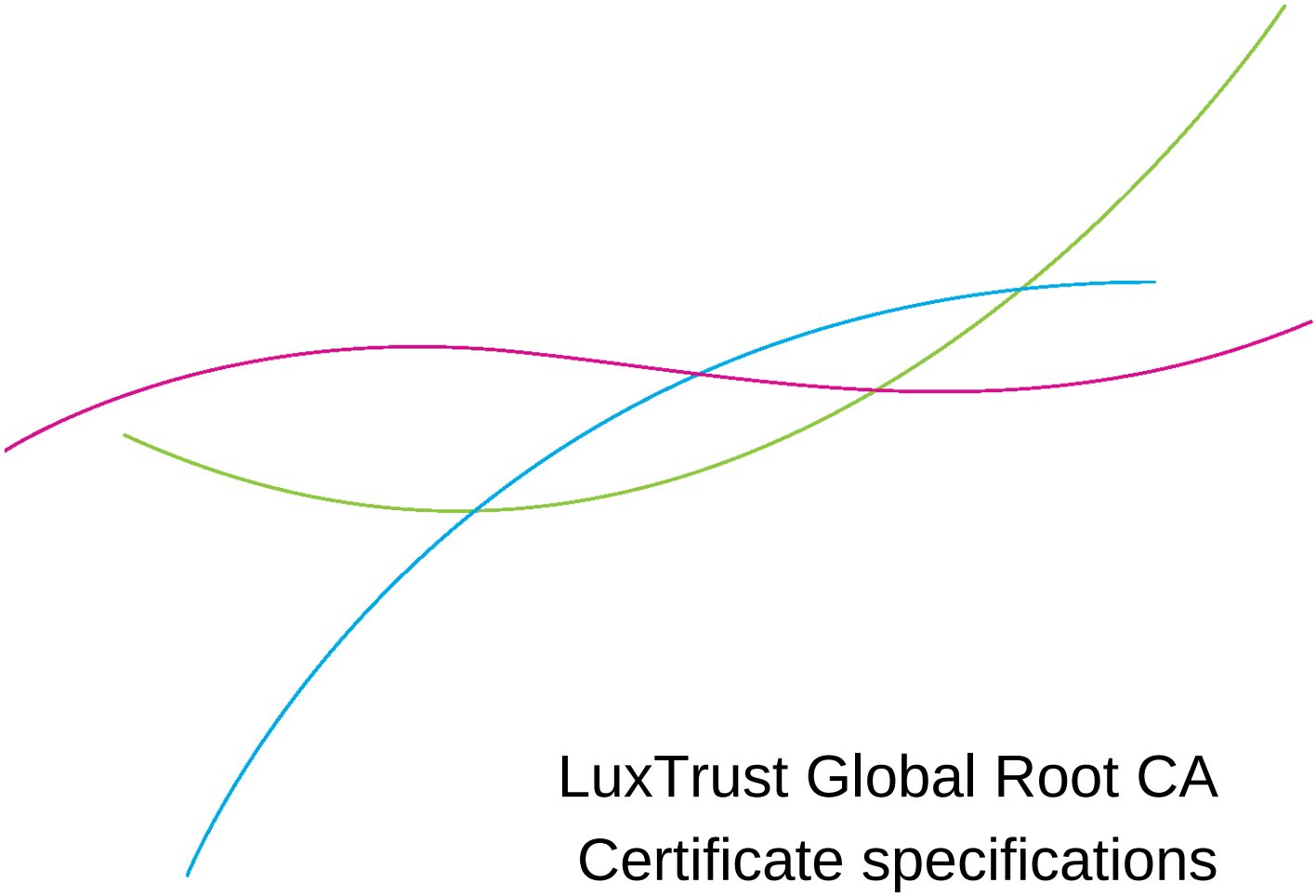
LUXTRUST®
Enabling a digital world



LuxTrust Global Root CA
Certificate specifications

Version number: 1.26
Publication Date: 13/02/2018
Effective Date: 27/02/2018

LuxTrust S.A
IVY Building | 13-15, Parc d'activités | L-8308 Capellen
Luxembourg | VAT LU 20976985 | RCS B112233
Business Number N°00135240/0
Phone: +352 26 68 15 – 1
Fax: +352 26 68 15 – 789

ILNAS
Institut luxembourgeois de la normalisation de l'accréditation, de la sécurité et qualité des produits et services

PRESTATAIRE DE SERVICES DE CONFIANCE QUALIFIÉ
SUPERVISION N°2016/8/001
Règlement européen n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance

Document Information

Document title:	LuxTrust Global Root CA - Certificate specifications
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Technical Specification
Document Distribution List	Any
Document Classification	Public
Document Owner	CSP Board

Version History

Version	Who	Date	Reason of modification
1.0	MSC	29/08/2011	Initial Version DRAFT
1.01	MSC	27/10/2011	Added CRL validity period, revision
1.02	MSC	24/11/2011	Modified – Document OIDs for Cas
1.03	MSC	09/02/2012	Modified – Added LCP for integration purposes.
1.04	MSC	01/03/2012	Modified: • Added LCP for integration purposes for CSS • Table for OIDs • Modification of the CRL issuance algorithm (SHA256 to SHA1)
1.05	MSC	19/03/2012	Modifications following review by Chris Quaresimin and Laurent Breuskin: • Removal of + Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime for non-SSL products • Display text for CSS integration product • Correct CRL and AIA for CSS integration product • SSL Object certificate profile
1.06	MSC	26/03/2012	Modifications for CSS certificates, signature will be performed using SHA1WithRsa. Changes performed in CSS certificate profile for prod and integration, page 43 and 51.
1.07	MSC	14/06/2012	Added: TimeStamping CA and TimeStamping certificate profile
1.08	MSC	29/06/2012	Added: Private key usage Period in TSP
1.09	LBR	01/08/2012	Added: Certificate Profiles under LuxTrust Global Qualified CA • SC LORA & LRS Certificate Modified: • Table for OIDs & LuxTrust CA Hierarchy
1.09.1	LBR	02/08/2012	Update of OID Page 22
1.09.2	MSC	07/08/2012	Added: Certificate profile for Extended Validation Certificates : • EVCP – ETSI TS 102 042 • EVCP+ - ETSI TS 102 042 Added: Certificate profile for Secure Online File Exchange (SOFiE)
1.10	YNU	23/08/2012	Review for validation of CP
1.10	CSPBoard	24/08/2012	Validation
1.11	CSPBoard	20/09/2012	Typo update
1.12	YNU TKO	21/12/2012	Added CP SSL/TLS Certificate for Client Authentication • Added CP non SSCD NCP+ Certificates supporting Advanced Electronic Signatures for Mass Signature Services • Various syntactical and format corrections
1.13	CSP Board	23/04/2013	insertion of ILNAS logo including accreditation reference and technical standards reference
1.14	YNU	29/11/2013	Update specific requirements for CP under the SSL CA
1.15	YNU	18/01/2014	Clarification on Mozilla request
1.16	YNU	05/06/2014	Update Cp - for LuxTrust Global Root Renew - QcS2 et QcS3 - Typo Add CP Seal Signature Services
1.17	YNU	30/06/2014	Add certificate profile for eID • CP eID QCP+ • CP eID NCP+ Update CP Seal Signature Services OID
1.18	YNU	15/10/2014	Update AIA in SSL CA
1.19	YNU	11/11/2014	Update AIA in CP under the SSL CA since SSL CA 2
1.20	YNU	19/12/2014	Add Integration CP for eID Update eID CP with pseudonym

			Update Global Root CA CP with OID attribute Update SSL CA profile since SSL CA 3 Update lifetime of SSL Server/Object/SSL Client auth to 24 months
1.21	CSP Board	25/03/2015	Update LT CA - lifetime up to 20 years - AIA Update Display text - EV SSL CP Update eID CP Update ILNAS Logo
1.22	YNU	03/11/2015	Update Common Names in non SSL certificates Remove NetscapeCertType extension from SSL and Object Signing Certificates Added: OCSP signing Certificate which contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560
1.23	YNU	05/08/2016	Add Timestamping Profile under Global Qualified CA Update Signing Server LCP Certificate profil
1.24	DEL	12/06/2017	Add: • LuxTrust Qualified Timestamping Certificate profile with QC statements • SPARE LuxTrust Signing Server LCP Certificate Profile • Qualified/Advanced eSeal certificate profiles • eIDAS qualified certificate profiles • Signing Server Signature and eSeal certificates and QWAC certificate and signing stick certificates
1.25	DEL	30/08/2017	• Add Microsoft OIDs in SSL certificates profiles to ensure alignement with Microsoft Trusted Root certificate Program requirements (https://technet.microsoft.com/en-us/library/cc751157.aspx).
1.26	NDE DEL DEL	24/11/2017 15/12/2017 01/01/2018	• Increase CRL validity from 4h30min to 8h30min for SSL certificates • Update hash functions in accordance with normative requirements • Add Advanced eSeal certificate profile

Table of content

Intellectual Property Rights

References

[1] The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

[3] ETSI TS 101 456 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

[4] ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[5] ETSI TS 102 023 – Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

[6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.

[7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.

[8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.

[9] Règlement Grand-Ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».

[10] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[11] LuxTrust Time Stamping Policy, latest version in force.

[12] Guidelines for the Issuance and Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.

[13] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force.

[14] eID Certificate Life Cycle Procedure latest version in force

[15] RNCID : National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16

[16] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité

[17] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité

[18] Loi du 19 juin 2013 Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques

[19] EN 319 411 – 1 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[20] EN 319 411 – 2 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[21] According to EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)

[22] According to EN 319 422 V1.1.1, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (2016-03)

[23] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)

[24] According to EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)

[25] According to EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)

[26] According to EN 319 412-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (2016-02)

[27] According to EN 319 412-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)

[28] According to EN 319 412-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)

[29] According to EN 319 412-4 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (2016-02)

[30] According to EN 319 412-5 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements (2016-02)

[31] eIDAS regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

INTRODUCTION

1.1The 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 also promotes new "e-business" and "e-government" opportunities, making the best possible use of existing legal and commercial assets which 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 provider of certification services as defined in the law of the Grand-Duchy of Luxembourg modified on 14/08/2000 [7] itself derived from the European Directive on electronic signatures (1999/93/EC; cf. [1]). These laws and directives set out the legal framework for electronic signatures in the Grand-Duchy of Luxembourg as well as for LuxTrust activities as TTP.

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

Under eIDAS [31], transitional measures are on ongoing status to support qualified smart cards and qualified trust services.

1.2 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 and accelerate eLuxembourg. Within this context, LuxTrust will form the catalyser of such services and applications.

1.3 LuxTrust PKI Hierarchy

LuxTrust S.A., acting as CSP as described in the law of Grand-Duchy of Luxembourg modified on 14/08/2000 [7], is using several Certification Authorities (CAs), as shown in the certificates hierarchy, to issue LuxTrust end-users certificates. These top level CAs are displayed on Figure 1 and figure 2.

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 CSP 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.

LuxTrust Certification Authorities

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

1.4 Two-level CA hierarchy

The top level is the *LuxTrust Global Root CA*, the highest level of authority managed by LuxTrust. The LuxTrust PKI is formed using additional subordinates CAs: The legal person (organisation) responsible for these CAs is LuxTrust S.A. acting as CSP.

The LuxTrust PKI consists in a two-level CA hierarchy:

- One “LuxTrust Global Root CA” root-signing all subordinates LuxTrust CAs

- LuxTrust subordinate CAs. Each of these CAs is root-signed by the LuxTrust Global Root CA:
  - LuxTrust Global Qualified CA
  - LuxTrust SSL CA
  - LuxTrust Time Stamping Authority

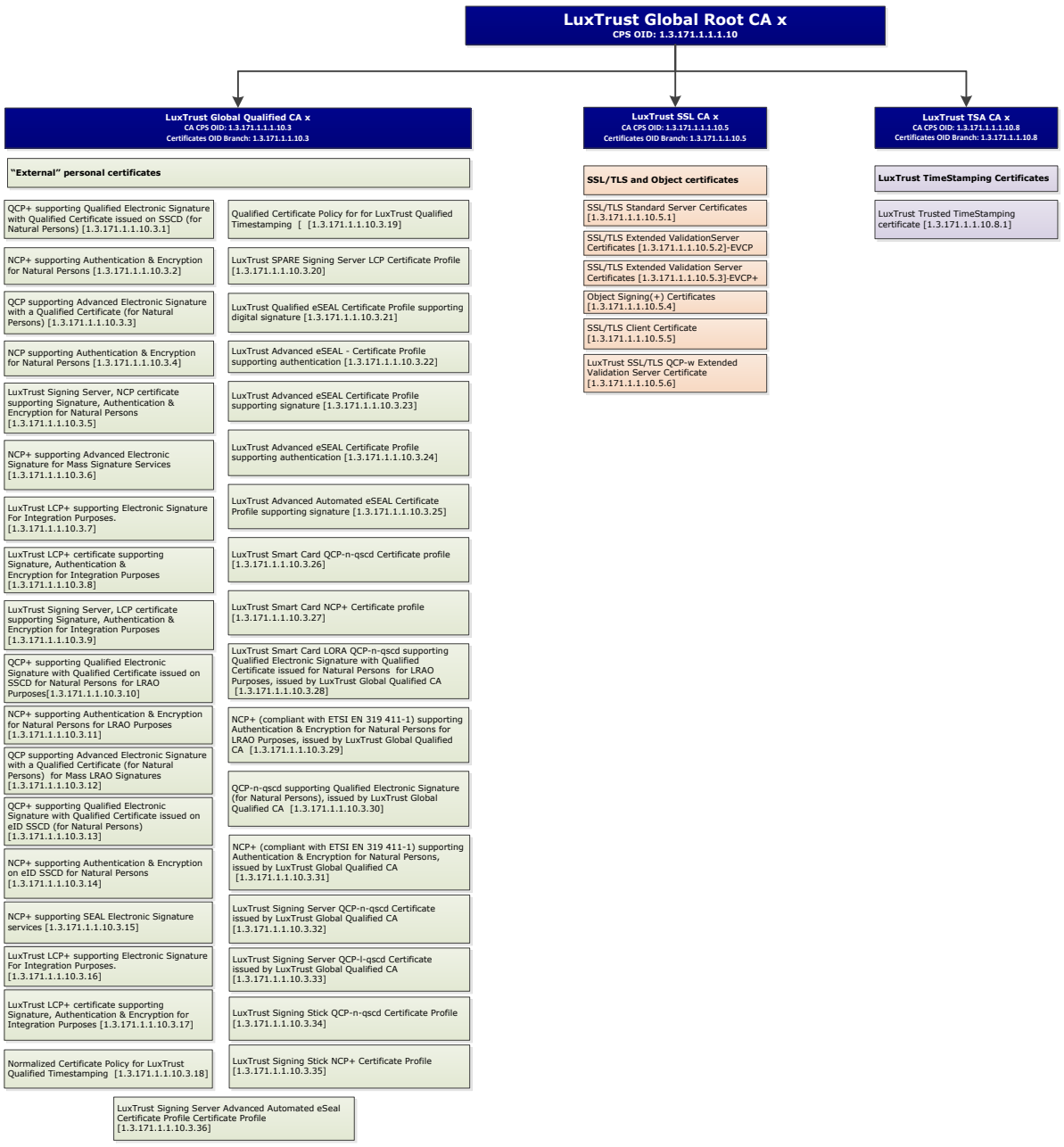
- Additional CAs or CA hierarchies might be signed in the future under the LuxTrust Global Root CA

Subordinate CAs are operating within a grant of authority for issuing certificates under the LuxTrust CPS and the applicable CP. This grant has been provided by the “LuxTrust Global Root CA” (hereafter “LTGRCA”) under the responsibility and authority of LuxTrust S.A. acting as CSP.

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

LuxTrust S.A. acting as CSP 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.

Figure 1- LuxTrust running CA Hierarchy



CERTIFICATE AND CRL PROFILES

1.5Certificate types

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

CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Qualified Certification Authority				

CP identification	CP OID	CPS OID	Short Description	Ref.
QCP+ supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.1**	**1.3.171.1.1.1.10.3**	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures
NCP+ supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.2**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption. These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption
QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.3**	**1.3.171.1.1.1.10.3**	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate.	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures
NCP supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.4**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.5**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a **non** SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption
NCP+ supporting Advanced Electronic Mass Signature Services **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.6**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Mass Signature Services.	LuxTrust NCP+ Certificates supporting Mass Signature Services

CP identification	CP OID	CPS OID	Short Description	Ref.
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.7**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.8**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.9**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for INTEGRATION PURPOSES.	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes
QCP+ supporting Qualified Electronic Signature with Qualified Certificate issued on SSCD for Natural Persons for LRAO Purposes **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.10**	**1.3.171.1.1.1.10.3**	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes
NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.11**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for LRAO Purposes.	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes
QCP supporting Advanced Electronic Signature with a Qualified Certificate for Mass LRAO Signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.12**	**1.3.171.1.1.1.10.3**	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for Mass LRAO Signatures.	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures
QCP+ supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.13**	**1.3.171.1.1.1.10.3**	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures

CP identification	CP OID	CPS OID	Short Description	Ref.
NCP+ supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.14**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption
NCP+ Advanced Electronic Seal Signature Services **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.15**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Seal Signature Services.	LuxTrust NCP+ Certificates supporting SEAL Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.16**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.17**	**1.3.171.1.1.1.10.3**	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of authentication (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption
Normalized Certificate Policy for Qualified Timestamping **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.18**	**1.3.171.1.1.1.10.3**	EN 319 421 compliant.	Normalized Certificate Policy for Qualified Timestamping
Qualified Certificate Policy for Qualified Timestamping **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.19**	**1.3.171.1.1.1.10.3**	EN 319 421 compliant.	Qualified Certificate Policy for Qualified Timestamping
LuxTrust SPARE Signing Server LCP Certificate Profile **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.20**	**1.3.171.1.1.1.10.3**	LuxTrust SPARE Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy.	SPARE Signing Server LCP Certificate Profile
LuxTrust Qualified eSEAL Certificate Profile supporting digital signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.21**	**1.3.171.1.1.1.10.3**	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-l-qscd certificate policy.	Qualified eSEAL Certificate Profile supporting digital signature

CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Advanced eSeal - Certificate Profile supporting authentication **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.22**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced eSEAL Certificate Profile supporting digital signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.23**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSEAL Certificate Profile supporting authentication **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.24**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced Automated eSEAL Certificate Supporting digital signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.25**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate on HSM compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced Mass eSEAL Certificate Profile supporting digital signature
LuxTrust Smart Card QCP-n-qscd Certificate Profile **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.26**	**1.3.171.1.1.1.10.3**	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 **QCP-n-qscd** certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature.	LuxTrust Smart Card QCP-n-qscd Certificate Profile
LuxTrust Smart Card NCP+ Certificate Profile **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.27**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose.	LuxTrust Smart Card NCP+ Certificate Profile
LuxTrust Smart Card LORA QCP-n-qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes, **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.28**	**1.3.171.1.1.1.10.3**	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 **QCP-n-qscd** certificate policy, with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smart Card LORA QCP-n-qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes,
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes, **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.29**	**1.3.171.1.1.1.10.3**	LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes,

CP identification	CP OID	CPS OID	Short Description	Ref.
QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.30**	**1.3.171.1.1.1.10.3**	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons),
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons, **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.31**	**1.3.171.1.1.1.10.3**	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons,
LuxTrust Signing Server QCP-n-qscd Certificate **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.32**	**1.3.171.1.1.1.10.3**	Signing Server certificate for qualified signature	LuxTrust Signing Server QCP-n-qscd Certificate profile
LuxTrust Signing Server QCP-l-qscd Certificate **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.33**	**1.3.171.1.1.1.10.3**	Signing Server certificate for qualified eSeal	LuxTrust Signing Server QCP-l-qscd Certificate profile
LuxTrust Signing Stick QCP-n-qscd Certificate Profile	**1.3.171.1.1.10.3.34**	**1.3.171.1.1.1.10.3**	Signing Stick QCP-n-qscd Certificate Profile	Signing Stick QCP-n-qscd Certificate Profile
LuxTrust Signing Stick NCP+ Certificate Profile	**1.3.171.1.1.10.3.35**	**1.3.171.1.1.1.10.3**	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile
LuxTrust Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	**1.3.171.1.1.10.3.36**	**1.3.171.1.1.1.10.3**	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile
LuxTrust SSL Certification Authority				
SSL/TLS Standard Server Certificates **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.1**	**1.3.171.1.1.1.10.5**	ETSI TS 102 042 **LCP** compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption

CP identification	CP OID	CPS OID	Short Description	Ref.
SSL/TLS(+) Extended Validation Server Certificates - EVCP **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.2**	**1.3.171.1.1.1.10.5**	ETSI TS 102 042 **EVCP** compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentication & Encryption
SSL/TLS(+) Extended Validation Server Certificates – EVCP+ **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.3**	**1.3.171.1.1.1.10.5**	ETSI TS 102 042 **EVCP+** compliant certificate, on Secure User Device, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Authentication & Encryption
Object Signing(+) Certificates **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.4**	**1.3.171.1.1.1.10.5**	ETSI TS 102 042 **LCP** compliant certificate produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption.	LuxTrust Object (or Code) Signing Certificates
LuxTrust SSL/TLS Certificate for Client Authentication **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.5**	**1.3.171.1.1.1.10.5**	ETSI TS 102 042 **LCP** compliant certificate produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for client authentication and secure e-mail.	LuxTrust SSL/TLS Certificate for Client Authentication
LuxTrust SSL/TLS QCP-w Extended Validation Server Certificates **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.6**	**1.3.171.1.1.1.10.5**	SSL/TLS Qualified website authentication certificate	LuxTrust SSL/TLS Qualified website authentication certificate
LuxTrust TSA (Timestamping) Certification Authority				
LuxTrust Trusted TimeStamping certificate **issued by LuxTrust TSA CA**	**1.3.171.1.1.10.8.1**	**1.3.171.1.1.1.10.8**	LuxTrust certificate compliant with ETSI TS 102 023. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority. These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	Timestamping certificate profile

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

In addition to these "external" certificate types, "Internal Certificate Policies" are exclusively reserved by LuxTrust S.A. acting as CSP 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 CSP 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 CSP 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 [11].

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 CSP includes the activities and provision of trusted time stamping services as expressed in the European Directive on electronic signatures (cf. [1]). LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy [11].

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 CSP 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 CSP 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.

LuxTrust PKI OID :	**1.3.171.1.1**			
ETSI OIDs for info	**QCP+**	**0.4.0.1456.1.1**	**EVCP+**	**0.4.0.2042.1.5**
	QCP	**0.4.0.1456.1.2**	**QCP-l**	**0.4.0.194112.1.1**
	NCP	**0.4.0.2042.1.1**	**QCP-n-qscd**	**0.4.0.194112.1.2**
	NCP+	**0.4.0.2042.1.2**	**QCP-l-qscd**	**0.4.0.194112.1.3**
	LCP	**0.4.0.2042.1.3**	**QCP-w**	**0.4.0.194112.1.4**
	EVCP	**0.4.0.2042.1.4**		

Domain	Document category	Document	Sub-document – description		LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
1 LuxTrust PKI	**LuxTrust Certification Practice Statements**								
	1 CPS LuxTrust	***1*** *CPS Summary GTE/Verizon Chain*	***0***			***x***	***y***	*1.3.171.1.**1.1.1.0.x.y***	*N/A*
		2 *Not Used*		***Not Used***		-	-	*not used*	*N/A*
		10 CPS LuxTrust Global Root Chain	**LuxTrust Global Root CA**			-	-	1.3.171.1.**1.1.10**	N/A
			3	**LuxTrust Global Qualified CA**		-	-	1.3.171.1.**1.1.10.3**	N/A
			5	**LuxTrust SSL CA**		-	-	1.3.171.1.**1.1.10.5**	N/A
			8	**LuxTrust Global Timestamping CA**		-	-	1.3.171.1.**1.1.10.8**	N/A
1 LuxTrust PKI	**LuxTrust Certificate Policies**								
	10 CP's LuxTrust Global Chain	**3 LuxTrust Global Qualified CA Certificates**	**1**	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1.**1.10.3.1**	0.4.0.1456.1.1
			2	NCP+ supporting Authentication & Encryption for Natural Persons	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1.**1.10.3.2**	0.4.0.2042.1.2
			3	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick PRI/PRO Signature Certificate	-	-	1.3.171.1.**1.10.3.3**	0.4.0.1456.1.2
			4	NCP Authentication & Encryption	Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1.**1.10.3.4**	0.4.0.2042.1.1
			5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1.**1.10.3.5**	0.4.0.2042.1.1
			6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-	-	1.3.171.1.**1.10.3.6**	0.4.0.2042.1.1

7	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration SmartCard Signature Certificate	-	-	1.3.171.1.**1.10.3.7**	0.4.0.2042.1.3
8	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration SmartCard Authentication Certificate	-	-	1.3.171.1.**1.10.3.8**	0.4.0.2042.1.3
9	LuxTrust LCP Certificates supporting Signature, Authentication & Encryption for integration purposes	Integration Signing Server Certificate	-	-	1.3.171.1.**1.10.3.9**	0.4.0.2042.1.3
10	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons) for Natural Persons for LRAO Purposes	SmartCard LORA Signature Certificate	-	-	1.3.171.1.**1.10.3.10**	0.4.0.1456.1.1
11	NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes	SmartCard LORA Authentication Certificate	-	-	1.3.171.1.**1.10.3.11**	0.4.0.2042.1.2
12	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) for Mass LRAO Signatures	Mass LRAO Signature Certificate	-	-	1.3.171.1.**1.10.3.12**	0.4.0.1456.1.2
13	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	eID SmartCard Signature Certificate	-	-	1.3.171.1.**1.10.3.13**	0.4.0.1456.1.1
14	NCP+ supporting Authentication & Encryption for Natural Persons	eID SmartCard Authentication Certificate	-	-	1.3.171.1.**1.10.3.14**	0.4.0.2042.1.2
15	NCP+ supporting Advanced Electronic Seal Signature Services	Seal Signature Services	-	-	1.3.171.1.**1.10.3.15**	0.4.0.1456.1.2
16	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration eID SmartCard Signature Certificate	-	-	1.3.171.1.**1.10.3.16**	0.4.0.2042.1.3
17	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration eID SmartCard Authentication Certificate	-	-	1.3.171.1.**1.10.3.17**	0.4.0.2042.1.3
18	Normalized Certificate Policy for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1.**1.10.3.18**	0.4.0.2042.1.2
19	Qualified Certificate Policy for for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1.**1.10.3.19**	0.4.0.194112.1.1
20	LuxTrust SPARE Signing Server LCP Certificate	LuxTrust SPARE Signing Server LCP Certificate	-	-	1.3.171.1.**1.10.3.20**	0.4.0.2042.1.3
21	LuxTrust Qualified eSEAL Certificate supporting digital signature	LuxTrust Qualified eSeal	-	-	1.3.171.1.**1.10.3.21**	0.4.0.194112.1.3
22	LuxTrust Advanced eSeal NCP+ Certificate for authentication	LuxTrust Qualified eSeal	-	-	1.3.171.1.**1.10.3.22**	0.4.0.2042.1.2

		23	LuxTrust Advanced eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1.**1.10.3.23**	0.4.0.2042.1.2
		24	LuxTrust Advanced eSEAL Certificate supporting authentication	LuxTrust Advanced eSeal	-	-	1.3.171.1.**1.10.3.24**	0.4.0.2042.1.2
		25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1.**1.10.3.25**	0.4.0.2042.1.2
		26	LuxTrust Smart Card QCP-n-qscd Certificate Profile	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1.**1.10.3.26**	0.4.0.194112.1.2
		27	LuxTrust Smart Card NCP+ Certificate Profile	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1.**1.10.3.27**	0.4.0.2042.1.2
		28	LuxTrust Smart Card LORA NCP+ - Signature Certificate for LRAO Purposes	SmartCard LORA Signature Certificate	-	-	1.3.171.1.**1.10.3.28**	0.4.0.2042.1.2
		29	LuxTrust Smart Card LORA NCP+ - authentication Certificate for LRAO Purposes	SmartCard LORA Authentication Certificate	-	-	1.3.171.1.**1.10.3.29**	0.4.0.2042.1.2
		30	LuxTrust eID Smart Card QCP-n-qscd Certificate	eID SmartCard Signature Certificate	-	-	1.3.171.1.**1.10.3.30**	0.4.0.194112.1.2
		31	LuxTrust eID Smart card NCP+ Certificate	eID SmartCard Authentication Certificate	-	-	1.3.171.1.**1.10.3.31**	0.4.0.2042.1.2
		32	LuxTrust Signing Server QCP-n-qscd Certificate	Signing Server certificate for qualified signature	-	-	1.3.171.1.**1.10.3.32**	0.4.0.194112.1.2
		33	LuxTrust Signing Server QCP-l-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1.**1.10.3.33**	0.4.0.194112.1.3
		34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171.**1.1.10.3.34**	0.4.0.194112.1.2
		35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171.**1.1.10.3.35**	0.4.0.2042.1.2
		36	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile			**1.3.171.1.1.10.3.36**	0.4.0.2042.1.3
	5 LuxTrust SSL CA Certificates	**1**	SSL/TLS Standard Server Certificates	SSL/TLS Standard Server Certificates	-	-	1.3.171.1.**1.10.5.1**	0.4.0.2042.1.3
		2	SSL/TLS(+) Extended Validation Server Certificates – EVCP	SSL/TLS Extended Validation Server Certificates	-	-	1.3.171.1.**1.10.5.2**	0.4.0.2042.1.4

			3	SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	**-**	**-**	1.3.171.1.**1.10.5.3**	0.4.0.2042.1.5
			4	Object Signing(+) Certificates	Object Signing(+) Certificates	**-**	**-**	1.3.171.1.**1.10.5.4**	0.4.0.2042.1.3
			5	SSL/TLS Client Certificate	SSL/TLS Client Certificate	**-**	**-**	1.3.171.1.**1.10.5.5**	0.4.0.2042.1.3
			6	SSL/TLS QCP-w Extended Validation Server Certificates	SSL/TLS Qualified website authentication certificate	**-**	**-**	1.3.171.1.**1.10.5.6**	0.4.0.194112.1.4
		8 LuxTrust Global Timestamping CA Certificates	**1**	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate	**-**	**-**	1.3.171.1.**1.10.8.1**	0.4.0.2042.1.3

1.6LuxTrust Certification Authorities – Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

1.7LuxTrust Global Root CA

LuxTrust Global Root CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	X		SHA256 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time **+ 10;20 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). **20 years certificate requires a 4096 key length.**	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root x[1]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Root x[1]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies[2]	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier	CPSuri	X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE[6]		

[1] X is a sequential value to distinguish the old CA from the renewed CA. The value 1 is omitted as it is the first CA issued.

[2] Since LuxTrust Global Root 2

LuxTrust Global Root CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE[6]		
CA		X		TRUE	Fixed
pathLenConstraint		X		None	Fixed

1.8LuxTrust Global Qualified CA

LuxTrust Global Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	X		SHA256 with RSA Encryption	Fixed
SignatureValue		X		Issuing LTGRCA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time +**up to 20 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). **20 years certificate requires a 4096 key length.**	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root x[1]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA x[3]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		

[3] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Global Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
policyIdentifier		X		1.3.171.1.1.1.10.3	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier	CPSuri	X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE[6]		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
authorityInfoAccess[4]	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		x		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		x		http://ca.luxtrust.lu/LTGRCAx[17].crt	Fixed
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.luxtrust.lu/LTGRCAx[5].crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE[6]	N/A	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

1.8.1 LuxTrust SSL CA

LuxTrust SSL CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	X		SHA256 with RSA Encryption	Fixed
SignatureValue		X		Issuing LTGRCA Signature	
Validity					

[4] Since LuxTrust Global Qualified CA 3

[5] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued

[6] Criticality of this extension should be carefully considered with regards to the compliance with RFC 5280 stating in its section 4.2.1.10 that "*This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates".*

LuxTrust SSL CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time +**up to 20 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). **20 years certificate requires a 4096 key length.**	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root x[1]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust SSL CA x[7]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier (1)		X		1.3.171.1.1.1.10.5	Fixed
policyQualifiers (1)				N/a	
policyQualifierId (1)	{ id-qt-1 }	X		CPS	Fixed
Qualifier (1)		X		https://repository.luxtrust.lu	Fixed
policyIdentifier (2)	{ anyPolicy }	X		2.5.29.32.0	Fixed
policyQualifiers (2)				N/a	
policyQualifierId (2)					
Qualifier (2)					
KeyUsage	{id-ce 15}	X	TRUE[6]		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
authorityInfoAccess[8]	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		x		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		x		http://ca.luxtrust.lu/LTGRCAx[17].crt	Fixed
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					

[7] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

[8] Since LuxTrust SSL CA 4

LuxTrust SSL CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
FullName		X		http://crl.luxtrust.lu/LTGRCAx[1].crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE[6]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

1.8.2 LuxTrust TSA (Timestamping) CA

LuxTrust Global Timestamping CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	X		SHA256 with RSA Encryption	Fixed
SignatureValue		X		Issuing LTGRCA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time **+up to 20 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). **20 years certificate requires a 4096 key length.**	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root x[1]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA x[9]	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10.8	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE[6]		
keyCertSign				Set	Fixed
crlSign				Set	Fixed

[9] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Global Timestamping CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
authorityInfoAccess10	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		x		http://ltqroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		x		http://ca.luxtrust.lu/LTGRCAx[1].crt	Fixed
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.luxtrust.lu/LTGRCA[5].crl	Fixed
Basic Constraints	{id-ce 19}	X	TRUE[6]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

1.8.3 Certificate extensions

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

1.8.4 Algorithm object identifiers

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

1.8.5 Name forms

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

1.8.6 Name constraints

Name constraints are supported as per RFC 5280.

1.8.7 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

1.8.8 Usage of Policy Constraints extension

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

1.8.9 Policy qualifiers syntax and semantics

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

1.9LuxTrust End-entity – Certificates profiles

1.9.1 Certificate profiles

Under the new LuxTrust Global root and associated CAs, multiple types of certificates will be issued.

[10] Since LuxTrust Global Timestamping CA 2

For the purpose of integration with current devices such as the smartcard, the signing stick and signing server, the following five types of LuxTrust Certificates will be issued under the LuxTrust Global Qualified CA. They are respectively issued to three types of end-user devices according to the following:

- **LuxTrust SSCD Smartcards**: These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP+[11] Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy OID ***1.3.171.1.1.10.3.1***, and
  - One LuxTrust NCP+[12] certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID ***1.3.171.1.1.10.3.2***.

  Under eIDAs regulation, those profiles are updated to the following certificate policies:
  - LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID **1.3.171.1.1.10.3.26.**
  - LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID **1.3.171.1.1.10.3.27.**

- **LuxTrust non SSCD Signing Sticks**: These physical user devices that are not considered as SSCD according to [1] (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP[11] Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID ***1.3.171.1.1.10.3.3***, and
  - One LuxTrust NCP[12] certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID ***1.3.171.1.1.10.3.4***.

- **LuxTrust Signing Server Accounts (Virtual Smartcards)**: These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy
  - One LuxTrust NCP[12] certificate for Natural Persons for the combined purposes of electronic signature, data/entity authentication and encryption facilities, under the Certificate Policy OID ***1.3.171.1.1.10.3.5***.

- **LuxTrust eSeal Smart card-based certificates:** The eSeal smart card exists in two versions: advanced and qualified.

The qualified eSeal product is based on two certificate policies:

- LuxTrust Qualified eSeal Certificate Profile supporting digital signature under the Certificate Policy OID 1.3.171.1.1.10.3.21
- LuxTrust Advanced eSeal - Certificate Profile supporting authentication under the Certificate Policy OID 1.3.171.1.1.10.3.22

The advanced eSeal product is based on two certificate policies:

- LuxTrust Advanced eSeal - Certificate Profile supporting signature under the Certificate Policy OID **1.3.171.1.1.10.3.23.**
- LuxTrust Advanced eSeal - Certificate Profile supporting authentication under the Certificate Policy OID **1.3.171.1.1.10.3.24.**

For the purpose of enabling Web-based data communication conduits via the TLS/SSL protocols and for verifying the authenticity of executable code, the following types of LuxTrust Certificates will be issued under the LuxTrust SSL CA:

- **LuxTrust SSL/TLS Standard Server Certificates:** SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy ***1.3.171.1.1.10.5.1.***

- **LuxTrust SSL/TLS Extended Validation Server Certificates EVCP:** SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy ***1.3.171.1.1.10.5.2.***

- **LuxTrust SSL/TLS Extended Validation Server Certificates EVCP+:** SSL compliant ETSI TS 102 042 [4] Certificate generated on Secure User Device, under the Certificate OID Policy ***1.3.171.1.1.10.5.3.***

- **LuxTrust Object Signing (+) Certificates:** Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy ***1.3.171.1.1.10.5.4.***

- **LuxTrust SSL/TLS Client Certificates:** Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy ***1.3.171.1.1.10.5.5.***

1.9.2 Version number(s)

X.509 v3 is supported and used.

1.9.3 LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures

LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures are Qualified Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

[11] As defined by ETSI TS 101 456 (cf. [3]).

[12] As defined in ETSI TS 102 042 (cf. [4]).

These LuxTrust SSCD QCP+ Certificates are compliant with and include the OID reference of the QCP+ certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.1; cf. [3]).

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.1**>.

The following table provides the description of the fields for LuxTrust SSCD QCP+ Certificates.

LuxTrust SSCD QCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*

[13] IN = Included: Attribute / field included within the certificate profile.

[14] CE = Critical Extension.

[15] O/M: O = Optional, M = Mandatory.

[16] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[17] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust SSCD QCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only***: *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Support of Qualified Electronic Signature.
	PolicyIdentifier	✓				0.4.0.1456.1.1
QualifiedCertificateStat						
	QcCompliance	✓		M	S	0.4.0.1862.1.1
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	✓		M	D	0.4.0.1862.1.4

[18] SINCE LTGQCA3

1.9.4 LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption

LuxTrust SSCD NCP+ Certificates are Normalised Certificates issued on SSCD Hardware token such as LuxTrust Smartcard with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD NCP+ Certificates are compliant with and include the OID reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.1.10.3.2>**.

The following table provides the description of the fields for the LuxTrust SSCD NCP+ Certificate type supporting Authentication and Encryption.

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Data or Entity Authentication and Data Encryption.
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.5 LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures

LuxTrust non SSCD QCP Certificates are Qualified Certificates **not** issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust non SSCD QCP Certificates are compliant with and include the OID reference of the QCP certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.2; cf. [3]).

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate. These Certificates include the corresponding LuxTrust QCP OID, i.e., < **OID 1.3.171.1.1.10.3.3**>.

The following table provides the description of the fields for LuxTrust non SSCD QCP Certificates.

LuxTrust non SSCD QCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*

LuxTrust non SSCD QCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False

LuxTrust non SSCD QCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	✓				LuxTrust Qualified Certificate not on SSCD compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert
	PolicyIdentifier	✓				0.4.0.1456.1.2
QualifiedCertificateStat						
	QcCompliance	✓		M	S	*0.4.0.1862.1.1*
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	✓				**NOT SET**

1.9.6 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

LuxTrust non SSCD NCP Certificates are Normalised Certificates **not** issued on SSCD Hardware token with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust non SSCD NCP Certificates are compliant with and include the OID reference of the NCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.1; cf. [4]).

The usage purpose of these NCP Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust non SSCD NCP OID, i.e., **<OID 1.3.171.1.1.10.3.4>**.

The following table provides the description of the fields for the LuxTrust non SSCD NCP Authentication and Encryption Certificate type.

LuxTrust non SSCD NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*

LuxTrust non SSCD NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			

LuxTrust non SSCD NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.4
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Data or Entity Authentication and Data Encryption.
	PolicyIdentifier	✓				0.4.0.2042.1.1

1.9.7 *LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption*

LuxTrust Signing Server Account NCP Certificates are Normalised Certificates **not** issued on SSCD Hardware token with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust Signing Server Account NCP Certificates are compliant with and include the OID reference of the NCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.1; cf. [4]).

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption. These Certificates include the corresponding LuxTrust Signing Server Account NCP OID, i.e., **<OID 1.3.171.1.1.10.3.5>**.

The following table provides the description of the fields for the LuxTrust Signing Server Account NCP Signature, Authentication and Encryption Certificate type.

LuxTrust Signing Server NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.5" – if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.

LuxTrust Signing Server NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA[17].crl

LuxTrust Signing Server NCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.5
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Signature, Data or Entity Authentication and Data Encryption.
	PolicyIdentifier	✓				0.4.0.2042.1.1

1.9.8 LuxTrust NCP+ Certificates supporting Mass Signature Services

LuxTrust NCP+ Certificates for Advanced Mass Signature Services are Normalised Certificates certified as generated on Secure User Device, with creation of the keys by the Subscriber, with 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust Secure User Device NCP+ Certificates are compliant with and include the OID reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a normalised certificate for Mass Signature purposes. These Certificates include the corresponding LuxTrust NCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.6**>.

The following table provides the description of the fields for LuxTrust Secure User Device NCP+ Certificates.

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	*OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption*
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	commonName	✓		M	D	*Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped*
	countryName	✓		M	D	*Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)*
	stateOrProvinceName	✓		O	D	
	emailAddress	✓		O	D	*Subject's email address if available*
	organizationName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	localityName	✓		M	D	*Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)*
	organizationalUnitName 1	✓		O	D	*As provided by Subscriber*
	organizationalUnitName 2	✓		O	D	*As provided by Subscriber*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation				S	True
	keyEncipherment	✓			S	False

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: *Advanced electronic massive signature services.*
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.9 LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures

LuxTrust SSCD LCP+ Certificates supporting Qualified Signatures are Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD LCP+ Certificates are compliant with and include the OID reference of the LCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]).

The usage purpose of these LuxTrust SSCD LCP+ Certificates is limited to sole authorised usage of supporting the creation of Integration electronic signatures for system integration purposes with non-repudiation signatures. The LuxTrust SSCD LCP+ Certificates include the corresponding LuxTrust OID, i.e., < **OID 1.3.171.1.1.10.3.7**>.

The following table provides the description of the fields for LuxTrust SSCD LCP Certificates.

LuxTrust Integration Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s)*
	givenName	✓		M	D	***TEST ONLY*** **+ " " +** *As provided by Subscriber*
	surname	✓		M	D	*As provided by Subscriber*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*As provided by Subscriber*

LuxTrust Integration Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	Title	✓		M	D	***PRIVATE products:*** *Fixed value:* ***"Private Person"*** ***PRO products:*** ***"Professional Person"*** *(default) or* ***"Professional Administrator"***
	organizationName	✓		M	D	***PRO products only****: Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only****: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only****: Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*N/A*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.7
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.3

1.9.10 LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption

LuxTrust SSCD LCP+ Certificates are Normalised Certificates issued on SSCD Hardware token such as LuxTrust Smartcard with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD LCP+ Certificates are compliant with and include the OID reference of the LCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]).

The usage purpose of these LuxTrust SSCD LCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD LCP+ OID, i.e., **<OID 1.3.171.1.1.10.3.8>**.

The following table provides the description of the fields for the LuxTrust SSCD LCP+ Certificate type supporting Authentication and Encryption.

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***LGQCA XX SC PRI V3 (XX a number selected internally by LuxTrust)***
	givenName	✓		M	D	***LGQCA XX (XX a number selected internally by LuxTrust)***
	Surname	✓		M	D	***SC PRI V3***
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*N/A*
	Title	✓		M	D	***Private Person***
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*N/A*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.8
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on SSCD compliant with ETSI TS 102 042 LCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Authentication and Encryption for Integration Purposes.
	PolicyIdentifier	✓				0.4.0.2042.1.3

1.9.11 *LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes*

LuxTrust Signing Server LCP Certificates are Lightweight Certificates **not** issued on SSCD Hardware token with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]).

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption for integration only. These Certificates include the corresponding LuxTrust Signing Server Account OID, i.e., **<OID 1.3.171.1.1.10.3.9>**.

The following table provides the description of the fields for the LuxTrust Signing Server Account LCP Signature, Authentication and Encryption Certificate type.

LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.5" – if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	

LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***LGQCA XX CSS (XX a number selected internally by LuxTrust) or** Concatenation of given name(s) and surname(s) separated by a "Space" character.*
	givenName	✓		M	D	***LGQCA XX (XX a number selected internally by LuxTrust) or** Given name(s) as on ID document*
	Surname	✓		M	D	***CSS or** Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*LU or Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*N/A*
	Title	✓		M	D	***Private Person***
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*N/A*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.9

LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				INTEGRATION Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. **Sole Authorised Usage**: Signature, Data or Entity Auth. and Data Enc. for integration purposes
	PolicyIdentifier	✓				0.4.0.2042.1.3

1.9.12 LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes

LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures are Qualified Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD QCP+ Certificates are compliant with and include the OID reference of the QCP+ certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.1; cf. [3]).

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures for LRAO purposes. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.10**>.

The following table provides the description of the fields for LuxTrust SSCD LORA QCP+ Certificate Profile.

LuxTrust SSCD LORA QCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	*Given name(s) as on ID card*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***"LuxTrust RA Officer"***
	organizationName	✓		M	D	*Constructed by LuxTrust*

LuxTrust SSCD LORA QCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	localityName	✓		M	D	*Country of RA*
	organizationalUnitName 1	✓		M	D	*RA code Constructed by LuxTrust*
	organizationalUnitName 2	✓		M	D	*RAO code Constructed by LuxTrust*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.10
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Support of Qualified Electronic Signature for LRAO purposes
	PolicyIdentifier	✓				0.4.0.1456.1.1
QualifiedCertificateStat						
	QcCompliance	✓		M	S	*0.4.0.1862.1.1*
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	✓		M	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

1.9.13 LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes

LuxTrust SSCD NCP+ Certificates are Normalised Certificates issued on SSCD Hardware token such as LuxTrust Smartcard with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD NCP+ Certificates are compliant with and include the OID reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption for LRAO purposes. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.1.10.3.11>**.

The following table provides the description of the fields for the LuxTrust SSCD LORA NCP+ Certificate Profile type supporting Authentication and Encryption.

LuxTrust SSCD LORA NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	*Given name(s) as on ID card*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***"LuxTrust RA Officer"***
	organizationName	✓		M	D	*Constructed by LuxTrust*
	localityName	✓		M	D	*Country of RA*
	organizationalUnitName 1	✓		M	D	*RA code Constructed by LuxTrust*
	organizationalUnitName 2	✓		M	D	*RAO code Constructed by LuxTrust*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			

LuxTrust SSCD LORA NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.11
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Data or Entity Authentication and Data Encryption for LRAO purposes.
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.14 LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures

LuxTrust non SSCD QCP Certificates are Qualified Certificates **not** issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust non SSCD QCP Certificates are compliant with and include the OID reference of the QCP certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.2; cf. [3]).

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate for Mass LRAO Signature purposes. These Certificates include the corresponding LuxTrust QCP OID, i.e., < **OID 1.3.171.1.1.10.3.12**>.

The following table provides the description of the fields for LuxTrust non SSCD QCP Certificates.

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	*Given name(s) as on ID card*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	*"LuxTrust RA officer – LRS"*
	organizationName	✓		M	D	*"RA" & RA number & " – " & Name of the LuxTrust RA*
	localityName	✓		M	D	*Country of RA (as in articles of association)*
	organizationalUnitName 1	✓		M	D	*RA code Constructed by LuxTrust*
	organizationalUnitName 2	✓		O	D	*RAO code Constructed by LuxTrust*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the **LuxTrust Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.12
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate not SSCD compliant with ETSI TS101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Support of Advanced Electronic Signature for Mass LRAO purposes
	PolicyIdentifier	✓				0.4.0.1456.1.2
QualifiedCertificateStat						
	QcCompliance	✓		M	S	*0.4.0.1862.1.1*
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	✓				**NOT SET**

1.9.15 LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures

LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures are Qualified Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the eID certificate life cycle procedure, with a 2048-bit key size and 61 months validity from issuing start date or 1 day validity from issuing start date for pseudonym certificate

These LuxTrust SSCD QCP+ Certificates are compliant with and include the OID reference of the QCP+ certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.1; cf. [3]).

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.13**>.

According to the Luxembourg legislation, the eID card must always contain certificates. When ordering an eID card, the citizen has the choice to request or not the activation of his certificates. In case he has chosen not to activate his certificates, LuxTrust is not allowed to detain the personal citizen data according to the personal data protection and management of the national register law. Therefore, when a citizen does not want to activate and use his certificates:

1. Pseudonym certificates are issued due to the laws on data protection and national register
2. The Given name and the Surname are encrypted alphanumeric strings
3. The pseudonym certificates are immediately revoked as the citizen will not use his certificates

The certificate re-key is not allowed.

The following table provides the description of the fields for LuxTrust SSCD QCP+ Certificates.

LuxTrust eID SSCD QCP+ Certificate Profile						
Attribute	**Field**	**IN**[19]	**CE**[20]	**O/M**[21]	**CO**[22]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[23]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **maximum 120** Months; Certificate generation process date/time + 1 day **for PSEUDONYM Certificate**
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*Given name(s) as on ID card or as provided by the RNCID*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***"Private Person"***
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						

[19] IN = Included: Attribute / field included within the certificate profile.

[20] CE = Critical Extension.

[21] O/M: O = Optional, M = Mandatory.

[22] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[23] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust eID SSCD QCP+ Certificate Profile						
Attribute	**Field**	**IN**[19]	**CE**[20]	**O/M**[21]	**CO**[22]	**Value**
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.13
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Support of Qualified Electronic Signature.
	PolicyIdentifier	✓				0.4.0.1456.1.1
QualifiedCertificateStat						
	QcCompliance	✓		M	S	*0.4.0.1862.1.1*
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	✓		M	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

1.9.16 LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption

LuxTrust SSCD NCP+ Certificates are Normalised Certificates issued on SSCD Hardware with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the eID certificate life cycle procedure, with a 2048-bit key size and 61 months validity from issuing start date or 1 day validity from issuing start date for pseudonym certificate.

These LuxTrust SSCD NCP+ Certificates are compliant with and include the OID reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.1.10.3.14>**.

According to the Luxembourg legislation, the eID card must always contain certificates. When ordering an eID card, the citizen has the choice to request or not the activation of his certificates. In case he has chosen not to activate his certificates, LuxTrust is not allowed to detain the personal citizen data according to the personal data protection and management of the national register law. Therefore, when a citizen does not want to activate and use his certificates:

1. Pseudonym certificates are issued due to the laws on data protection and national register

2. The Given name and the Surname are encrypted alphanumeric strings
3. The pseudonym certificates are immediately revoked as the citizen will not use his certificates

The certificate re-key is not allowed.

The following table provides the description of the fields for the LuxTrust SSCD NCP+ Certificate type supporting Authentication and Encryption.

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **maximum 120** Months; Certificate generation process date/time + 1 day **for PSEUDONYM Certificate**
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*Given name(s) as on ID card or as provided by the RNCID*
	surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***"Private Person"***
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.14
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Data or Entity Authentication and Data Encryption.
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.17 LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures

LuxTrust eID SSCD LCP+ Certificates are Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the eID certificate life cycle procedure, with a 2048-bit key size and 12 months validity from issuing start date or 1 day validity from issuing start date for pseudonym certificate.

These LuxTrust SSCD LCP+ Certificates are compliant with and include the OID reference of the LCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]).

The usage purpose of these LuxTrust SSCD LCP+ Certificates is limited to sole authorised usage of supporting the creation of Integration electronic signatures for system integration purposes with non-repudiation signatures. The LuxTrust SSCD LCP+ Certificates include the corresponding LuxTrust LCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.16**>.

According to the Luxembourg legislation, the eID card must always contain certificates. When ordering an eID card, the citizen has the choice to request or not the activation of his certificates. In case he has chosen not to activate his certificates, LuxTrust is not allowed to detain the personal citizen data according to the personal data protection and management of the national register law. Therefore, when a citizen does not want to activate and use his certificates:

1. Pseudonym certificates are issued due to the laws on data protection and national register
2. The Given name and the Surname are encrypted alphanumeric strings
3. The pseudonym certificates are immediately revoked as the citizen will not use his certificates

The certificate re-key is not allowed.
The following table provides the description of the fields for LuxTrust SSCD LCP+ Certificates.

LuxTrust eID SSCD LCP Integration Signature Certificate Profile						
Attribute	**Field**	**IN**[24]	**CE**[25]	**O/M**[26]	**CO**[27]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[28]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12** Months; Certificate generation process date/time + 1 day **for PSEUDONYM Certificate**
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*specimen-x provided by the RNCID*
	surname	✓		M	D	*specimen-x as provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*specimen-x Subject's email address as provided by the RNCID*
	title	✓		M	D	***"Private Person"***
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			

[24] IN = Included: Attribute / field included within the certificate profile.

[25] CE = Critical Extension.

[26] O/M: O = Optional, M = Mandatory.

[27] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

28 X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust eID SSCD LCP Integration Signature Certificate Profile						
Attribute	**Field**	**IN**[24]	**CE**[25]	**O/M**[26]	**CO**[27]	**Value**
	Rfc822Name	✓		O	D	*specimen-x Subject's email address as provided by the RNCID*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.16
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Electronic signature for Integration Purposes.
	PolicyIdentifier	✓				0.4.0.1456.1.1
QualifiedCertificateStat						
	QcCompliance	✓		M	S	*0.4.0.1862.1.1*
	QcLimitValue			O	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			O	D	As provided by LuxTrust S.A. in compliance with [3]

1.9.18 LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption

LuxTrust SSCD LCP+ Certificates are Certificates issued on SSCD Hardware with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the eID certificate life cycle procedure, with a 2048-bit key size and 12 months validity from issuing start date or 1 day validity from issuing start date for pseudonym certificate.

These LuxTrust SSCD LCP+ Certificates are compliant with and include the OID reference of the LCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these LuxTrust SSCD LCP+ Certificates is for the combined purpose of authentication and encryption for system integration. These Certificates include the corresponding LuxTrust SSCD LCP+ OID, i.e., **<OID 1.3.171.1.1.10.3.17>**.

According to the Luxembourg legislation, the eID card must always contain certificates. When ordering an eID card, the citizen has the choice to request or not the activation of his certificates. In case he has chosen not to activate his certificates, LuxTrust is not allowed to detain the personal citizen data according to the personal data protection and management of the national register law. Therefore, when a citizen does not want to activate and use his certificates:

1. Pseudonym certificates are issued due to the laws on data protection and national register
2. The Given name and the Surname are encrypted alphanumeric strings
3. The pseudonym certificates are immediately revoked as the citizen will not use his certificates

The certificate re-key is not allowed.

The following table provides the description of the fields for the LuxTrust SSCD LCP+ Certificate type supporting Authentication and Encryption.

LuxTrust eID SSCD LCP Integration AE Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"

LuxTrust eID SSCD LCP Integration AE Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12** Months; Certificate generation process date/time + 1 day **for PSEUDONYM Certificate**
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*specimen-x provided by the RNCID*
	surname	✓		M	D	*specimen-x provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*specimen-x Subject's email address as provided by the RNCID*
	title	✓		M	D	***"Private Person"***
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*specimen-x Subject's email address as provided by the RNCID*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True

LuxTrust eID SSCD LCP Integration AE Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.17
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Authentication and Encryption for Integration Purposes
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.19 LuxTrust NCP+ Certificates supporting SEAL Signature Services

LuxTrust NCP+ Certificates for Advanced Seal Signature Services are Normalised Certificates certified as generated on Secure User Device, with creation of the keys by the Subscriber and LuxTrust, with 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust Secure User Device NCP+ Certificates are compliant with and include the OID reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2; cf. [4]).

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a normalised certificate for Seal Signature purposes. These Certificates include the corresponding LuxTrust NCP+ OID, i.e., < **OID 1.3.171.1.1.10.3.15**>.

The following table provides the description of the fields for LuxTrust Secure User Device NCP+ Certificates.

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	*OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption*
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	commonName	✓		M	D	*Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped*

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	countryName	✓		M	D	*Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)*
	stateOrProvinceName	✓		O	D	
	emailAddress	✓		O	D	*Subject's email address if available*
	organizationName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	localityName	✓		M	D	*Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)*
	organizationalUnitName 1	✓		O	D	*As provided by Subscriber*
	organizationalUnitName 2	✓		O	D	*As provided by Subscriber*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.15
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	DisplayText	✓				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: *Advanced electronic seal signature services.*
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.20 LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption

LuxTrust SSL/TLS Standard Server Certificates are ETSI TS 102 042 LCP Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with 2048-bit key size and one (1), two (2) or three (3) years validity from issuing start date.

These LuxTrust SSL/TLS Standard Server Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.3).

The usage purpose of these LuxTrust SSL/TLS Standard Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding **LuxTrust LCP OID for SSL/TLS server certificates**, i.e., **<1.3.171.1.1.10.5.1>**.

The following table provides the description of the fields for LuxTrust Server Certificates.

LuxTrust SSL Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12;24;36** Months
subject		✓	False			
	countryName	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		O	D	
	localityName	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	✓		M	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName1	✓		O	D	As provided by Subscriber

LuxTrust SSL Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	organizationalUnitName2	✓		O	D	As provided by Subscriber
	commonName	✓		M	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or IP address or unique name of server.
	serialNumber	✓		O	D	Serial Number as provided by subscriber
	emailAddress	✓		O	D	Subject's email address
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu[29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.

[29] Since SSL CA 2

LuxTrust SSL Server LCP Certificate Profile						
Attribute	**Field**	**IN[13]**	**CE[14]**	**O/M[15]**	**CO[16]**	**Value**
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.5.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.2042.1.3

LuxTrust SSL Server LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	PolicyIdentifier					2.23.140.1.2.2
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	True

1.9.21 SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentication & Encryption

LuxTrust SSL/TLS Extended Validation Server Certificates (hereinafter EV SSL Certificates) are ETSI TS 102 042 EVCP Certificates, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or two (2) years validity from issuing start date.

These LuxTrust SSL/TLS Extended Validation Server Certificates are compliant with and include the OID reference of the EVCP certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.4).

The usage purpose of these LuxTrust SSL/TLS Extended Validation Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust EVCP Server Certificates include the corresponding **LuxTrust EVCP OID for SSL/TLS extended validation server certificates**, i.e., **<1.3.171.1.1.10.5.2>**.

Appropriate Certificate uses:
The primary purposes of these Certificates are to:

- **Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV SSL Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
- **Enable encrypted communications with a Web site:** Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of these Certificates are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV SSL Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
- Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

Prohibited Certificate uses:
The EV SSL Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, these Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EV SSL Certificate is actively engaged in doing business;
- That the Subject named in the EV SSL Certificate complies with applicable laws;
- That the Subject named in the EV SSL Certificate is trustworthy, honest, or reputable in its business dealings; or
- That it is “safe” to do business with the Subject named in the EV SSL Certificate.

Moreover, usages of EV SSL Certificates for other purposes than those identified in the present CP are prohibited.

Verification of Applicant’s Legal Existence and Identity:

For EV SSL Certificates, Applicant’s legal existence and identity are verified in compliance with the EV Guidelines [13]:

- For Private Organization Subjects:
  i. Verify the Applicant’s Legal Existence as stipulated in the EV Guidelines [13]);
  ii. Verify the Applicant’s Organization Name as stipulated in the EV Guidelines [13]);
  iii. Verify the Applicant’s Registration Number as stipulated in the EV Guidelines [13]);
  iv. Verify the Applicant’s Registered Agent as stipulated in the EV Guidelines [13]).
- For Government Entity Subjects:

i. Verify the Applicant's Legal Existence as stipulated in the EV Guidelines [13]);

ii. Verify the Applicant's Entity name as stipulated in the EV Guidelines [13]);

iii. Verify the Applicant's Registration Number as stipulated in the EV Guidelines [13]);

For EV SSL Certificates, LuxTrust SSL CA shall use a single naming convention as set forth in the EV Guidelines [13] and the Baseline Requirements [14] published by the CA/Browser Forum.

The following table provides the description of the fields for LuxTrust Server Certificates.

SSL/TLS Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12;24** Months
subject		✓	False			
	countryName **(OID: 2.5.4.6)**	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	jurisdictionCountryName **(OID: 1.3.6.1.4.1.311.60.2.1.3)**	✓		M	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName **(OID: 2.5.4.8)**	✓		M	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionStateOrProvinceName **(OID: 1.3.6.1.4.1.311.60.2.1.2)**	✓		O	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName **(2.5.4.7)**	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)

SSL/TLS Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	✓		O	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	✓		M	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	✓		M	D	Depending on the Subject qualifications, this field contains one of the following String: • Private Organization • Government Entity
	serialNumber (OID: 2.5.4.5)	✓		M	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	✓		O	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	✓		O	D	Number and Street of the physical location of the subject
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu [29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			

SSL/TLS Extended Validation Server Certificates						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	SubjectAltName-dNSName	✓		M		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates..
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyIdentifier		✓	False			

SSL/TLS Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.5.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.2042.1.4
	PolicyIdentifier	✓				2.23.140.1.1
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

1.9.22 SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Authentication & Encryption

LuxTrust SSL/TLS Extended Validation+ Server Certificates are ETSI TS 102 042 EVCP+ Certificates (hereinafter EVCP+ Certificates) certified as generated on Qualified Electronic Signature Creation Device, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or two (2) years validity from issuing start date.

These LuxTrust SSL/TLS Extended Validation+ Server Certificates are compliant with and include the OID reference of the EVCP+ certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.5).

The usage purpose of these LuxTrust SSL/TLS Extended Validation+ Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust EVCP+ Certificates include the corresponding **LuxTrust EVCP+ OID for SSL/TLS extended validation+ server certificates**, i.e., **<1.3.171.1.1.10.5.3>**.

Appropriate Certificate uses:
The primary purposes of these Certificates are to:

- **Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EVCP+ Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
- **Enable encrypted communications with a Web site:** Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of these Certificates are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EVCP+ Certificates may help to:

- Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
- Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
- Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

Prohibited Certificate uses:
The EVCP+ Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, these Certificates are not intended to provide any assurances, or otherwise represent or warrant:

- That the Subject named in the EVCP+ Certificate is actively engaged in doing business;
- That the Subject named in the EVCP+ Certificate complies with applicable laws;
- That the Subject named in the EVCP+ Certificate is trustworthy, honest, or reputable in its business dealings; or

- That it is "safe" to do business with the Subject named in the EVCP+ Certificate.

Moreover, usages of EVCP+ Certificates for other purposes than those identified in the present CP are prohibited.

Verification of Applicant's Legal Existence and Identity:

For EVCP+ Certificates, Applicant's legal existence and identity are verified in compliance with the EV Guidelines [13]:

- For Private Organization Subjects:
  - v. Verify the Applicant's Legal Existence as stipulated in the EV Guidelines [13]);
  - vi. Verify the Applicant's Organization Name as stipulated in the EV Guidelines [13]);
  - vii. Verify the Applicant's Registration Number as stipulated in the EV Guidelines [13]);
  - viii. Verify the Applicant's Registered Agent as stipulated in the EV Guidelines [13]).
- For Government Entity Subjects:
  - iv. Verify the Applicant's Legal Existence as stipulated in the EV Guidelines [13]);
  - v. Verify the Applicant's Entity name as stipulated in the EV Guidelines [13]);
  - vi. Verify the Applicant's Registration Number as stipulated in the EV Guidelines [13]);

For EVCP+ Certificates, LuxTrust SSL CA shall use a single naming convention as set forth in the EV Guidelines [13] and the Baseline Requirements [14] published by the CA/Browser Forum.

Certificates generated according to this profile are anticipated for future usage.

The following table provides the description of the fields for LuxTrust Server Certificates.

SSL/TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12;24** Months
Subject		✓	False			
	countryName **(OID: 2.5.4.6)**	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)

SSL/TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	✓		M	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	✓		M	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	✓		O	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName (2.5.4.7)	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	✓		O	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	✓		M	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein
	businessCategory (OID: 2.5.4.15)	✓		M	D	Depending on the Subject qualifications, this field contains one of the following String: • Private Organization • Government Entity

SSL/TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	serialNumber **(OID: 2.5.4.5)**	✓		M	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode **(OID: 2.5.4.17)**	✓		O	D	Postal code of the subject place of business.
	streetAddress **(OID: 2.5.4.9)**	✓		O	D	Number and Street of the physical location of the subject
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu[29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	SubjectAltName-dNSName	✓		M		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.

SSL/TLS Extended Validation Server Certificates on Secure User Device						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).

SSL/TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.5.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.2042.1.5
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

1.9.23 LuxTrust Object (or Code) Signing Certificates

LuxTrust Code Signing Certificates are ETSI TS 102 042 LCP Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with a 2048-bit key size and one (1), two (2) or three (3) years validity from issuing start date.

These LuxTrust Code Signing Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.3).

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., ***<1.3.171.1.1.10.5.4>.*** This profile is not currently implemented.

The following table provides the description of the fields for LuxTrust Code Signing Certificates.

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12; 24; 36** months

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Subject		✓	False			
	countryName	✓		M	D	*Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)*
	stateOrProvinceName	✓		O	D	
	localityName	✓		M	D	*Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)*
	organizationName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	organizationalUnitName1	✓		O	D	*As provided by Subscriber*
	organizationalUnitName2	✓		O	D	*As provided by Subscriber*
	commonName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	serialNumber	✓		O	D	*NA or Serial Number as provided by subscriber*
	emailAddress	✓		O	D	*Subject's email address if available*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				*Public Key: Key length: 2048 (RSA); public exponent: Fermat-4 (=010001).*
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu [29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
CRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	*The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).*
Policy Properties						

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN[13]**	**CE[14]**	**O/M[15]**	**CO[16]**	**Value**
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓			S	**1.3.171.1.1.10.5.4**
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	http://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on http://repository.luxtrust.lu. Signed by an SSL CA.
	PolicyIdentifier	✓			S	0.4.0.2042.1.3
Extended Key Usage		✓	False			
	Object Signing	✓			S	Set

1.9.24 LuxTrust SSL/TLS Certificate for Client Authentication

LuxTrust SSL/TLS Client Certificates are ETSI TS 102 042 LCP Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with 2048-bit key size and one (1), two (2) or three (3) years validity from issuing start date.

These LuxTrust SSL/TLS Client Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.3).

The usage purpose of these LuxTrust SSL/TLS Client Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding **LuxTrust LCP OID for SSL/TLS client certificates**, i.e., **<1.3.171.1.1.10.5.5>**.

The following table provides the description of the fields for LuxTrust Server Certificates.

LuxTrust SSL Client LCP Certificate Profile						
Attribute	**Field**	**IN[13]**	**CE[14]**	**O/M[15]**	**CO[16]**	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12; 24; 36** Months
Subject		✓	False			

LuxTrust SSL Client LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	countryName	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		O	D	
	localityName	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	✓		M	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	✓		O	D	As provided by Subscriber
	organizationalUnitName 2	✓		O	D	As provided by Subscriber
	commonName	✓		M	D	As provided by Subscriber
	serialNumber	✓		O	D	Serial Number as provided by subscriber
	emailAddress	✓		O	D	Subject's email address
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu[29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.5.5
	policyQualifierID	✓			S	Id-qt-1 (CPS)

LuxTrust SSL Client LCP Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	Qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.2042.1.3
Extended Key Usage		✓	False			
	serverAuth	✓			S	False
	clientAuth	✓			S	True
	emailProtection	✓			S	True

1.9.25 SSL/TLS QCP-w Extended Validation Server Certificates

QCP-w: certificate policy for European Union (EU) qualified website authentication certificates, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key encryption as well as extended key usage for server and client authentication. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.5.6>.

SSL/TLS QCP-w Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **SSL** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12;24** Months
subject		✓	False			
	countryName **(OID: 2.5.4.6)**	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	jurisdictionCountryName **(OID: 1.3.6.1.4.1.311.60.2.1.3)**	✓		M	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName **(OID: 2.5.4.8)**	✓		M	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionStateOrProvinceName **(OID: 1.3.6.1.4.1.311.60.2.1.2)**	✓		O	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName **(2.5.4.7)**	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)

SSL/TLS QCP-w Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	✓		O	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	✓		M	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	✓		M	D	Depending on the Subject qualifications, this field contains one of the following String: • Private Organization • Government Entity
	serialNumber (OID: 2.5.4.5)	✓		M	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	✓		O	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	✓		O	D	Number and Street of the physical location of the subject
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu [29]
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx[17].crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx[17].crl
Subject Properties						
subjectAltName		✓	False			

SSL/TLS QCP-w Extended Validation Server Certificates						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	SubjectAltName-dNSName	✓		M		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates..
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyIdentifier		✓	False			

SSL/TLS QCP-w Extended Validation Server Certificates						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.5.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.194112.1.4
	PolicyIdentifier	✓				0.4.0.2042.1.4
	PolicyIdentifier	✓			S	2.23.140.1.1
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-web (0.4.0.1862.1.6.3)

1.9.26 LuxTrust SPARE Signing Server LCP Certificate Profile

LuxTrust Signing Server LCP Certificates are Lightweight Certificates **not** issued on QSCD with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 2048-bit key size and 3 years validity from issuing start date.
These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]).The usage purpose of these Certificates is only authentication <OID 1.3.171.1.1.10.3.20>.
The LuxTrust SPARE Signing Server LCP Certificate Profile include the corresponding SPARE Signing Server LCP Certificate, i.e., <1.3.171.1.1.10.3.20>.

SPARE LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[18]	**CE**[19]	**O/M**[20]	**CO**[21]	**Value**
Base Profile						
Version		☐	False			
					S	Version 3 Value = “2”
SerialNumber		☐	False			

SPARE LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[18]	**CE**[19]	**O/M**[20]	**CO**[21]	**Value**
					FDV	Validated on duplicates.
signatureAlgorithm			False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue			False			
					D	Issuing CA Signature.
Issuer			False		S	
	countryName				S	LU
	commonName				S	LuxTrust **Global Qualified** CA x
	organizationName				S	LuxTrust S.A.
Validity			False			
	NotBefore				D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time + **36** Months
Subject			False			
	serialNumber			M	D	*Serial Number as constructed by LRAO*
	commonName			M	D	***LGQCA XX CSS (XX a number selected internally by LuxTrust) or*** *Concatenation of given name(s) and surname(s) separated by a "Space" character.*
	givenName			M	D	***LGQCA XX (XX a number selected internally by LuxTrust) or*** *Given name(s) as on ID document*
	Surname			M	D	***CSS or*** *Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName			M	D	*LU or Nationality of holder (ISO3166)*
	emailAddress			O	D	*N/A*
	Title			M	D	***Private Person***
subjectPublicKeyInfo			False			
	Algorithm					Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey			M		
Extensions						

SPARE LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[18]	**CE**[19]	**O/M**[20]	**CO**[21]	**Value**
Authority Properties						
authorityKeyIdentifier		☐	False			
	keyIdentifier	☐				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		☐	False			
	AccessMethod	☐				Id-ad-2
	accessLocation	☐				http://ca.luxtrust.lu/LTGQCAx[22].crt
	AccessMethod	☐				Id-ad-1
	accessLocation	☐				http://qca.ocsp.luxtrust.lu/[23]
cRLDistributionPoint		☐	False			
	distributionPoint	☐			S	
	fullName	☐				http://crl.luxtrust.lu/LTGQCAx[22].crl
Subject Properties						
subjectAltName		☐	False			
	Rfc822Name	☐		O	D	*N/A*
subjectKeyIdentifier		☐	False			
	keyIdentifier	☐			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		☐	True			
	digitalSignature	☐			S	True
certificatePolicies		☐	False			
	PolicyIdentifier	☐				1.3.171.1.1.10.3.20
	policyQualifierID	☐			S	Id-qt-1 (CPS)
	Qualifier	☐			S	https://repository.luxtrust.lu
	PolicyIdentifier	☐				0.4.0.2042.1.3

1.9.27 LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature

LuxTrust Certificates for Qualified Seal Signature Services are Qualified Certificates certified as generated on Secure User Device, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date.

This profile aims at issuing qualified electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these

LuxTrust Qualified eSEAL Certificate Profile						
Attribute	**Field**	**IN**[30]	**CE**[31]	**O/M**[32]	**CO**[33]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[34]

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 [20] QCP-l-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < **OID 1.3.171.1.1.10.3.21**>.

The following table provides the description of the fields for LuxTrust Qualified Certificates for digital signature purpose.

[30] IN = Included: Attribute / field included within the certify
cate profile.

[31] CE = Critical Extension.

[32] O/M: O = Optional, M = Mandatory.

[33] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[34] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **24** Months
Subject		✓	False			
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier **(2.5.4.97)**	✓		M	D	Shall contain information using the following structure in the presented order: – 3 character legal person identity type reference; – 2 character ISO 3166 country code; – hyphen-minus "-" and – identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		O	D	Company/institution department or other information item
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[35]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	

[35] SINCE LTGQCA3

	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.21
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.194112.1.3
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

1.9.28 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

Keys are generated on Secure User Device, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. 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 1.3.171.1.1.10.3.22>.

LuxTrust NCP+ Certificate Profile for authentication						
Attribute	**Field**	**IN**[36]	**CE**[37]	**O/M**[38]	**CO**[39]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			

[36] IN = Included: Attribute / field included within the certify
cate profile.

[37] CE = Critical Extension.

[38] O/M: O = Optional, M = Mandatory.

[39] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[40]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **24** Months
Subject		✓	False			
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	✓		M	D	Shall contain information using the following structure in the presented order: – 3 character legal person identity type reference; – 2 character ISO 3166 country code; – hyphen-minus "-" and – identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		O	D	Company/institution department or other information item
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			

[40] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[41]
cRLDistributionPoint		✓	False			
LuxTrust Advanced eSEAL Certificate Profile						
Attribute	**Field**	**IN[42]**	**CE[43]**	**O/M[44]**	**CO[45]**	**Value**
Base Profile						
Version		✓	False			
	keyIdentifier	✓			Fixed S	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits). Version 3 Value = "2"
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.22
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.29 LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature

This profile aims at issuing advanced electronic eSeals. The usage purpose of these Certificates is limited to the creation of advanced eseals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Keys are generated on QSCD, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. These Certificates include the corresponding LuxTrust OID, i.e., **<** OID 1.3.171.1.1.10.3.23**>.**

[41] SINCE LTGQCA3

[42] IN = Included: Attribute / field included within the certify

cate profile.

[43] CE = Critical Extension.

[44] O/M: O = Optional, M = Mandatory.

[45] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[46]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **24** Months
Subject		✓	False			
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier **(2.5.4.97)**	✓		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		O	D	Company/institution department or other information item
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			

[46] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[47]
cRLDistributionPoint		✓	False			
LuxTrust Advanced eSEAL Certificate Profile						
Attribute	**Field**	**IN[48]**	**CE[49]**	**O/M[50]**	**CO[51]**	**Value**
Base Profile						
Version		✓	False			
	keyIdentifier	✓			Fixed S	The Key Identifier comprises a four-bit field with a 0100 value followed by the least significant 60 bits of the SHA-1 Hash of the value of subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits). Version 3 Value = "2"
SerialNumber		✓	False			
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.23
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.30 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

LuxTrust Certificates for Advanced Seal Signature Services are Advanced Certificates certified with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eseals supported by Advanced Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < **OID 1.3.171.1.1.10.3.24**>. The following table provides the description of the fields for LuxTrust Advanced Certificates for authentication purpose.

[47] SINCE LTGQCA3

[48] IN = Included: Attribute / field included within the certify cate profile.

[49] CE = Critical Extension.

[50] O/M: O = Optional, M = Mandatory.

[51] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[52]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **24** Months
Subject		✓	False			
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier **(2.5.4.97)**	✓		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		O	D	Company/institution department or other information item
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			

[52] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[53]
cRLDistributionPoint		✓	False			
LuxTrust Advanced Automated eSEAL Certificate Profile						
Attribute	**Field**	**IN[54]**	**CE[55]**	**O/M[56]**	**CO[57]**	**Value**
Base Profile						
Version		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.24
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.31 LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature

LuxTrust Certificates for Advanced Mass Seal Signature Services are Advanced Certificates certified as generated on HSM, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date.
LuxTrust Certificates for Advanced automated Seal Signature Services are Advanced Certificates compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy certified as generated on Hardware Security Module (HSM), with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. The following table provides the description of the fields for LuxTrust Advanced Mass eSeal for digital signature purpose.

[53] SINCE LTGQCA3

[54] IN = Included: Attribute / field included within the certify cate profile.

[55] CE = Critical Extension.

[56] O/M: O = Optional, M = Mandatory.

[57] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[58]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **24** Months
Subject		✓	False			
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier **(2.5.4.97)**	✓		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		O	D	Company/institution department or other information item
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key

[58] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[59]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.25
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.32 LuxTrust Smart Card QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.26>.

[59] SINCE LTGQCA3

LuxTrust Smart Card QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[60]	**CE**[61]	**O/M**[62]	**CO**[63]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[64]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		M	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., conditional (O) for PRIV prod.)	D	***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).*

[60] IN = Included: Attribute / field included within the certificate profile.

[61] CE = Critical Extension.

[62] O/M: O = Optional, M = Mandatory.

[63] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[64] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Smart Card QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[60]	**CE**[61]	**O/M**[62]	**CO**[63]	**Value**
	organizationalUnit Name 2	✓		O	D	***PRO products only***: *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[65]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.26
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.194112.1.2
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	*True*
	QcSSCD (0.4.0.1862.1.4)			M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-esign

[65] SINCE LTGQCA3

1.9.33 LuxTrust Smart Card NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.27>.

LuxTrust Smart Card NCP+ Certificate Profile						
Attribute	**Field**	**IN**[66]	**CE**[67]	**O/M**[68]	**CO**[69]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[70]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		M	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*

[66] IN = Included: Attribute / field included within the certificate profile.

[67] CE = Critical Extension.

[68] O/M: O = Optional, M = Mandatory.

[69] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[70] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Smart Card NCP+ Certificate Profile						
Attribute	**Field**	**IN** [66]	**CE** [67]	**O/M** [68]	**CO** [69]	**Value**
	organizationalUnit Name 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnit Name 2	✓		O	D	***PRO products only***: *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[71]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.27
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.34 LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature

[71] SINCE LTGQCA3

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 **NCP+** certificate policy, with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.

These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.28>.

LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	*Given name(s) as on ID card*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***"LuxTrust RA Officer"***
	organizationName	✓		M	D	*Constructed by LuxTrust*
	localityName	✓		M	D	*Country of RA*
	organizationalUnitName 1	✓		M	D	*RA code Constructed by LuxTrust*
	organizationalUnitName 2	✓		M	D	*RAO code Constructed by LuxTrust*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1

LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.28
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.35 *LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purposes*

LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.29>.

LuxTrust Smart Card LORA NCP+ - authentication Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	*Given name(s) as on ID card*

LuxTrust Smart Card LORA NCP+ - authentication Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	***"LuxTrust RA Officer"***
	organizationName	✓		M	D	*Constructed by LuxTrust*
	localityName	✓		M	D	*Country of RA*
	organizationalUnitName 1	✓		M	D	*RA code Constructed by LuxTrust*
	organizationalUnitName 2	✓		M	D	*RAO code Constructed by LuxTrust*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.29
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.36 QCP-n-qscd supporting Qualified Electronic Signature for eID smart cards

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to

the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.30>.

LuxTrust eID Smart Card QCP-n-qscd Certificate Profile						
Attribute	Field	IN[72]	CE[73]	O/M[74]	CO[75]	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x[76]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*Given name(s) as on ID card or as provided by the RNCID*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*Subject's email address*
	Title	✓		M	D	*"Private Person"*
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	

[72] IN = Included: Attribute / field included within the certificate profile.

[73] CE = Critical Extension.

[74] O/M: O = Optional, M = Mandatory.

[75] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

[76] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust eID Smart Card QCP-n-qscd Certificate Profile						
Attribute	Field	IN[72]	CE[73]	O/M[74]	CO[75]	Value
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.30
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.194112.1.2
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-esign

1.9.37 NCP+ supporting Authentication & Encryption for eID smart cards

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.31>.

LuxTrust eID Smart card NCP+ Certificate Profile						
Attribute	**Field**	**IN[77]**	**CE[78]**	**O/M[79]**	**CO[80]**	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	

[77] IN = Included: Attribute / field included within the certificate profile.

[78] CE = Critical Extension.

[79] O/M: O = Optional, M = Mandatory.

[80] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

LuxTrust eID Smart card NCP+ Certificate Profile						
Attribute	**Field**	**IN**[77]	**CE**[78]	**O/M**[79]	**CO**[80]	**Value**
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[81]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **maximum 120** Months; Certificate generation process date/time + 1 day **for PSEUDONYM Certificate**
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	*Concatenation of given name(s) and surname(s) separated by the space character*
	givenName	✓		M	D	*Given name(s) as on ID card or as provided by the RNCID*
	Surname	✓		M	D	*Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID*
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	Subject's email address
	Title	✓		M	D	***"Private Person"***
	organizationalUnitName 1	✓		O	D	*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA x public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False

[81] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust eID Smart card NCP+ Certificate Profile						
Attribute	**Field**	**IN**[77]	**CE**[78]	**O/M**[79]	**CO**[80]	**Value**
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.31
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.38 LuxTrust Signing Server QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by LuxTrust, up to 4096 bit key size and with a key usage that supports qualified electronic signature, entity authentication and data origin authentication with integrity and keyEncipherment. (This profile is on ongoing certification process).

LuxTrust Signing Server QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*

LuxTrust Signing Server QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., conditional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.32
	policyQualifierID	✓			S	Id-qt-1 (CPS)

LuxTrust Signing Server QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[1] [5]	**CO**[16]	**Value**
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.194112.1.2
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)

1.9.39 LuxTrust Signing Server QCP-l-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-l-qscd certificate policy with creation of the keys by LuxTrust, up to 4096 bit key size and with a key usage limited to the support of qualified electronic eSeals (This profile is on ongoing certification process).

LuxTrust Signing Server QCP-l-qscd Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12, 24, Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)

LuxTrust Signing Server QCP-l-qscd Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	organisationIdentifier **(2.5.4.97)**	✓		M	D	Shall contain information using the following structure in the presented order: – 3 character legal person identity type reference; – 2 character ISO 3166 country code; – hyphen-minus "-" and – identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName 1	✓		O	D	Company/institution department or other information item
	organizationalUnitName 2	✓		O	D	Company/institution department or other information item
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA[17].crl

LuxTrust Signing Server QCP-l-qscd Certificate Profile						
Attribute	**Field**	**IN[13]**	**CE[14]**	**O/M[15]**	**CO[16]**	**Value**
Subject Properties						
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.33
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	PolicyIdentifier	✓				0.4.0.194112.1.3
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

1.9.40 LuxTrust Signing Stick QCP-n-qscd certificate profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.34>.

LuxTrust Signing Stick QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN[82]**	**CE[83]**	**O/M[84]**	**CO[85]**	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU

[82] IN = Included: Attribute / field included within the certificate profile.

[83] CE = Critical Extension.

[84] O/M: O = Optional, M = Mandatory.

[85] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

LuxTrust Signing Stick QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[82]	**CE**[83]	**O/M**[84]	**CO**[85]	**Value**
	commonName	✓			S	LuxTrust **Global Qualified** CA x[86]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., condi-tional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[87]

[86] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Signing Stick QCP-n-qscd Certificate Profile						
Attribute	**Field**	**IN**[82]	**CE**[83]	**O/M**[84]	**CO**[85]	**Value**
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.34
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.194112.1.2
QualifiedCertificateStat		✓	False			
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcSSCD (0.4.0.1862.1.4)			M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-esign

1.9.41 LuxTrust Signing Stick NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.35>.

LuxTrust Signing Stick NCP+ Certificate Profile						
Attribute	**Field**	**IN**[88]	**CE**[89]	**O/M**[90]	**CO**[91]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			

[87] SINCE LTGQCA3

[88] IN = Included: Attribute / field included within the certificate profile.

[89] CE = Critical Extension.

[90] O/M: O = Optional, M = Mandatory.

