LuxTrust Global Root CA - Certificate specifications

Version number: 1.11

Publication Date: 21/09/2012

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	Application Providers
Document Classification	Confidential
Document Owner	YNU

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	CSB Board	20/09/2012	Typo update

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

Table of content

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

Intellectual Property Rights

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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] ICAO (International Civil Aviation Organization) – Machine Readable Travel Documents – Technical Report – PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, October 01, 2004

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

[7] 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.

[8] 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.

[9] 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.

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

[11] 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'accrédidation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[12] LuxTrust Time Stamping Policy. Document OID 1.3.171.1.1.3.1.0, latest version in force.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

1 INTRODUCTION

1.1 The LuxTrust project

The LuxTrust project was created in the form of a Trusted Third Party (hereafter also "TTP"), with an international reach, aiming to establish a national expertise centre 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 [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.

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;
- 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.

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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

2 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.

2.1 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, cross signed 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

- Cross-signed LuxTrust subordinate CAs. Each of these CAs is root-signed by the LuxTrust Root CA. Currently, the following CAs are foreseen:
    - LuxTrust Qualified CA
    - LuxTrust Privacy+ CA
    - LuxTrust SSL and EV CA
    - LuxTrust TEST CA
    - LuxTrust Internal CA
    - LuxTrust Time Stamping Authority
    - LuxTrust eGovernment CA

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

Cross-signed 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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

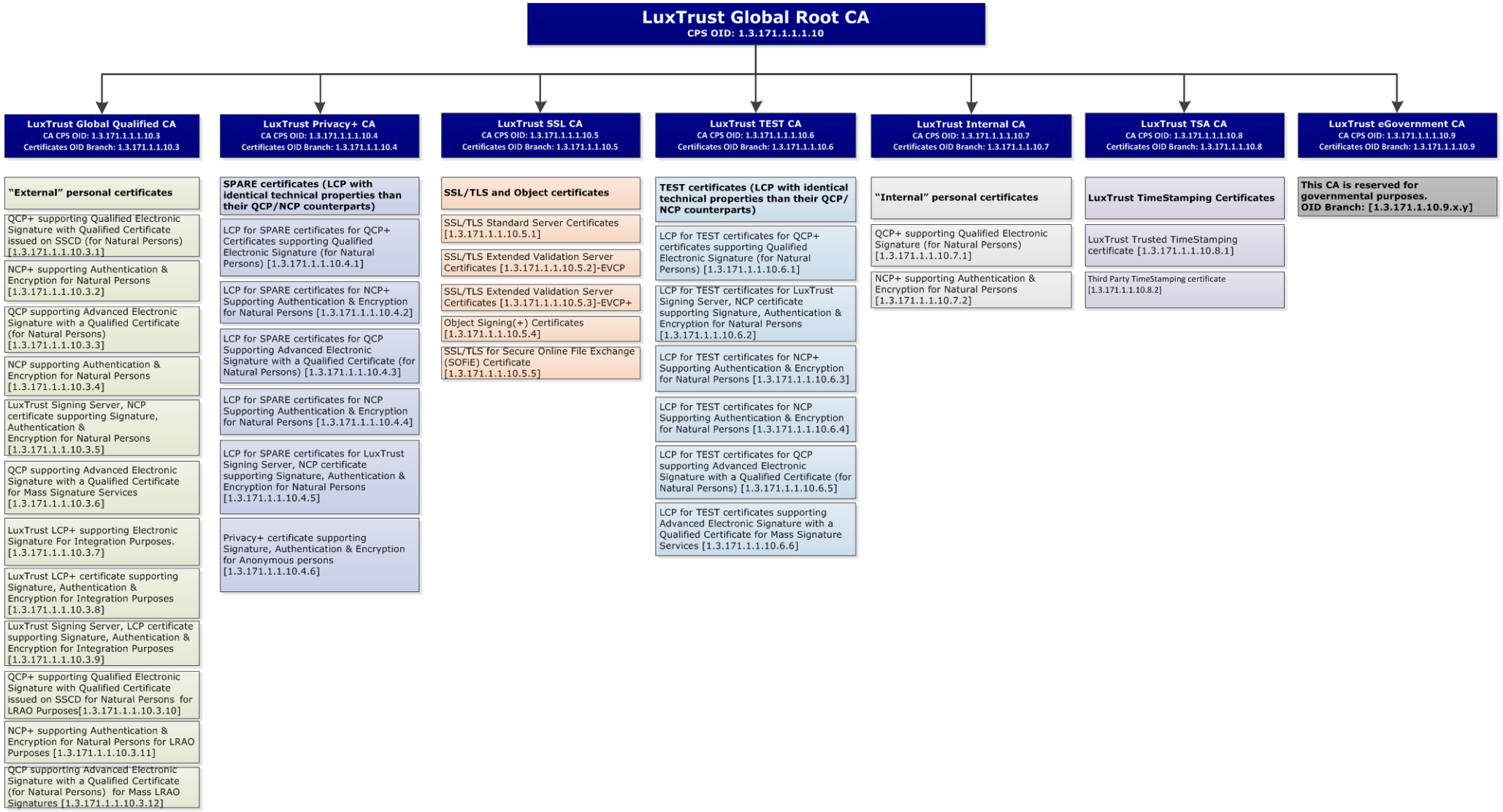

Figure 1 - LuxTrust CA Hierarchy

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

3 CERTIFICATE AND CRL PROFILES

3.1 Certificate types

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

CP identification	CP OID	Document OID	Short Description	Ref.[1]
LuxTrust Qualified Certification Authority				
QCP+ supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.1**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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. The CP accreditation by ILNAS is in progress.	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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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. The CP accreditation by ILNAS is in progress.	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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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

[1] If this field is empty, the corresponding CP will be later defined.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
NCP supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.4**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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
QCP supporting Advanced Electronic Signature with a Qualified Certificate for Mass Signature Services **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.6**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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 Signature Services.	
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.7**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.8**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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 Account 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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes **issued by LuxTrust Global Qualified CA**	**1.3.171.1.1.10.3.11**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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**	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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
LuxTrust Privacy+ Certification Authority				
LCP for SPARE certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.1**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	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 SPARE purposes of QCP+ signature certificates.	
LCP for SPARE certificates for NCP+ supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.2**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	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 SPARE purposes of NCP+ authentication and encryption certificates.	

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
LCP for SPARE certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.3**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant 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 SPARE purposes of QCP signature certificates.	
LCP for SPARE certificates for NCP supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.4**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant 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 for SPARE purposes of NCP authentication and encryption certificates.	
LCP for SPARE certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.5**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a **non** SSCD centralised 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 SPARE purposes of NCP authentication, encryption and signature certificates.	
Privacy+ certificate supporting Signature, Authentication & Encryption for Anonymous persons **issued by LuxTrust Privacy+ CA**	**1.3.171.1.1.10.4.6**	1.3.171.1.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a **non** 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 signature, authentication purpose and/or key & data encryption for authentication, encryption and signature certificates.	
LuxTrust SSL Certification Authority				

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
SSL/TLS(+) Standard Server Certificates **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.1**	1.3.171.1.1.1.10.2.5 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SCD, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) 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
SSL/TLS(+) Extended Validation Server Certificates - EVCP **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.2**	1.3.171.1.1.1.10.2.5 .x(version) .y(sub-version)	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**	1.3.171.1.1.1.10.2.5 .x(version) .y(sub-version)	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**	1.3.171.1.1.1.10.2.5 .x(version) .y(sub-version)	ETSI TS 102 042 **LCP** compliant certificate, on SCD, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption.	LuxTrust Object (or code) Signing Certificates

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
SSL/TLS for Secure Online File Exchange (SOFiE) Certificate **issued by LuxTrust SSL CA**	**1.3.171.1.1.10.5.5**	1.3.171.1.1.1.10.2.5 .x(version) .y(sub-version)	ETSI TS 102 042 **LCP** compliant certificate, on SCD, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) 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 TEST Certification Authority				
LCP for TEST certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.1**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	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 TEST purposes of QCP+ signature certificates.	
LCP for TEST certificates for NCP+ supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.2**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	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 authentication purpose (to the exclusion of electronic signature) and key & data encryption for TEST purposes of NCP+ authentication and encryption certificates.	
LCP for TEST certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.3**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant 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 TEST purposes of QCP signature certificates.	

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
LCP for TEST certificates for NCP supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.4**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant 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 for TEST purposes of NCP authentication and encryption certificates.	
LCP for TEST certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.5**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a **non** SSCD centralised hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity or validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for TEST purposes of NCP authentication, encryption and signature certificates.	
LCP for TEST certificates supporting Advanced Electronic Signature with a Qualified Certificate for Mass Signature Services **issued by LuxTrust Test CA**	**1.3.171.1.1.10.6.6**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	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 Signature Services.	
LuxTrust Internal Certification Authority				
QCP+ supporting Qualified Electronic Signature (for Natural Persons) **issued by LuxTrust Internal CA**	**1.3.171.1.1.10.7.1**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)		

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

CP identification	CP OID	Document OID	Short Description	Ref.[1]
NCP+ supporting Authentication & Encryption for Natural Persons **issued by LuxTrust Internal CA**	**1.3.171.1.1.10.7.2**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)		
LuxTrust TSA (Timestamping) Certification Authority				
LuxTrust Trusted TimeStamping certificate **issued by LuxTrust TSA CA**	**1.3.171.1.1.10.8.1**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	LuxTrust certificate compliant with ETSI TS 102 023. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority. The CP accreditation by ILNAS is in progress.	Timestamping Certificate Profile
Third Party TimeStamping certificate **issued by LuxTrust TSA CA**	**1.3.171.1.1.10.8.2**	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)		

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 [12].

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 [1]. LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy [12].

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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust S.A. OID : 1.3.171.1			**ETSI OIDs**	**QCP+**		**0.4.0.1456.1.1**
LuxTrust PKI: 1.3.171.1.1			***for info***	**QCP**		**0.4.0.1456.1.2**
				NCP		**0.4.0.2042.1.1**
				NCP+		**0.4.0.2042.1.2**
				LCP		**0.4.0.2042.1.3**

Document category	Document		Sub-document - description	LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
LuxTrust Certification Practice Statements								
1 CPS LuxTrust	**1** CPS Summary		**0** (master)		**x**	**y**	1.3.171.1.1.**1.1.0.x.y**	N/A
								N/A
	2 Full CPS GTE Chain	**0**	**Not Used**		N/A	N/A	not used	N/A
		1	**First document**		**x**	**y**	1.3.171.1.1.**1.2.1.x.y**	N/A
		2	**Second document**		**x**	**y**	1.3.171.1.1.**1.2.2.x.y**	N/A
		3	**Third document**		**x**	**y**	1.3.171.1.1.**1.2.3.x.y**	N/A
		4	**Fourth document**		**x**	**y**	1.3.171.1.1.**1.2.4.x.y**	N/A
			etc.		**x**	**y**	1.3.171.1.1.**1.2.5.x.y**	N/A
	10 CPS LuxTrust Global Root	**0**	**0 Reserved**		**N/A**			N/A
		1	**Reserved**		**N/A**			N/A
		2	**LuxTrust Global Root CA**		**x**	**y**	1.3.171.1.1.**1.10.2.x.y**	N/A
		3	**LuxTrust Global Qualified CA**		**x**	**y**	1.3.171.1.1.**1.10.3.x.y**	N/A
		4	**LuxTrust Privacy+ CA**		**x**	**y**	1.3.171.1.1.**1.10.4.x.y**	N/A
		5	**LuxTrust SSL CA**		**x**	**y**	1.3.171.1.1.**1.10.5.x.y**	N/A
		6	**LuxTrust TEST CA**		**x**	**y**	1.3.171.1.1.**1.10.6.x.y**	N/A
		7	**LuxTrust Internal CA**		**x**	**y**	1.3.171.1.1.**1.10.7.x.y**	N/A
		8	**LuxTrust Global Timestamping CA**		**x**	**y**	1.3.171.1.1.**1.10.8.x.y**	N/A
		9	**LuxTrust eGovernment CA**		**x**	**y**	1.3.171.1.1.**1.10.9.x.y**	N/A
LuxTrust Certificate Policies								
10 CP's LuxTrust Global	**1 Reserved**							N/A
	2 Reserved							N/A

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

Document category	Document	Sub-document - description		LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
Chain	**3** LuxTrust Global Qualified CA Certificates issued to Natural Persons	**0**	**Master document**	**N/A**	**x**	**y**	1.3.171.1.1.10.**3.0.x.y**	N/A
		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	QCP supporting AdES with a qualified certificate 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	SmartCard LORA	-	-	1.3.171.1.1.10.**3.10**	0.4.0.1456.1.1

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

Document category	Document	Sub-document - description		LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
			Natural Persons) for Natural Persons for LRAO Purposes	Signature Certificate				
		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 [1.3.171.1.1.10.3.12]	Mass LRAO Signature Certificate	-	-	1.3.171.1.1.10.**3.12**	0.4.0.1456.1.2
10 CP's LuxTrust Global Chain	**4** LuxTrust Privacy+ CA	**0**	Master document		**x**	**y**	1.3.171.1.1.10.**4.0.x.y**	N/A
		1	LCP for SPARE certificates for QCP+ Certificates supporting Qualified Electronic Signature (for Natural Persons)	SmartCard SPARE Signature certificate	-	-	1.3.171.1.1.**10.4.1**	0.4.0.2042.1.3
		2	LCP for SPARE certificates for NCP+ Supporting Authentication & Encryption for Natural Persons	SmartCard SPARE Authentication Certificate	-	-	1.3.171.1.1.**10.4.2**	0.4.0.2042.1.3
		3	LCP for SPARE certificates for QCP Supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick SPARE Signature Certificate	-	-	1.3.171.1.1.10.**4.3**	0.4.0.2042.1.3
		4	LCP for SPARE certificates for NCP Supporting Authentication & Encryption for Natural Persons	Signing Stick SPARE Authentication Certificate	-	-	1.3.171.1.1.**10.4.4**	0.4.0.2042.1.3
		5	LCP for SPARE certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons	Signing Server SPARE certificate	-	-	1.3.171.1.1.**10.4.5**	0.4.0.2042.1.3
		6	Privacy+ certificate supporting Signature, Authentication & Encryption for Anonymous persons	Signing Server Privacy+ Certificate	-	-	1.3.171.1.1.**10.4.6**	
	5	0	Master document	**N/A**	**x**	**y**	1.3.171.1.1.10.**5.0.x.y**	N/A

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

Document category	Document	Sub-document - description		LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
	LuxTrust SSL CA	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 for Secure Online File Exchange (SOFiE) Certificate	SOFiE Certificate			1.3.171.1.1.**10.5.4**	0.4.0.2042.1.3
	6 LuxTrust TEST CA	**0**	**Master document**	**N/A**	**x**	**y**	1.3.171.1.1.**10.6.0**	N/A
		1	LCP for TEST certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons)		-	-	1.3.171.1.1.**10.6.1**	0.4.0.2042.1.3
		2	LCP for TEST certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons		-	-	1.3.171.1.1.**10.6.2**	0.4.0.2042.1.3
		3	LCP for TEST certificates for NCP+ Supporting Authentication & Encryption for Natural Persons		-	-	1.3.171.1.1.**10.6.3**	0.4.0.2042.1.3
		4	LCP for TEST certificates for NCP Supporting Authentication & Encryption for Natural Persons		-	-	1.3.171.1.1.**10.6.4**	0.4.0.2042.1.3
		5	LCP for TEST certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)		-	-	1.3.171.1.1.**10.6.5**	0.4.0.2042.1.3
		6	LCP for TEST certificates supporting Advanced Electronic Signature with a Qualified Certificate		-	-	1.3.171.1.1.**10.6.6**	0.4.0.2042.1.3

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

Document category	Document	Sub-document - description		LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
			for Mass Signature Services					
	7 LuxTrust Internal CA	**0**	**Master document**	N/A	**x**	**y**	1.3.171.1.1.**10.7.0**	N/A
		1	QCP+ supporting Qualified Electronic Signature (for Natural Persons)	RA SmartCard Signature certificate	**-**	**-**	1.3.171.1.1.**10.7.1**	0.4.0.1456.1.2
		2	NCP+ supporting Authentication & Encryption for Natural Persons	RA SmartCard Authentication certificate	**-**	**-**	1.3.171.1.1.**10.7.2**	0.4.0.2042.1.2
	8 LuxTrust Global Timestamping CA	**0**	**Master document**	N/A			1.3.171.1.1.**10.8.0**	N/A
		1	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate			1.3.171.1.1.**10.8.1**	
		2	Third Party TimeStamping certificate	Third Party TimeStamping certificate			1.3.171.1.1.**10.8.2**	
	8 LuxTrust eGovernment CA	**0**	**Master document**	N/A			1.3.171.1.1.**10.9.0**	N/A
		Reserved for future use						

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu

www.luxtrust.lu

3.2 LuxTrust Certification Authorities – Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

3.2.1 LuxTrust 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 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
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		
CA		X		TRUE	Fixed

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Global Root CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
pathLenConstraint		X		None	Fixed

3.2.2 LuxTrust 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 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
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		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Global Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
KeyIdentifier		X		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.luxtrust.lu/LTGRCA.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [2]	N/A	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.3 LuxTrust Privacy+ CA

LuxTrust Privacy+ 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 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Privacy+ CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10.4	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed

[2] 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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Privacy+ CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
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.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [3]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.4 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					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time **+up to 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed

[3] 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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust SSL CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10.5	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
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.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [4]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.5 LuxTrust TEST CA

LuxTrust TEST 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] 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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust TEST CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time +**up to 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust TEST CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10.6	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
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.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [5]	N/A	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.6 LuxTrust Internal CA

LuxTrust Internal CA

[5] 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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Internal CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.10.7	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
digitalSignature				Set	Fixed
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
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.crl	Fixed

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Internal CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
BasicConstraints	{id-ce 19}	X	TRUE [6]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.7 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 10 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA	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		
keyCertSign				Set	Fixed
crlSign				Set	Fixed

[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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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	
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.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [7]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.8 LuxTrust e-Government CA

LuxTrust eGovernment 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 6 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust Global Root	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust eGovernment CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		

[7] 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*".

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust eGovernment CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
policyIdentifier		X		1.3.171.1.1.1.10.9	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
digitalSignature				Set	Fixed
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
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.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [8]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

3.2.9 Certificate extensions

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

3.2.10 Algorithm object identifiers

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

3.2.11 Name forms

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

3.2.12 Name constraints

Name constraints are supported as per RFC 5280.

3.2.13 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

[8] 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".*

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

3.2.14 Usage of Policy Constraints extension

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

3.2.15 Policy qualifiers syntax and semantics

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

3.3 LuxTrust End-entity – Certificates profiles

3.3.1 Certificate profiles

Under the new LuxTrust Global root and associated CAs, multiple types of certificates will be issued. 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 future LuxTrust 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+ [9] 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+ [10] 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*.

- **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 [13] 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*.

3.3.2 Version number(s)

X.509 v3 is supported and used.

3.3.3 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.

[9] As defined by ETSI TS 101 456 [2].
[10] As defined in ETSI TS 102 042 [4].
[11] As defined by ETSI TS 101 456 [2].
[12] As defined in ETSI TS 102 042 [4].
[13] As defined in ETSI TS 102 042 [4].

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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) [2].

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[14]**	**CE[15]**	**O/M[16]**	**CO[17]**	**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
	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)*

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

[15] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD QCP+ Certificate Profile						
Attribute	Field	IN[14]	CE[15]	O/M[16]	CO[17]	Value
	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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD QCP+ Certificate Profile						
Attribute	Field	IN[14]	CE[15]	O/M[16]	CO[17]	Value
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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 [5]
	QcRetentionPeriod	✓		O	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓		M	D	Set

3.3.4 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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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) [3].

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**[18]	**CE**[19]	**O/M**[20]	**CO**[21]	**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
	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)*

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

[19] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	Field	IN[18]	CE[19]	O/M[20]	CO[21]	Value
	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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	Field	IN[18]	CE[19]	O/M[20]	CO[21]	Value
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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

3.3.5 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) [2].

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>**.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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

LuxTrust non SSCD QCP Certificate Profile						
Attribute	**Field**	**IN[22]**	**CE[23]**	**O/M[24]**	**CO[25]**	**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
	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*

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

[23] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Certificate Profile						
Attribute	**Field**	**IN[22]**	**CE[23]**	**O/M[24]**	**CO[25]**	**Value**
	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: 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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Certificate Profile						
Attribute	Field	IN[22]	CE[23]	O/M[24]	CO[25]	Value
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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	✓				1.3.171.1.1.10.3.3
	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** on SSCD compliant with ETSI TS 101 456 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 [5]

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Certificate Profile						
Attribute	Field	IN[22]	CE[23]	O/M[24]	CO[25]	Value
	QcRetentionPeriod	✓		O	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓				NOT SET

3.3.6 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) [3].

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[26]	CE[27]	O/M[28]	CO[29]	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
	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			

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

[27] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD NCP Certificate Profile						
Attribute	Field	IN[26]	CE[27]	O/M[28]	CO[29]	Value
	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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD NCP Certificate Profile						
Attribute	Field	IN[26]	CE[27]	O/M[28]	CO[29]	Value
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (=010001).
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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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	✓				1.3.171.1.1.10.3.4
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD NCP Certificate Profile						
Attribute	Field	IN[26]	CE[27]	O/M[28]	CO[29]	Value
	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

3.3.7 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) [3].

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.

Note: Due to technical constraints within the Signing Server, the signature algorithm will be SHA1WithRsa instead of SHA256WithRsa.

LuxTrust Signing Server NCP 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 = "1.2.840.113549.1.1.5" – SHA1 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA
	organizationName	✓			S	LuxTrust S.A.

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Signing Server NCP Certificate Profile						
Attribute	Field	IN[30]	CE[31]	O/M[32]	CO[33]	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).*

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Signing Server NCP Certificate Profile						
Attribute	Field	IN[30]	CE[31]	O/M[32]	CO[33]	Value
	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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓				1.3.171.1.1.10.3.5
	policyQualifierID	✓			S	Id-qt-1 (CPS)

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Signing Server NCP Certificate Profile						
Attribute	Field	IN[30]	CE[31]	O/M[32]	CO[33]	Value
	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

3.3.8 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., 0.4.0.2042.1.1) [2].

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 QCP+ oid, i.e., **< OID 1.3.171.1.1.10.3.7>**.

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

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	Field	IN[34]	CE[35]	O/M[36]	CO[37]	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
	organizationName	✓			S	LuxTrust S.A.

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

[35] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	Field	IN[34]	CE[35]	O/M[36]	CO[37]	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	***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: 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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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).

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	Field	IN[34]	CE[35]	O/M[36]	CO[37]	Value
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)
	noticeNumbers					
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on SSCD compliant with ETSI TS 102 042 LCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage:** Support of Integration Electronic Signature.
	PolicyIdentifier	✓				0.4.0.2042.1.3
QualifiedCertificateStat						
	QcCompliance	✓		O	S	Not Set
	QcLimitValue	✓		O	D	Not Set
	QcRetentionPeriod	✓		O	D	Not Set
	QcSSCD	✓		M	D	Set

3.3.9 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., 0.4.0.2042.1.2) [3].

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[38]	CE[39]	O/M[40]	CO[41]	Value

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

[39] CE = Critical Extension.

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	Field	IN[38]	CE[39]	O/M[40]	CO[41]	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
	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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LCP+ Integration Certificate Profile						
Attribute	Field	IN[38]	CE[39]	O/M[40]	CO[41]	Value
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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	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)
	noticeNumbers					
	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

3.3.10 LuxTrust Signing Server Account LCP Certificates supporting Signature, Authentication & Encryption for integration purposes

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 LCP Certificates are compliant with and include the oid reference of the NCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3) [3].

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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 1.3.171.1.1.10.3.9>**.

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

Note: Due to technical constraints within the Signing Server, the signature algorithm will be SHA1WithRsa instead of SHA256WithRsa.

LuxTrust Signing Server LCP Certificate Profile						
Attribute	**Field**	**IN**[42]	**CE**[43]	**O/M**[44]	**CO**[45]	**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" – SHA1 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA
	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)***
	givenName	✓		M	D	***LGQCA XX (XX a number selected internally by LuxTrust)***
	surname	✓		M	D	***CSS***
	countryName	✓		M	D	*LU*
	emailAddress	✓		O	D	*N/A*
	title	✓		M	D	***Private Person***

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Signing Server LCP Certificate Profile						
Attribute	Field	IN[42]	CE[43]	O/M[44]	CO[45]	Value
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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Signing Server LCP Certificate Profile						
Attribute	Field	IN[42]	CE[43]	O/M[44]	CO[45]	Value
	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

3.3.11 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) [2].

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[46]	CE[47]	O/M[48]	CO[49]	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
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.

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

[47] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LORA QCP+ Certificate Profile						
Attribute	Field	IN[46]	CE[47]	O/M[48]	CO[49]	Value
	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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.crl
Subject Properties						
subjectAltName		✓	False			

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LORA QCP+ Certificate Profile						
Attribute	**Field**	**IN[46]**	**CE[47]**	**O/M[48]**	**CO[49]**	**Value**
	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 [5]
	QcRetentionPeriod	✓		O	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓		M	D	Set

3.3.12 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) [3].

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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**[50]	**CE**[51]	**O/M**[52]	**CO**[53]	**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
	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*

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

[51] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LORA NCP+ Certificate Profile						
Attribute	Field	IN[50]	CE[51]	O/M[52]	CO[53]	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: 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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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)

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSCD LORA NCP+ Certificate Profile						
Attribute	Field	IN[50]	CE[51]	O/M[52]	CO[53]	Value
	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

3.3.13 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) [2].

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[54]	CE[55]	O/M[56]	CO[57]	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.

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	Field	IN[54]	CE[55]	O/M[56]	CO[57]	Value
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust **Global Qualified** CA
	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						

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	Field	IN[54]	CE[55]	O/M[56]	CO[57]	Value
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/LTGQCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA.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					

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	**Field**	**IN[54]**	**CE[55]**	**O/M[56]**	**CO[57]**	**Value**
	DisplayText	✓				LuxTrust Qualified Certificate **not** SSCD compliant with ETSI TS 101 456 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 [5]
	QcRetentionPeriod	✓		O	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓				**NOT SET**

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

LuxTrust Server Certificates are ETSI TS 102 042 LCP Certificates [5] not certified as generated on SSCD, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or three (3) years validity from issuing start date.

These LuxTrust 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 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[58]**	**CE[59]**	**O/M[60]**	**CO[61]**	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			

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

[59] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL Server LCP Certificate Profile						
Attribute	Field	IN[58]	CE[59]	O/M[60]	CO[61]	Value
	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;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 or, **if commonName contains a unique server name**, this field (OU1) **must** contain the text: INTERNAL USE ONLY
	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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL Server LCP Certificate Profile						
Attribute	Field	IN[58]	CE[59]	O/M[60]	CO[61]	Value
	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://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA.crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCA.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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL Server LCP Certificate Profile						
Attribute	Field	IN[58]	CE[59]	O/M[60]	CO[61]	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-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-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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL Server LCP Certificate Profile						
Attribute	Field	IN[58]	CE[59]	O/M[60]	CO[61]	Value
	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
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Standard SSL/TLS Server Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on http://repository.luxtrust.lu. Signed by a SSL CA.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust SSL Server LCP Certificate Profile						
Attribute	Field	IN[58]	CE[59]	O/M[60]	CO[61]	Value
	PolicyIdentifier	✓				0.4.0.2042.1.3
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	True
Netscape Proprietary						
Netscape Certificate Type		✓	False			
	SSL Client	✓			S	Set
	SSL Server	✓			S	Set
	S/MIME	✓			S	Set

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

LuxTrust Extended Validation Server Certificates are ETSI TS 102 042 EVCP Certificates [5], 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 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 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 server certificates**, i.e., **<1.3.171.1.1.10.5.2>**.

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

SSL/TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	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	

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

[63] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	Value
	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** 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)
	jurisdictionOfIncorporationCountryName* (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)
	jurisdisctionOfIncorporationStateOrProvinceName (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)

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	Value
	jurisdictionOfIncorporationLocalityName **(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 • Business Entity • Non-Commercial Entity
	serialNumber **(OID: 2.5.4.5)**	✓		M	D	See EV Guidelines 1.4: For Private Organizations: contains the Registration (or similar) Number assigned to the Subject, or the date of incorporation Government entities Registration number or readily verifiable date of Creation. For Business Organizations: contains the Registration (or similar) Number assigned to the Subject, or the date of incorporation
	postalCode **(OID: 2.5.4.17)**	✓		O	D	Postal code of the subject place of business.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	Value
	streedAddress (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://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA.crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCA.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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	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. Wildcard name not allowed.
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	✓				1.3.171.1.1.10.5.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				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.
	PolicyIdentifier	✓				0.4.0.2042.1.4
Extended Key Usage		✓	False			

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates						
Attribute	Field	IN[62]	CE[63]	O/M[64]	CO[65]	Value
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

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

LuxTrust Server Certificates are ETSI TS 102 042 EVCP+ Certificates [5] certified as generated on Secure User 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 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 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 server certificates**, i.e., **<1.3.171.1.1.10.5.3>**.

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[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 **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** Months
subject		✓	False			

[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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates on Secure User Device						
Attribute	Field	IN[66]	CE[67]	O/M[68]	CO[69]	Value
	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)
	jurisdictionOfIncorporationCountryName* (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)
	jurisdisctionOfIncorporationStateOrProvinceName (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)
	jurisdictionOfIncorporationLocalityName (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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN[66]**	**CE[67]**	**O/M[68]**	**CO[69]**	**Value**
	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 • Business Entity • Non-Commercial Entity
	serialNumber **(OID: 2.5.4.5)**	✓		M	D	See EV Guidelines 1.4: For Private Organizations: contains the Registration (or similar) Number assigned to the Subject, or the date of incorporation Government entities Registration number or readily verifiable date of Creation. For Business Organizations: contains the Registration (or similar) Number assigned to the Subject, or the date of incorporation
	postalCode **(OID: 2.5.4.17)**	✓		O	D	Postal code of the subject place of business.
	streedAddress **(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			

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates on Secure User Device						
Attribute	**Field**	**IN[66]**	**CE[67]**	**O/M[68]**	**CO[69]**	**Value**
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust **SSL** CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA.crt
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCA.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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates on Secure User Device						
Attribute	Field	IN[66]	CE[67]	O/M[68]	CO[69]	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
	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. Wildcard name not allowed.
subjectKeyIdentifier		✓	False			

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

SSL / TLS Extended Validation Server Certificates on Secure User Device						
Attribute	Field	IN[66]	CE[67]	O/M[68]	CO[69]	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	✓				1.3.171.1.1.10.5.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				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.
	PolicyIdentifier	✓				0.4.0.2042.1.5
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

3.3.17 LuxTrust Object (or code) Signing Certificates

LuxTrust Code Signing Certificates are ETSI TS 102 042 LCP Certificates [5] not certified as generated on SSCD, with creation of the keys by the Subscriber, with a 2048-bit key size and one (1) or three (3) years validity from issuing start date.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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>.***

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

*Items marked **Green** have to be provided by the requesting company; items marked **Red** can be provided optionally.*

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [70]	**CE** [71]	**O/M** [72]	**CO** [73]	**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; 36** months **(1 or 3 years validity)**
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*

[70] IN = Included: Attribute / field included within the certificate profile.
[71] CE = Critical Extension.
[72] O/M: O = Optional, M = Mandatory.
[73] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [70]	**CE** [71]	**O / M** [72]	**CO** [73]	**Value**
						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://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA.crt
CRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCA.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*

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [70]	**CE** [71]	**O / M** [72]	**CO** [73]	**Value**
						unused bit-string bits).
Policy Properties						
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
Netscape Proprietary						
NetscapeCertificateType		✓	False			
	Object Signing	✓			S	Set

3.3.18 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 [6]. 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.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Timestamping Certificate Profile						
Attribute	Field	IN[74]	CE[75]	O/M[76]	CO[77]	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
	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.***
	organizationalUnitName1	✓		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/LTGTSACA.crt
	AccessMethod	✓				Id-ad-1

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

[75] CE = Critical Extension.

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

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

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

LuxTrust Timestamping Certificate Profile						
Attribute	Field	IN[74]	CE[75]	O/M[76]	CO[77]	Value
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGTSACA.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

3.3.19 Certificate extensions

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

3.3.20 Algorithm object identifiers

Algorithms OID are conforming to IETF RFC 3279 [10] and RFC 5280 [11].

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

3.3.21 Name forms

Name forms are in the X.500 distinguished name form as implemented in RFC 3739 [12].

3.3.22 Name constraints

Name constraints are supported as per RFC 5280 [11].

3.3.23 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739 [12].

3.3.24 Usage of Policy Constraints extension

Usage of Policy Constraints extension is supported as per RFC 5280 [11].

3.3.25 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 5280 [11] is supported.

3.3.26 Processing semantics for the critical Certificate Policies

Not applicable.

3.4 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	Sha1RSA
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 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>

3.4.1 Version number(s)

See section 3.4.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu

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.

3.4.2 CRL entry extensions

See section 3.4.

3.5 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported. 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.

3.5.1 Version number(s)

See section 3.5.

3.5.2 OCSP extensions

See section 3.5.

IVY Building | 13-15 Parc d'activités | L-8308 Capellen | TVA LU20976985 | RCS: B112233 | Phone: +352 26 68 15 - 1 | Fax: +352 26 68 15 - 789 | info@luxtrust.lu
www.luxtrust.lu