 1	
	2.5.4.11	organizationalUnitName 2	
	2.5.4.97	organizationIdentifier	
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://<LastDigitOID>.qca4.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qca4.luxtrust.lu/LTGQCA4-XX.crt
cRLDistributionPoints	2.5.29.31		
		cdp-url	<a href="http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl">http://<LastDigitOID>.qca4.crl.luxtrust.lu/LTGQCA4-XX-Y.crl
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		n/a
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		

	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.14
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	n/a
	0.4.0.1862.1.4	QcSSCD	n/a
	0.4.0.1862.1.5	QcPDS	n/a
	0.4.0.1862.1.6	QcType	n/a

3.4.14 Signing Server Itsme Delegated Sign QCP-n-qscd

LuxTrust Certificate for Qualified Signature Service are Qualified Certificate generated on a Remote Secure User Device with creation of the keys by LuxTrust. This profile aims at issuing qualified electronic signature as per Regulation (EU) No 2024/1183. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signature supported by Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd policy. This profile is only associated with identification performed with an itsme notified eID. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.15 || 1.3.171.1.1.1.14.15>

Field	Field OID		Signing Server Itsme DelegatedSign QCP-n-qscd
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20977000
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	15m
Subject			
	2.5.4.5	SerialNumber	V4
	2.5.4.3	commonName	V4
	2.5.4.42	givenName	V4
	2.5.4.4	surname	V4

	2.5.4.6	countryName	V4
	1.2.840.113549.1.9.1	emailAddress	n/a
	2.5.4.12	title	n/a
	2.5.4.10	organizationName	n/a
	2.5.4.7	localityName	n/a
	2.5.4.11	organizationalUnitName 1	V4
	2.5.4.11	organizationalUnitName 2	n/a
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	n/a
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	n/a
cRLDistributionPoints	2.5.29.31		
		cdp-url	n/a
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		TRUE
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.15
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	TRUE
	0.4.0.1862.1.4	QcSSCD	TRUE
	0.4.0.1862.1.5	QcPDS	PDS
	0.4.0.1862.1.6	QcType	0.4.0.1862.1.6.1

3.4.15 Smartcard Integration Delegated Sign QCP

LuxTrust Certificate for Signature Service are Certificate with creation of the keys by the subject and subscriber LuxTrust. This profile aims at issuing advanced electronic signature. The usage purpose of these Certificates is limited to sole authorized usage of testing and monitoring of the signature service. It is only associated with an internal LuxTrust identification carried out in accordance with LuxTrust's internal procedures. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.1.13.16 || 1.3.171.1.1.1.14.16 >

Field	Field OID		Smartcard Integration Delegated Sign QCP
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA 4 XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20977001
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	15m
Subject			
	2.5.4.5	SerialNumber	V2
	2.5.4.3	commonName	V2
	2.5.4.42	givenName	V2
	2.5.4.4	surname	V2
	2.5.4.6	countryName	V2
	1.2.840.113549.1.9.1	emailAddress	V2
	2.5.4.12	title	V2
	2.5.4.10	organizationName	V2
	2.5.4.7	localityName	V2
	2.5.4.11	organizationalUnitName 1	V2
	2.5.4.11	organizationalUnitName 2	V2
	2.5.4.97	organizationIdentifier	n/a
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	2.5.29.16	privateKeyUsagePeriod	n/a
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		

	1.3.6.1.5.5.7.48.1	aia-ocsp-url	n/a
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	n/a
cRLDistributionPoints	2.5.29.31		
		cdp-url	n/a
id-etsi-valassured-ST-certificate	0.4.0.194121.2.1		TRUE
subjectAltName	2.5.29.17		
		Rfc822Name	n/a
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	FALSE
	n/a	contentCommitment FKA nonRepudiation	TRUE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	n/a
	1.3.6.1.5.5.7.3.8	TimeStamping	n/a
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	.16
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.194112.1.0
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a
QcStatements	0.4.0.1862.1		
	0.4.0.1862.1.1	QcCompliance	n/a
	0.4.0.1862.1.4	QcSSCD	n/a
	0.4.0.1862.1.5	QcPDS	n/a
	0.4.0.1862.1.6	QcType	n/a

Legend

XX	RSA or EC
Y	Last digit of EE CP OID
n/a	Not Applicable
SSN1	Serial Number as constructed by LRAO
CN1	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
GN1	PRO and PRIVATE products: Given name(s) as on ID card
SN1	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
C1	Nationality of holder (ISO3166)
E1	Subject's email address
T1	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
O1	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
L1	PRO products only: Company/institution country of HQ (as in articles of association)
OU1	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
OU2	PRO products only: Company/institution department or other information item
E2	Certificate Holder's email address
CN2	Shall contain the full registered name of the subject (legal person).
C2	the country in which the subject (legal person) is established (ISO3166)

<i>O2</i>	Shall contain the full registered name of the subject (legal person).
<i>OU3</i>	Company/institution department or other information item
<i>O11</i>	<p>Shall contain information using the following structure in the presented order:</p> <ul style="list-style-type: none"> - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference). <p>The three initial characters shall have one of the following defined values:</p> <ol style="list-style-type: none"> 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entity when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.
<i>PDS</i>	https://repository.luxtrust.com
keyUsage	Critical Extension
<i>GN2</i>	Given name(s) as on ID card or as provided by the RNCID
<i>OU4</i>	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
<i>V1</i>	As provided by the BE eID product
<i>V2</i>	As provided by the LuxTrust product
<i>V3</i>	As provided by the LU eID product
<i>SSN2</i>	YYYYMMDDYYYYMMDD1000
<i>CN3</i>	TSP-Chip-Monitoring TEST
<i>GN3</i>	TSP-Chip-Monitoring
<i>SN3</i>	TEST
<i>V4</i>	As provided by the Itsme product
<i>CNeID</i>	Concatenation of given name(s) and surname(s) separated by the space character
<i>GNeID</i>	Given name(s) as on ID card or as provided by the RNCID
<i>SNeID</i>	is (are) the birth name(s) as they appear on the identity card without the indication 'spouse', 'ép.' or similar and the subsequent name(s) or as they appear in the RNCID unless the applicant provides documentary evidence related to the requested family name other than the birth name as it appears on the identity document.