[91] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

LuxTrust Signing Stick NCP+ Certificate Profile						
Attribute	**Field**	**IN** [88]	**CE** [89]	**O/M** [90]	**CO** [91]	**Value**
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x[92]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **36** Months
Subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.*
	givenName	✓		M	D	***PRO and PRIVATE products**: Given name(s) as on ID card*
	surname	✓		M	D	***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*
	countryName	✓		M	D	*Nationality of holder (ISO3166)*
	emailAddress	✓		O	D	*Subject's email address*
	title	✓		M	D	***PRIVATE products:*** *Fixed value: **"Private Person"*** ***PRO products:*** ***"Professional Person"** (default) or **"Professional Administrator"*** *(Other titles possible for special purpose certificates)*
	organizationName	✓		M	D	***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.*
	localityName	✓		M	D	***PRO products only**: Company/institution country of HQ (as in articles of association)*
	organizationalUnitName 1	✓		M for PRO prod., conditional (O) for PRIV prod.)	D	***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).*
	organizationalUnitName 2	✓		O	D	***PRO products only**:* *Company/institution department or other information item*
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						

[92] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Signing Stick NCP+ Certificate Profile						
Attribute	Field	IN[88]	CE[89]	O/M[90]	CO[91]	Value
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[93]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Certificate Holder's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.35
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.42 LuxTrust Signing Server Advanced Automated eSeal Certificate Profile

LuxTrust Lightweight Certificate Policy Certificate compliant with ETSI EN 319 411-1 LCPcertificate policy, with creation of the keys by the LuxTrust, 4096 -bit key size and two (2) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.36>.

Advanced eSeal - LCP Certificate Profile						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			

[93] SINCE LTGQCA3

Advanced eSeal - LCP Certificate Profile						
Attribute	**Field**	**IN[13]**	**CE[14]**	**O/M[15]**	**CO[16]**	**Value**
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12, **24** Months
subject		✓	False			
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)

Advanced eSeal - LCP Certificate Profile						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	organisationIdentifier (2.5.4.97)	✓		M	D	Shall contain information using the following structure in the presented order: – 3 character legal person identity type reference; – 2 character ISO 3166 country code; – hyphen-minus "-" and – identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 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. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName 1	✓		O	D	Company/institution department or other information item

Advanced eSeal - LCP Certificate Profile						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	organizationalUnitName 2	✓		O	D	Company/institution department or other information item
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Global Qualified** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/[18]
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA[17].crl
Subject Properties						
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.36
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu

Advanced eSeal - LCP Certificate Profile						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
	PolicyIdentifier	✓				0.4.0.2042.1.3

1.10 Timestamping Certificate Profile

LuxTrust Timestamping Certificates are issues by the LuxTrust Timestamping CA with keys located on HSM devices, with generation by LuxTrust CSP according to the processes and procedures described in the applicable CP, with a 2048-bit key size and 5 years validity from issuing start date.

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

LuxTrust Timestamping Certificate Profile						
Attribute	Field	IN[13]	CE[14]	O/M[15]	CO[16]	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Timestamping** CA x[17]
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		✓	False			
	commonName	✓		M	D	***tts.luxtrust.lu***
	localityName	✓		M	D	***Capellen***
	organizationName	✓		M	D	***LuxTrust S.A.***
	organizationalUnitName 1	✓		M	D	*PKI Entity*
	countryName	✓		O	D	*LU*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: **2048** bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **Timestamping** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGTSACAx[17].crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu

LuxTrust Timestamping Certificate Profile						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGTSACAx[17].crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*info@luxtrust.lu*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
Extended Key Usage		✓	False			
	TimeStamping (1.3.6.1.5.5.7.3.8)	✓			S	Set
Private Key Usage Period		✓	False			
	Usage period (2.5.29.16)	✓		M	D	Certificate generation process date/time + 12 Months
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.8.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust LCP certificate compliant with ETSI TS 102 042. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority.
	PolicyIdentifier	✓				0.4.0.2042.1.3

1.10.1 Normalized Certificate Policy for LuxTrust Qualified Timestamping

LuxTrust Qualified Timestamping Certificates are issued by the LuxTrust Qualified CA with keys located on HSM devices, with generation by LuxTrust CSP according to the processes and procedures described in the applicable CP, with a key size up to 4096 and 5 years validity from issuing start date.
The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 and RFC5816. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.
This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. 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 to the requirements of the standard ETSI EN 319 411-1 describing the Requirements for trust service providers issuing Extended Normalized Certificate Policy.

Normalized Certificate Policy for LuxTrust Qualified Timestamping						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	

Normalized Certificate Policy for LuxTrust Qualified Timestamping						
Attribute	**Field**	**IN**[13]	**CE**[14]	**O/M**[15]	**CO**[16]	**Value**
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		✓	False			
	organisationIdentifier (2.5.4.97)	✓		M	D	VATLU-20976985
	commonName	✓		M	D	LuxTrust Qualified Timestamping
	organizationName	✓		M	D	***LuxTrust S.A.***
	countryName	✓		M	D	*LU*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: up to **4096** bit (RSA) public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*info@luxtrust.lu*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
Extended Key Usage		✓	True			
	TimeStamping (1.3.6.1.5.5.7.3.8)	✓			S	Set
Private Key Usage Period		✓	False			
	Usage period (2.5.29.16)	✓		M	D	Certificate generation process date/time + 12 Months
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.18
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.10.2 Qualified Timestamping Certificate Profile

LuxTrust Qualified Timestamping Certificates are issuesd by the LuxTrust Qualified CA with keys located on HSM devices, with generation by LuxTrust CSP according to the processes and procedures described in the applicable CP, with a key size up to 4096 and 5 years validity from issuing start date.
The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 and RFC5816. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [21] and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles [22].
This profile complies to the requirements of the standard ETSI EN 319 411-2 [20] describing the Requirements for trust service providers issuing EU qualified certificates.

Qualified Certificate Policy for for LuxTrust Qualified Timestamping						
Attribute	**Field**	**IN13**	**CE14**	**O/M15**	**CO16**	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = “1.2.840.113549.1.1.11” - SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		✓	False			
	organisationIdentifier (2.5.4.97)	✓		M	D	VATLU-20976985
	commonName	✓		M	D	LuxTrust Qualified Timestamping
	organizationName	✓		M	D	LuxTrust S.A.
	countryName	✓		M	D	LU
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: up to 3072 bit (RSA) public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltName		✓	False			

Qualified Certificate Policy for for LuxTrust Qualified Timestamping						
Attribute	**Field**	**IN13**	**CE14**	**O/M15**	**CO16**	**Value**
	Rfc822Name	✓		O	D	info@luxtrust.lu
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
Extended Key Usage		✓	True			
	TimeStamping (1.3.6.1.5.5.7.3.8)	✓			S	Set
Private Key Usage Period		✓	False			
	Usage period (2.5.29.16)	✓		M	D	Certificate generation process date/time + 12 Months
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.19
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	PolicyIdentifier	✓				0.4.0.194112.1.1
certificatePolicies		✓				
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)
	QcCompliance (0.4.0.1862.1.1)	✓		M	S	True
	QcPDS (0.4.0.1862.1.5)	✓		M	S	https://www.luxtrust.lu/upload/data/repository/GTC_F_v2_4.pdf

1.10.3 TimeStamp Request and Response Format

1.10.3.1 TimeStamp Request Format

Time stamp requests sent to the CAs are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 3161 for detailed syntax. The following table lists the fields that are expected by the Time Stamping Services.

LuxTrust Time Stamp Request	
Field	**Value / comment**
Document Hash	Hash of the document on which the TimeStamp must be computed
Hash OID	(SHA-256/SHA-512) Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.
Policy OID	1.3.171.1.1.10.3.18.1 The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.

LuxTrust Time Stamp Request	
Field	**Value / comment**
Nonce	A random number, also referred to as “nonce”, allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.
Should TSA Certificate be included?	TRUE/FALSE
Request Extensions	**Value ***
None	None

*no extension is required to be supported

1.10.3.2 TimeStamp Response Format

See RFC 3161 for detailed syntax. The following table lists which fields are populated by the Time Stamping Services.

LuxTrust Time Stamp Response	
Field	**Value / comment**
Generation Time	The time at which the time-stamp token has been created by the TSA. It is expressed as UTC time (Coordinated Universal Time).
Document Hash	Hash of the document on which the TimeStamp response has been computed
Hash OID	(SHA-256/SHA-512) Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.
Serial Number	Serial Number of the current TSU certificate (unique, up to 160 bits)
Policy OID	1.3.171.1.1.10.3.18.1 / Qualified timestamp token 1.3.171.1.1.10.8.1.1 / Non-qualified timestamp token The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returnedtoken will include a policy identifier that is not defined by LuxTrust.
Nonce	A random number, also referred to as “nonce”, allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.
Accuracy	1 second
TSA Certificate Information	Current TSU Certificate
Request Extensions	**Value ***
None	None

*no extension is required to be generated, no extension shall be critical

1.11 Certificate extensions

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

1.12 Algorithm object identifiers

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

1.13 Name forms

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

1.14 Name constraints

Name constraints are supported as per RFC 5280.

1.15 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

1.16 Usage of Policy Constraints extension

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

1.17 Policy qualifiers syntax and semantics

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

1.18 Processing semantics for the critical Certificate Policies

Not applicable.

1.19 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 CRL Profile	
Field	**Comments**
Version	v2
Signature	Same signature algorithm as related CA
Issuer	<subjectCA>
thisUpdate	<creation time>
nextUpdate	<creation time + 100 days for Global Root CA> <creation time + 4,5 hours (4 hours and 30 minutes) for subordinate Qualified > <creation time + 8,5 hours (8 hours and 30 minutes) for subordinate SSL CAs> <creation time + 24 hours for other subordinate CAs>
revokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
reasonCode	<*Insert List of used revocation reason code*>
crlExtensions	
cRLNumber	Non-critical <subject key identifier CA>
authorityKeyIdentifier	Non-critical <CA assigned unique number>

1.19.1 Version number(s)

See section 3.4.

The CA will support X.509 version 2 CRLs, retrievable by online at http://crl.luxtrust.lu.

As an alternative to CRLs the CA may provide other web based or "other" revocation checking service.

1.19.2 CRL entry extensions

See section 3.4.

1.20 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 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.

1.20.1 Version number(s)

See section 3.5.

1.20.2 OCSP extensions

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

LuxTrust OCSP Certificate Profile						
Attribute	**Field**	IN18	CE19	O/M20	CO21	Value
Base Profile						
Version		☐	False			
					S	Version 3 Value = "2"
SerialNumber		☐	False			
					FDV	Validated on duplicates.
signatureAlgorithm		☐	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue		☐	False			
					D	Issuing LTGRCA Signature
issuer		☐	False		S	
	countryName	☐			S	LU
	commonName	☐			S	LuxTrust Global Root x
	organizationName	☐			S	LuxTrust S.A.
Validity		☐	False			
	NotBefore	☐			D	Certificate generation process date/time.
	NotAfter	☐			D	Certificate generation process date/time + maximum 12 Months
subject		☐	False			
	countryName	☐		M	D	LU
	organizationName	☐		M	D	LuxTrust S.A.
	organizationalUnitName 1	☐		O	D	Pki entity
	commonName	☐		M	D	LuxTrust S.A. OCSP Server 2
subjectPublicKeyInfo		☐	False			
	algorithm	☐				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	☐		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		☐	False			
	keyIdentifier	☐				SHA-1 Hash of the LuxTrust LTGR x CA public key
id-ocsp-nocheck		☐	False			
		☐			S	NULL
Subject Properties						
subjectKeyIdentifier		☐	False			

LuxTrust OCSP Certificate Profile						
Attribute	**Field**	IN18	CE19	O/M20	CO21	Value
	keyIdentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
	nonRepudiation				S	False
	keyEncipherment				S	False
	dataEncipherment				S	False
certificatePolicies			False			
	PolicyIdentifier					1.3.171.1.1.1.1.0.1.0
	policyQualifierID				S	Id-qt-1 (CPS)
	qualifier				S	https://repository.luxtrust.lu
	policyQualifierID				S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText					LuxTrust S.A. Online Certificate Status Server. IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported.
	PolicyIdentifier					0.4.0.2042.1.3
Extended Key Usage			False			
	OCSPSigning				S	True