4. LuxTrust CRL / OCSP – Certificates profiles

4.1 CRL profile

In conformance with the IETF PKIX RFC 2459, the LuxTrust CAs support CRLs compliant with:

- Version numbers supported for CRLs
- CRL and CRL entry extensions populated and their criticality.

The profile of the CRL is provided in the table below:

LuxTrust Qualified Timestamping CA EC: 1.3.171.1.1.1.16 & RSA: 1.3.171.1.1.1.17				
Field	OID		Non Public	Public - By OID
	n/a	Version	Version 2 Value = "1"	
	n/a	SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512	
	n/a	SignatureValue	Issuing CA Signature	
Issuer				
	2.5.4.6	countryName	LU	
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX	
	2.5.4.10	organizationName	LuxTrust S.A.	
	2.5.4.97	organizationIdentifier	VATLU-20976985	
Validity				
	n/a	Last Update - UTC Time	Certificate generation process date/time. - UTC Time	
	n/a	NextUpdate = LastUpdate + x - UTC Time	24 hours = 6 hours (Update Interval) + 18 hours (Margin)	4 hours 30 minutes = 1 hour (Update Interval) + 3 hours 30 minutes (Margin)
CRL Extensions				
	2.5.29.28	Issuing Distribution Point	n/a	http://crl.luxtrust.lu/LTGTSCA-XX-Y.crl
	2.5.29.20	CRL Number	Non-critical CRL unique sequence number	
	2.5.29.60	expiredCertsOnCRL	Non-critical <CA issuance date>	n/a
	2.5.29.35	Authority Key Identifier	Non-critical <subject key identifier of the CA >	
revokedCertificates				
	n/a	Serial Number	<certificate serial number>	
	n/a	Revocation Date - UTC Time	<revocation date and time>	
	2.5.29.21	CRL Entry Extension - CRL Reason Code	<revocation reason>	

LuxTrust Global Qualified CA EC: 1.3.171.1.1.1.13 & RSA: 1.3.171.1.1.1.14				
Field	OID		Non Public	Public - By OID
	n/a	Version	Version 2 Value = "1"	
	n/a	SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512	
	n/a	SignatureValue	Issuing CA Signature	
Issuer				
	2.5.4.6	countryName	LU	
	2.5.4.3	commonName	LuxTrust Global Qualified CA XX	
	2.5.4.10	organizationName	LuxTrust S.A.	
	2.5.4.97	organizationIdentifier	VATLU-20976985	
Validity				
	n/a	Last Update - UTC Time	Certificate generation process date/time. - UTC Time	
	n/a	NextUpdate = LastUpdate + x - UTC Time	24 hours = 6 hours (Update Interval) + 18 hours (Margin)	4 hours 30 minutes = 1 hour (Update Interval) + 3 hours 30 minutes (Margin)
CRL Extensions				
	2.5.29.28	Issuing Distribution Point	n/a	http://crl.luxtrust.lu/LTGTSCA-XX-Y.crl
	2.5.29.20	CRL Number	Non-critical CRL unique sequence number	
	2.5.29.60	expiredCertsOnCRL	Non-critical <CA issuance date>	n/a
	2.5.29.35	Authority Key Identifier	Non-critical <subject key identifier of the CA >	
revokedCertificates				
	n/a	Serial Number	<certificate serial number>	
	n/a	Revocation Date - UTC Time	<revocation date and time>	
	2.5.29.21	CRL Entry Extension - CRL Reason Code	<revocation reason>	

XX	RSA or EC
Y	Last digit of EE CP OID
n/a	Not Applicable
<Field>	Critical Extension

4.2 OCSP profile

The OCSP profile follows IETF PKIX RFC 6960 OCSP v1 and v2. The LuxTrust CAs support signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA.

The following table provides the description of the fields for LuxTrust OCSP profile.

LuxTrust Qualified Timestamping CA EC: 1.3.171.1.1.1.16 & RSA: 1.3.171.1.1.1.17			
Field	Field OID		
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	3M
Subject			
	2.5.4.3	commonName	LuxTrust S.A. OCSP Server
	2.5.4.6	countryName	LU
	2.5.4.10	organizationName	LuxTrust S.A.
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
subjectAltName	2.5.29.17		
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	TRUE
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE

LuxTrust Global Qualified CA EC: 1.3.171.1.1.1.13 & RSA: 1.3.171.1.1.1.14			
Field	Field OID		
		Version	Version 3 Value = "2"
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Global Qualified CA XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	3M
Subject			
	2.5.4.3	commonName	LuxTrust S.A. OCSP Server
	2.5.4.6	countryName	LU
	2.5.4.10	organizationName	LuxTrust S.A.
		PublicKey	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
subjectAltName	2.5.29.17		
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	TRUE
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE