

Version number: 1.25 Publication Date: 06/11/2017 Effective Date: 13/11/2017

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



Copyright © 2017 - All rights reserved



Document Information

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

Version History

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



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



Table of content

DOCUMEN	T INFORMATION	2
	HISTORY	2
TABLE OF	CONTENT	4
INTELLECT	IUAL PROPERTY RIGHTS	6
REFERENC	CES	7
INTRODUC	TION	8
1.1	THE LUXTRUST PROJECT	
1.2	GOAL OF THE LUXTRUST PKI	
1.3	LUXTRUST PKI HIERARCHY	8
2	LUXTRUST CERTIFICATION AUTHORITIES	9
2.1	TWO-LEVEL CA HIERARCHY	9
3	CERTIFICATE AND CRL PROFILES	11
3.1	CERTIFICATE TYPES	11
3.2	LuxTrust Certification Authorities – Certificates profiles	22
3.3	LUXTRUST GLOBAL ROOT CA	22
3.4	LUXTRUST GLOBAL QUALIFIED CA	23
3.4.1	LuxTrust SSL CA	24
3.4.2	LuxTrust TSA (Timestamping) CA	26
3.4.3	Certificate extensions	27
3.4.4	Algorithm object identifiers	27
3.4.5	Name forms	27
3.4.6	Name constraints	
3.4.7	Certificate policy object identifier	
3.4.8	Usage of Policy Constraints extension	
3.4.9	Policy qualifiers syntax and semantics	
3.5	LUXTRUST END-ENTITY – CERTIFICATES PROFILES	
3.5.1	Certificate profiles	
3.5.2	Version number(s)	
3.5.3 3.5.4	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	
3.5.4 3.5.5	LuxTrust OSCD NCF+ Certificates supporting Advanced Electronic Signatures	
3.5.6	LuxTrust non SSCD CCP Certificates supporting Autoniced Electronic Signatures	
3.5.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	
3.5.8	LuxTrust NCP+ Certificates supporting Mass Signature Services	
3.5.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	
3.5.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	
3.5.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for it	
	purposes	-
3.5.12	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	
3.5.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	
3.5.14	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures	49
3.5.15	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures	51
3.5.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	53
3.5.17	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures	
3.5.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	57



3.5.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	59
3.5.20	LuxTrust SSL/TLS Standard Server Certificates - LCP certificates supporting Signature, Auth	entication
	Encryption	61
3.5.21	SSL/TLS Extended Validation Server Certificates - EVCP certificates supporting Signature, Auth	nentication
	Encryption	64
3.5.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Auth	nentication
	Encryption	68
3.5.23	LuxTrust Object (or Code) Signing Certificates	73
3.5.24	LuxTrust SSL/TLS Certificate for Client Authentication	75
3.5.25	SSL/TLS QCP-w Extended Validation Server Certificates	77
3.5.26	LuxTrust SPARE Signing Server LCP Certificate Profile	80
3.5.27	LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature	83
3.5.28	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	85
3.5.29	LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature	88
3.5.30	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	90
3.5.31	LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature	92
3.5.32	LuxTrust Smart Card QCP-n-qscd Certificate Profile	94
3.5.33	LuxTrust Smart Card NCP+ Certificate Profile	97
3.5.34	LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature	98
3.5.35	LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purposes	
3.5.36	QCP-n-qscd supporting Qualified Electronic Signature for eID smart cards	101
3.5.37	NCP+ supporting Authentication & Encryption for eID smart cards	
3.5.38	LuxTrust Signing Server QCP-n-qscd Certificate Profile	105
3.5.39	LuxTrust Signing Server QCP-I-qscd Certificate Profile	107
3.5.40	LuxTrust Signing Stick QCP-n-qscd certificate profile	
3.5.41	LuxTrust Signing Stick NCP+ Certificate Profile	111
3.6	TIMESTAMPING CERTIFICATE PROFILE	113
3.6.1	Normalized Certificate Policy for LuxTrust Qualified Timestamping	115
3.6.2	Qualified Timestamping Certificate Profile	116
3.6.3	TimeStamp Request and Response Format	118
3.7	CERTIFICATE EXTENSIONS	119
3.8	ALGORITHM OBJECT IDENTIFIERS	119
3.9	NAME FORMS	119
3.10	NAME CONSTRAINTS	119
3.11	CERTIFICATE POLICY OBJECT IDENTIFIER	119
3.12	USAGE OF POLICY CONSTRAINTS EXTENSION	119
3.13	POLICY QUALIFIERS SYNTAX AND SEMANTICS	119
3.14	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES	120
3.15	CRL PROFILE	120
3.15.1	Version number(s)	
3.15.2	CRL entry extensions	
3.16	OCSP PROFILE	
3.16.1	Version number(s)	
3.16.2	OCSP extensions	



VERSION 1.25

Intellectual Property Rights

Without limiting the "all rights reserved" copyright on the present document, and except as duly licensed under written form, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission of LuxTrust S.A.



VERSION 1.25

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.
- European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the [2] protection of individuals with regards to the processing of personal data and on the free movement of such data.
- ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities [3] issuing qualified certificates.
- [4] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities. [5]
- [6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 1 juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [10] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [11] LuxTrust Time Stamping Policy, latest version in force.
- [12] Guidelines for the Issuance and Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.
- [13] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force.
- [14] eID Certificate Life Cycle Procedure latest version in force
- [15] RNCID : National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16
- [16] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité [17] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [18] Loi du 19 juin 2013 Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques
- [19] EN 319 411 1 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [20] EN 319 411 2 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [21] According to EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security
- Requirements for Trust Service Providers issuing Time-Stamps (2016-03)
- [22] According to EN 319 422 V1.1.1, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (2016-03)
- [23] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)
- [24] According to EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)
- [25] According to EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)
- [26] According to EN 319 412-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (2016-02)
- [27] According to EN 319 412-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)
- [28] According to EN 319 412-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)
- [29] According to EN 319 412-4 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (2016-02)
- [30] According to EN 319 412-5 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements (2016-02)
- [31] eIDAS regulation: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG



INTRODUCTION

1.1The LuxTrust project

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

Established in November 2005 through a partnership between the Luxembourg government and the major private financial actors in Luxembourg, LUXTRUST S.A. was created to become a provider of certification services as defined in the law of the Grand-Duchy of Luxembourg modified on 14/08/2000 [7] itself derived from the European Directive on electronic signatures (1999/93/EC; cf. [1]). These laws and directives set out the legal framework for electronic signatures in the Grand-Duchy of Luxembourg as well as for LuxTrust activities as TTP.

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

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

1.2 Goal of the LuxTrust PKI

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

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

LuxTrust will also promote these services towards application service providers in order to facilitate the emergence of eapplications and accelerate eLuxembourg. Within this context, LuxTrust will form the catalyser of such services and applications.

1.3 LuxTrust PKI Hierarchy

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

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

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



VERSION 1.25

LuxTrust Certification Authorities

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

1.4 Two-level CA hierarchy

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

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

- One "LuxTrust Global Root CA" root-signing all subordinates LuxTrust CAs
- LuxTrust subordinate CAs. Each of these CAs is root-signed by the LuxTrust Global Root CA:
 - o LuxTrust Global Qualified CA
 - o LuxTrust SSL CA
 - LuxTrust Time Stamping Authority
- Additional CAs or CA hierarchies might be signed in the future under the LuxTrust Global Root CA

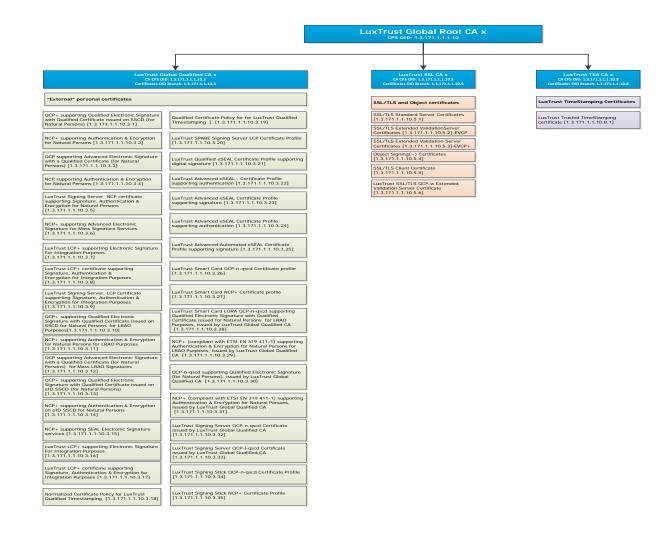
Subordinate CAs are operating within a grant of authority for issuing certificates under the LuxTrust CPS and the applicable CP. This grant has been provided by the "LuxTrust Global Root CA" (hereafter "LTGRCA") under the responsibility and authority of LuxTrust S.A. acting as CSP.

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

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



Figure 1- LuxTrust running CA Hierarchy





VERSION 1.25

CERTIFICATE AND CRL PROFILES

1.5Certificate types

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

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



CP identification	CP OID	CPS OID	Short Description	Ref.
NCP+ supporting Advanced Electronic Mass Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Mass Signature Services.	LuxTrust NCP+ Certificates supporting Mass Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.7	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.8	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048- bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.9	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048- bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for INTEGRATION PURPOSES.	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes
QCP+supportingQualifiedElectronicSignaturewithQualifiedCertificateissued onSSCD forNaturalPersonsLRAOPurposesissuedbyLuxTrustGlobalQualifiedCA	1.3.171.1.1.10.3.10	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes
NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.11	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for LRAO Purposes.	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes
QCP supporting Advanced Electronic Signature with a Qualified Certificate for Mass LRAO Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.12	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for Mass LRAO Signatures.	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures



CP identification	CP OID	CPS OID	Short Description	Ref.
QCP+ supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.13	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.14	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption
NCP+ Advanced Electronic Seal Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.15	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Seal Signature Services.	LuxTrust NCP+ Certificates supporting SEAL Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.16	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of authentication (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption
Normalized Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.18	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Normalized Certificate Policy for Qualified Timestamping
Qualified Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.19	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Qualified Certificate Policy for Qualified Timestamping
LuxTrust SPARE Signing Server LCP Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.20	1.3.171.1.1.1.10.3	LuxTrust SPARE Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy.	SPARE Signing Server LCP Certificate Profile



CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Qualified eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.21	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy.	Qualified eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSeal - Certificate Profile supporting authentication issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.22	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.23	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSEAL Certificate Profile supporting authentication issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.24	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced Automated eSEAL Certificate Supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.25	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate on HSM compliant with ETSI EN 319 411- 1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced Mass eSEAL Certificate Profile supporting digital signature
LuxTrust Smart Card QCP-n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.26	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature.	LuxTrust Smart Card QCP-n-qscd Certificate Profile
LuxTrust Smart Card NCP+ Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.27	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose.	LuxTrust Smart Card NCP+ Certificate Profile
LuxTrust Smart Card LORA QCP-n-qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.28	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy, with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smart Card LORA QCP-n- qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes,



CP identification	CP OID	CPS OID	Short Description	Ref.	
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.29	1.3.171.1.1.1.10.3	LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes,	
QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.30	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons),	
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.31	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons,	
LuxTrust Signing Server QCP-n- qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.32	1.3.171.1.1.1.10.3	Signing Server certificate for qualified signature	LuxTrust Signing Server QCP-n-qscd Certificate profile	
LuxTrust Signing Server QCP-I- qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.33	1.3.171.1.1.1.10.3	Signing Server certificate for qualified eSeal	LuxTrust Signing Server QCP-I-qscd Certificate profile	
LuxTrust Signing Stick QCP-n-qscd Certificate Profile	1.3.171.1.1.10.3.34	1.3.171.1.1.1.10.3	Signing Stick QCP-n-qscd Certificate Profile	Signing Stick QCP-n-qscd Certificate Profile	
LuxTrust Signing Stick NCP+ Certificate Profile	1.3.171.1.1.10.3.35	1.3.171.1.1.1.10.3	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile	
LuxTrust SSL Certification Authority					
SSL/TLS Standard Server Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	1.3.171.1.1.1.10.5	ETSI TS 102 042 LCP compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption	



VERSION 1.25

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

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

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

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



VERSION 1.25

In addition to the above described certifications services, the LuxTrust CSP activities include the LuxTrust Time Stamping Services (TSS). These services consist of the management of the infrastructure, and the provisioning of Time Stamp Tokens according to the LuxTrust Time Stamping Policy [11].

These services are provided by LuxTrust S.A. acting as LuxTrust Trusted Time Stamping Services Provider (TTSSP) to the Subscribers and are an integral part of the LuxTrust PKI. Hereafter the term CSP includes the activities and provision of trusted time stamping services as expressed in the European Directive on electronic signatures (cf. [1]). LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy [11].

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

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

VERSION	1 25
VERSION	1.20

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

Domain	Document category	Document		Sub-document – description	LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
1 LuxTrust	LuxTrust Certif Statements	ication Practice							
PKI	1 CPS LuxTrust	1 CPS Summary GTE/Verizon Chain	0			x	у	1.3.171.1 .1.1.1.0.x.y	N/A
		2 Not Used		Not Used		-	-	not used	N/A
		10 CPS LuxTrust	CPS LuxTrust			-	-	1.3.171.1 .1.1.10	N/A
		Global Root Chain				-	-	1.3.171.1 .1.1.10.3	N/A
			5	LuxTrust SSL CA		-	-	1.3.171.1. 1.1.10.5	N/A
			8	LuxTrust Global Timestamping CA		-	-	1.3.171.1. 1.1.10.8	N/A
1 LuxTrust	LuxTrust Certi	ficate Policies							
PKI	10 CP's LuxTrust Global Chain	3 LuxTrust Global Qualified CA	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
		Certificates	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			Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1. 1.10.3.4	0.4.0.2042.1.1
			5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1 .1.10.3.5	0.4.0.2042.1.1
			6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-	-	1.3.171.1. 1.10.3.6	0.4.0.2042.1.1

LuxTrust proprietary and confidential

Page 18



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

VERSION 1.25

]		23	LuxTrust Advanced eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.23	0.4.0.2042.1.2	
		24 LuxTrust Advanced eSEAL Certificate authentication		LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.24	0.4.0.2042.1.2	
		25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.25	0.4.0.2042.1.2	
		26	LuxTrust Smart Card QCP-n-qscd Certificate Profile	SmartCard PRI/PRO		-	1.3.171.1 .1.10.3.26	0.4.0.194112.1.2	
				Signature Certificate					
	23	27	LuxTrust Smart Card NCP+ Certificate Profile	SmartCard PRI/PRO			1.3.171.1 .1.10.3.27	0.4.0.2042.1.2	
		21	Lux rust Smart Card NCF+ Certificate Frome	Authentication Certificate	1	-	1.5.171.1.1.10.5.27	0.4.0.2042.1.2	
		28	LuxTrust Smart Card LORA NCP+ - Signature	SmartCard LORA		_	1.3.171.1 .1.10.3.28	0.4.0.2042.1.2	
	25	Certificate	Certificate for LRAO Purposes	Signature Certificate			1.3.171.111.10.3.20	0.4.0.2042.1.2	
		20	LuxTrust Smart Card LORA NCP+ - authentication	SmartCard LORA			1.3.171.1 .1.10.3.29	0.4.0.2042.1.2	
		29	Certificate for LRAO Purposes	Authentication Certificate	-	-	1.3.171.1 .1.10.3.29		
		20	30 LuxTrust eID Smart Card QCP-n-qscd Certificate	eID SmartCard			1.3.171.1 .1.10.3.30	0.4.0.194112.1.2	
		30		Signature Certificate	-	-	1.3.171.1 .1.10.3.30		
		04		eID SmartCard			4 0 474 4 4 40 0 04	0.4.0.0040.4.0	
		31	LuxTrust eID Smart card NCP+ Certificate	Authentication Certificate	-	-	1.3.171.1. 1.10.3.31	0.4.0.2042.1.2	
		32 LuxTrust Signing Server QCP-n-qscd Certificate		Signing Server certificate for qualified signature	-	-	1.3.171.1. 1.10.3.32	0.4.0.194112.1.2	
		33	LuxTrust Signing Server QCP-I-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1. 1.10.3.33	0.4.0.194112.1.3	
		34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171. 1.1.10.3.34	0.4.0.194112.1.2	
	3	35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171. 1.1.10.3.35	0.4.0.2042.1.2	
	5 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	
	Certificates	2	SSL/TLS(+) Extended Validation Server Certificates – EVCP	SSL/TLS Extended Validation Server Certificates	-	-	1.3.171.1. 1.10.5.2	0.4.0.2042.1.4	



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



1.6LuxTrust Certification Authorities – Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

1.7LuxTrust Global Root CA

	Lu	IXTrust Gl	obal Root	СА	
Base Profile	OID	Include d	Critical	Value	
Version		х		V3	
SerialNumber		х		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	х		SHA256 with RSA Encryption	Fixed
SignatureValue		х		Issuing CA Signature	
Validity					
NotBefore		х		Key Generation Process Date/Time	
NotAfter		х		Key Generation Process Date/Time + 10;20 years	Fixed
SubjectPublicKeyInf o		x		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). 20 years certificate requires a 4096 key length.	
Issuer					
CountryName	{ id-at-6 }	х		LU	Fixed
CommonName	{ id-at-3 }	х		LuxTrust Global Root x ¹	Fixed
organizationName		х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Root x ¹	Fixed
organizationName		х		LuxTrust S.A.	Fixed
CertificatePolicies ²	{id-ce 32}	х	FALSE		
policyIdentifier		х		1.3.171.1.1.10	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	х	TRUE ⁶		

 $^{^{1}}$ X is a sequential value to distinguish the old CA from the renewed CA. The value 1 is omitted as it is the first CA issued.

² Since LuxTrust Global Root 2



VERSION 1.25

	Lu	IxTrust Gl	obal Root	CA	
Base Profile	OID	Include d	Critical	Value	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyldentifie r	{id-ce 35}	Х	FALSE		
Keyldentifier		х		SHA-1 Hash	
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		х		SHA-1 Hash	
BasicConstraints	{id-ce 19}	х	TRUE ⁶		
CA		х		TRUE	Fixed
pathLenConstraint		Х		None	Fixed

1.8LuxTrust Global Qualified CA

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

 $^{^{3}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	Lu	xTrust Glob	al Qualifie	ed CA	
Base Profile	OID	Include d	Critical	Value	
policyIdentifier		х		1.3.171.1.1.10.3	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	х		CPS	Fixed
Qualifier	CPSuri	х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	х	TRUE ⁶		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifie r	{id-ce 35}	х	FALSE		
Keyldentifier		х		SHA-1 Hash of Authority public key	
authorityInfoAccess	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		Х		http://ca.luxtrust.lu/LTGRCAx17.crt	Fixed
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		х		SHA-1 Hash of Subject public key	
cRLDistributionPoin ts	{id-ce 31}	х	FALSE		
distributionPoint					
FullName		х		http://crl.luxtrust.lu/LTGRCAx ⁵ .crl	Fixed
BasicConstraints	{id-ce 19}	х	TRUE ⁶	N/A	
CA		х		TRUE	Fixed
pathLenConstraint		х		0 (Zero)	Fixed

1.8.1 LuxTrust SSL CA

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

⁴ Since LuxTrust Global Qualified CA 3

 $^{^{5}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued

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



VERSION 1.25

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

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

⁸ Since LuxTrust SSL CA 4



VERSION 1.25

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

1.8.2 LuxTrust TSA (Timestamping) CA

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

 $^{^{9}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	LuxTru	st Global T	imestamp	ing CA	
Base Profile	OID	Included	Critical	Value	
authorityKeyIdentifier	{id-ce 35}	х	FALSE		
Keyldentifier		х		SHA-1 Hash of Authority public key	
authorityInfoAccess10	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		x		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		x		http://ca.luxtrust.lu/LTGRCAx ¹ .crt	Fixed
subjectKeyldentifier	{id-ce 14}	х	FALSE		
Keyldentifier		х		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	х	FALSE		
distributionPoint					
FullName		Х		http://crl.luxtrust.lu/LTGRCA ⁵ .crl	Fixed
Basic Constraints	{id-ce 19}	Х	TRUE⁶	N/a	
CA		х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

1.8.3 Certificate extensions

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

1.8.4 Algorithm object identifiers

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

1.8.5 Name forms

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

1.8.6 Name constraints

Name constraints are supported as per RFC 5280.

1.8.7 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

1.8.8 Usage of Policy Constraints extension

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

1.8.9 Policy qualifiers syntax and semantics

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

1.9LuxTrust End-entity – Certificates profiles

1.9.1 Certificate profiles

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

 $^{^{10}}$ Since LuxTrust Global Timestamping CA $\rm 2$



VERSION 1.25

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

- LuxTrust SSCD Smartcards: These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
 - One LuxTrust QCP+¹¹ Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy OID **1.3.171.1.1.10.3.1**, and One LuxTrust NCP+¹² certificate for Natural Persons for the purpose of data/entity authentication and
 - encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.2.
 - Under elDAs regulation, those profiles are updated to the following certificate policies:
 - LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.26.
 - LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.10.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1] (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
 - One LuxTrust QCP¹¹ Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.10.3.3, and
 - One LuxTrust NCP¹² certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.0.3.4.
- 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 NCP¹² certificate for Natural Persons for the combined purposes of electronic signature, data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.5.
- LuxTrust eSeal Smart card-based certificates: The eSeal smart card exists in two versions: advanced and qualified.

The qualified eSeal product is based on two certificate policies:

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

The advanced eSeal product is based on two certificate policies:

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

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

- LuxTrust SSL/TLS Standard Server Certificates: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.1.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.2.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP+: SSL compliant ETSI TS 102 042 [4] Certificate generated on Secure User Device, under the Certificate OID Policy 1.3.171.1.1.10.5.3.
- LuxTrust Object Signing (+) Certificates: Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.4.
- LuxTrust SSL/TLS Client Certificates: Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.5.

1.9.2 Version number(s)

X.509 v3 is supported and used.

LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures 1.9.3

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

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

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



VERSION 1.25

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

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ OID, i.e., < OID 1.3.171.1.10.3.1>.

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

	L	uxTrust S				e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile			E a la a			
Version		✓	False		S	Version 3 Value = "2"
SerialNumb	er	✓	False		3	
Certairtairis			1 0100		FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓ ✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	\checkmark		М	D	Serial Number as constructed by LRAO
	commonName	~		м	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	✓		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		м	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	~		М	D	" Professional Person " (default) or
						"Professional Administrator" (Other titles possible for special purpose
						certificates)
						PRO products only:
	organizationName	~		М	D	Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	D	PRO products only : Company/institution country of HQ (as in articles of association)

 $^{^{13}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{14}}$ CE = Critical Extension.

¹⁵ O/M: O = Optional, M = Mandatory.

 $^{^{16}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $^{^{17}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	Lux	Trust SS	CD QC	P+ Cert	tificate	Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
, tti ibuto	11010			M for		PRO products:
	organizationalUnitName 1	V		PRO prod., condi- tional (O) for PRIV prod.)	D	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	✓		0	D	PRO products only : Company/institution department or other information item
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
F ort and s is a set	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	√	False			
	keyldentifier	~	1 uloo			SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		√	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint	✓			S	17
	fullName	\checkmark				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa		✓	False		_	
subjectKeylo	Rfc822Name	$\frac{\checkmark}{\checkmark}$	False	0	D	Certificate Holder's email address
Subjectivelyi	keyldentifier		Taise		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	\checkmark			S	True
	keyEncipherment	\checkmark			S	False
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	✓			_	1.3.171.1.1.10.3.1
	policyQualifierID	$\frac{\checkmark}{\checkmark}$			S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	qualifier policyQualifierID	✓ ✓			S S	https://repository.luxtrust.lu Id-qt-2 (User Notice)
	noticeNumbers	v			3	Id-ql-2 (Oser Nolice)
	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.
	Policyldentifier	\checkmark				0.4.0.1456.1.1
QualifiedCer						
	QcCompliance	\checkmark		M	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance
	QcSSCD	~		М	D	with [3] 0.4.0.1862.1.4

¹⁸ SINCE LTGQCA3



VERSION 1.25

1.9.4 LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption

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

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

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.10.3.2>**.

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

		uxirusi	33001	NCP+ Ce	lincale	Prome
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			Version 3 Value = "2"
SerialNumbe		✓	False		S	Version 3 value = "2"
Senanumbe			1 0150		FDV	Validated on duplicates.
signatureAlg	orithm	√	False		1.51	
<u> </u>	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVal	ue	✓	False			
		1			D	Issuing CA Signature.
issuer	a a un tru Marma	✓ ✓	False		S S	
	countryName commonName	✓ ✓			S	
		· ·				LuxTrust Global Qualified CA x ¹⁷
Validity	organizationName	✓ ✓	False		S	LuxTrust S.A.
valuity	NotBefore	▼ ✓	Faise		D	Certificate generation process date/time.
	NotAfter	· ·			D	Certificate generation process date/time + 36
						Months
subject	•	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						PRO and PRIVATE products: Concatenation
	commonName	~		М	D	of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	title	~		М	D	PRIVATE products:Fixed value: "Private Person"PRO products:"Professional Person" (default) or"Professional Administrator"(Other titles possible for special purpose
	organizationName	~		М	D	certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents,



	Lux	Trust	SSCD	NCP+ Cer	tificate	Profile
Attribute	Field	IN ¹³		O/M ¹⁵	CO ¹⁶	Value
	localityName	~		М	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	\checkmark		О	D	PRO products only : Company/institution department or other information item
subjectPubli		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
-	subjectPublicKey	~		M		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey		✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	√	False			
<u> </u>	AccessMethod	✓				ld-ad-2
	accessLocation	\checkmark				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	\checkmark				Id-ad-1
	accessLocation	\checkmark				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	\checkmark				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyld	entifier keyldentifier	✓ ✓	False		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		\checkmark	True			
	digitalSignature	\checkmark			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	\checkmark			S	True
certificatePo		✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.2
	policyQualifierID	√ √			S	Id-qt-1 (CPS)
	qualifier policyQualifierID	$\frac{\checkmark}{\checkmark}$			S S	https://repository.luxtrust.lu Id-qt-2 (User Notice)
	noticeNumbers	v				
	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.
	Policyldentifier	✓				0.4.0.2042.1.2



VERSION 1.25

1.9.5 LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures

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

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

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate. These Certificates include the corresponding LuxTrust QCP OID, i.e., < OID 1.3.171.1.10.3.3>.

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

						cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profil	e					
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	ber	✓	False			
					FDV	Validated on duplicates.
signatureA	Igorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	~	False			
					D	Issuing CA Signature.
Issuer	•	✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	~			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	PRIVATE products:Fixed value: "Private Person"PRO products:"Professional Person" (default) or"Professional Administrator"(Other titles possible for special purpose



	Lux	Trust	non SS	CD QCP	Certific	cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	organizationName	*		М	D	PRO products only : Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	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	~		0	D	PRO products only : Company/institution department or other information item
sub	jectPublicKeyInfo	✓	False			
	Algorithm	~				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	~		М		exponent: Fermat-4 (=010001).
Extensions						
Authority P	roperties					
authorityKe	yldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInf	oAccess	✓	False			
	AccessMethod	~				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	~				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribu	itionPoint	~	False			
	distributionPoint	~			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Pro	perties					
subjectAltN	ame	~	False			
	Rfc822Name	~		0	D	Certificate Holder's email address
subjectKey	ldentifier	~	False			
	keyldentifier	~			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 Prop	erties					
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	\checkmark			S	True
	keyEncipherment	\checkmark			S	False
	dataEncipherment	~			S	False



VERSION 1.25

	Lux	Trust	non SS	CD QCP	Certific	cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
certificateP	olicies	✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.3
	policyQualifierID	~			S	ld-qt-1 (CPS)
	qualifier	~			S	https://repository.luxtrust.lu
	policyQualifierID	~			S	Id-qt-2 (User Notice)
	DisplayText	~				LuxTrust Qualified Certificate not on SSCD compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert
	Policyldentifier	~				0.4.0.1456.1.2
QualifiedCe	ertificateStat					
	QcCompliance	~		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	~				NOT SET

1.9.6 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

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

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

The usage purpose of these NCP Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust non SSCD NCP OID, i.e., <**OID 1.3.171.1.10.3.4**>.

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

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



	LuxTrus	st non	SSCD N	ICP Cert	ificate	Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		м	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	~		0	D	PRO products only : Company/institution department or other information item
subjectPubli		✓	False			
	algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	SubjectFublicKey	•		IVI		
Authority						
Properties authorityKey	l Identifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInfo	Access AccessMethod	✓ ✓	False			
	accessLocation	✓ ✓				Id-ad-2 http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓			-	Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint fullName	✓ ✓			S	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties		✓	Foloo			
subjectAltNa	ame Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
subjectKeylo		 ✓ 	False			
subjectKeylo	Jentifier	v	raise			



VERSION 1.25

	LuxTrust non SSCD NCP Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
	keyldentifier	✓ 			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					
certificatePo	licies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.4					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	~			S	https://repository.luxtrust.lu					
	policyQualifierID	~			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	✓ 				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage : Data or Entity Authentication and Data Encryption.					
	Policyldentifier	\checkmark				0.4.0.2042.1.1					

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

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

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

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption. These Certificates include the corresponding LuxTrust Signing Server Account NCP OID, i.e., **<OID 1.3.171.1.10.3.5>**.

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

	LuxTrust Signing Server NCP Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		\checkmark	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg	gorithm	✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.					
signatureVa	lue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	~			S	LU					
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷					
	organizationName	✓			S	LuxTrust S.A.					



	LuxTrust	Signin	g Serve	r NCP C	ertifica	te Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Validity	NotPoforo	✓ ✓	False			Contificate apparation process data/time
	NotBefore NotAfter	✓ ✓			D	Certificate generation process date/time. Certificate generation process date/time +
						36 Months
subject	T	✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	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	~		0	D	PRO products only : Company/institution department or other information item
subjectPubli		√	False			
	algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions				111		
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓	False			
	AccessMethod accessLocation	✓ ✓				Id-ad-2 http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	· ·				http://ca.luxtrust.lu/LTGQCAx .crt Id-ad-1
	accessLocation	✓ ✓	1		1	http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut		~	False			
	distributionPoint	~			S	
	fullName	✓	1			http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl



VERSION 1.25

	LuxTrust	Signin	g Serve	r NCP C	ertificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Subject Properties						
subjectAltNa	ime	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		✓	False			
	keyldentifier	~			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
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.5
	policyQualifierID	✓			S	ld-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	~				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage : Signature, Data or Entity Authentication and Data Encryption.
	Policyldentifier	\checkmark				0.4.0.2042.1.1

1.9.8 LuxTrust NCP+ Certificates supporting Mass Signature Services

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

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

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a normalised certificate for Mass Signature purposes. These Certificates include the corresponding LuxTrust NCP+ OID, i.e., < OID 1.3.171.1.10.3.6>.

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

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



LuxTrust	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN ¹³		O/M ¹⁵	CO ¹⁶	Value
	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process
						date/time + 36 Months
subject		✓	False			
	commonName	~		М	D	Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped
	countryName	~		М	D	Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	emailAddress	~		0	D	Subject's email address if available
				-	_	
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	localityName	~		М	D	Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	~		ο	D	As provided by Subscriber
	organizationalUnitName 2	~		0	D	As provided by Subscriber
subjectPublicKeyInfo		√	False			
	algorithm subjectPublicKey	\checkmark		М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	SubjectFublicKey	•		IVI		
Authority Properties						
authorityKeyldentifier		√	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfoAccess		√	False			
	AccessMethod	\checkmark				Id-ad-2
	accessLocation	✓ ✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod accessLocation	v √				Id-ad-1
cRLDistributionPoint		• •	False			http://qca.ocsp.luxtrust.lu/18
	distributionPoint	▼ ✓	1 0130		S	
	fullName	~			-	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltName		✓	False			
aubia at land dan dita	Rfc822Name	✓ ✓	F - 1	0	D	Certificate Holder's email address
subjectKeyldentifier	keyldentifier	✓ ✓	False		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		√	True			
keyUsage	digitalSignature	✓ ✓	True		S	False
	nonRepudiation				S	True
	keyEncipherment	 ✓ 			S	False
	reyEncipherment	ľ			5	Faise



VERSION 1.25

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

1.9.9 LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures

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

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

The usage purpose of these LuxTrust SSCD LCP+ Certificates is limited to sole authorised usage of supporting the creation of Integration electronic signatures for system integration purposes with non-repudiation signatures. The LuxTrust SSCD LCP+ Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.7>.

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

	LuxTrust Integration Certificate Profile										
Attribute	Field	IN ¹³		O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg		✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	lue	✓	False								
					D	Issuing CA Signature.					
Issuer	F	✓	False		S						
	countryName	✓			S	LU					
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	✓			D	Certificate generation process date/time + 36 Months					
Subject		✓	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	~		М	D	Concatenation of given name(s) and surname(s)					
	givenName	~		М	D	TEST ONLY + " " + As provided by Subscriber					
	surname	✓		М	D	As provided by Subscriber					
	countryName	✓		М	D	LU					
	emailAddress	~		0	D	As provided by Subscriber					



	Lu	xTru	st Integ	gration	Certifi	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	Title	~		Μ	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator"
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	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	~		0	D	PRO products only : Company/institution department or other information item
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	√		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	Identifier	√	False			
	keyldentifier	✓ ✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	~				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	\checkmark				http://gca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	ionPoint	~	False			
	distributionPoint	~			S	
	fullName	\checkmark				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties subjectAltNa		√	Falss			
SubjectAltNa	me Rfc822Name	✓ ✓	False	0	D	N/A
subjectKeylo		▼ ✓	False	0	U	
	keyldentifier	× ×			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			
Reyusaye	digitalSignature	▼ ✓	nue		S	False
	nonRepudiation	√			S	True
	keyEncipherment	~			S	False
	dataEncipherment	~			S	False
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.7
	policyQualifierID	√			S	Id-qt-1 (CPS)
	Qualifier	√ √			S	https://repository.luxtrust.lu
	policyQualifierID PolicyIdentifier	\checkmark			S	Id-qt-2 (User Notice) 0.4.0.2042.1.3
	i oncyndenuller	v	1		1	0.7.0.2042.1.3



VERSION 1.25

1.9.10 LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption

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

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

The usage purpose of these LuxTrust SSCD LCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD LCP+ OID, i.e., **<OID 1.3.171.1.10.3.8>**.

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

Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	tificate Profile Value
Base	Field	IIN	CE	0/101	0	value
Profile						
Version		√	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
signatureVa	lue	✓	False			RSA Encryption.
signatureva	liue	•	Faise		D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	· ·	1 0150		S	LU
	commonName	√			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity	- gameanormanio	√	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36
						Months
Subject	1	✓	False			
	serialNumber	\checkmark		М	D	Serial Number as constructed by LRAO
	commonName	~		м	D	LGQCA XX SC PRI V3 (XX a numbe selected internally by LuxTrust)
	givenName			м	D	LGQCA XX (XX a number selected internally
	Surname	~		М	D	by LuxTrust) SC PRI V3
	Surname	v		IVI	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	N/A
	Title	~		М	D	Private Person
subjectPubl	icKeyInfo	✓	False			
	Algorithm	√				Public Key: Key length: 2048 bit (RSA); public
F	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	vldentifier	√	False			
aanontyne	keyldentifier	· ·	1 0.00			SHA-1 Hash of the LuxTrust Global Qualified
	-					CA public key
authorityInfo	oAccess	✓	False			
	AccessMethod	√				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/18
cRLDistribu		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl



VERSION 1.25

	LuxTrust SSCD LCP+ Integration Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Subject Properties											
subjectAltNa	me	✓	False								
	Rfc822Name	✓		0	D	N/A					
subjectKeyld		✓	False								
	keyldentifier	~			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											
keyÜsage	•	√	True								
	digitalSignature	~			S	True					
	nonRepudiation				S	False					
	keyEncipherment	~			S	True					
	dataEncipherment	~			S	True					
certificatePo	licies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.8					
	policyQualifierID	\checkmark			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	~			S	Id-qt-2 (User Notice)					
	DisplayText Policyldentifier	✓ ✓				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. 0.4.0.2042.1.3					

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

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

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

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption for integration only. These Certificates include the corresponding LuxTrust Signing Server Account OID, i.e., **<OID** 1.3.171.1.10.3.9>.

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

	LuxTrust Signing Server LCP Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	~	False								
					FDV	Validated on duplicates.					
signatureAlg	jorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.					
signatureVal	signatureValue		False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						



	LuxTrus	t Signin	g Serve	er LCP C	ertificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	countryName	✓	-		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
Validity	organizationName	✓ ✓	Foloa		S	LuxTrust S.A.
Validity	NotBefore	▼ ▼	False		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						36 Months
Subject	T	✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	LGQCA XX CSS (XX a number selected internally by LuxTrust) or Concatenation of given name(s) and surname(s) separated by a "Space" character.
	givenName	~		М	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s) as on ID document
	Surname	~		м	D	CSS or Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	LU or Nationality of holder (ISO3166)
	emailAddress	~		0	D	N/A
	Title	✓		М	D	Private Person
subjectPubli	icKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA);
Extensions	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey		✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	✓ ✓				Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod accessLocation	✓ ✓	-		-	Id-ad-1
cRLDistribut		· ·	Foloa			http://qca.ocsp.luxtrust.lu/ ¹⁸
CREDISTIDUT	distributionPoint	▼ ▼	False		S	
	fullName	✓			0	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	ame Rfc822Name	✓ ✓	False	0	D	N/A
subjectKeylo		✓ ✓	False	0	U	
- Subjective yit	keyldentifier	· ·			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			
пеубзаде	digitalSignature	 ✓	Tue		S	True
	nonRepudiation				S	True
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo		 ✓ 	False			
	Policyldentifier	\checkmark				1.3.171.1.1.10.3.9



VERSION 1.25

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

1.9.12 LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes

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

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

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures for LRAO purposes. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ OID, i.e., < OID 1.3.171.1.10.3.10>.

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

	LuxTrust SSCD LORA QCP+ Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg		✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	lue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	\checkmark			S	LuxTrust Global Qualified CA x ¹⁷					
	organizationName	~			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	~			D	Certificate generation process date/time + 36 Months					
Subject		✓	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	~		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.					
	givenName	~		М	D	Given name(s) as on ID card					
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)					
	countryName	~		М	D	Nationality of holder (ISO3166)					
	emailAddress	~		0	D	Subject's email address					
	Title	~		М	D	"LuxTrust RA Officer"					
	organizationName	✓		М	D	Constructed by LuxTrust					



	LuxTru	ust SSCD	LORA	QCP+ (Certific	ate Profile
Attribute	Field		CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Attribute			UL	0/11	00	Value
	localityName	\checkmark		М	D	Country of RA
	organizationalUnitName	✓		м	D	RA code Constructed by LuxTrust
	1	•		141	D	The code constructed by Edx must
	organizationalUnitName	✓		м	D	RAO code Constructed by LuxTrust
	2	•		141	D	NAO code constructed by Eax must
subjectPubli		✓	False			
	Algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	Subjecti ubilertey			101		
Authority						
Properties						
authorityKey	/Identifier keyldentifier	\checkmark	False	-		SHA-1 Hash of the LuxTrust Global
	reyldentiner	•				Qualified CA public key
authorityInfo	Access	\checkmark	False			
	AccessMethod	 ✓ 				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod accessLocation	✓ ✓				Id-ad-1
- DI Distrikus			F -1			http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	distributionPoint	✓ ✓	False		S	
	fullName	· •			0	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa		√	False			
subjectKeylo	Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
subjectkeyi	keyldentifier	✓ ✓	Faise		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			Taura			
keyUsage	digitalSignature	✓ ✓	True		S	False
	nonRepudiation	· •			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	√			S	False
certificatePo	Dicies Policyldentifier	✓ ✓	False			
	policyQualifierID	✓ ✓			S	1.3.171.1.1.10.3.10 Id-qt-1 (CPS)
	Qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	\checkmark				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
	Policyldentifier	√				purposes 0.4.0.1456.1.1
QualifiedCer						
	QcCompliance	√		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance
	QcRetentionPeriod			0	D	with [3] As provided by LuxTrust S.A. in compliance
	Gonotontioni Chou					with [3]
	QcSSCD	\checkmark		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }



VERSION 1.25

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

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

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

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption for LRAO purposes. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.10.3.11>**.

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

	LuxTru	ust SS		RA NCP+	Certific	cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base			1			
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		~	False		0	
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa		~	False			
Signature va		-	1 0100		D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	~			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	~			S	LuxTrust S.A.
Validity		√ 	False			
- y	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	✓	1		D	Certificate generation process date/time + 36
						Months
Subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
						,
						Concatenation of given name(s) and
	commonName	~		М	D	surname(s) as on ID card separated by a
						"Space" character
	givenName	~		М	D	Given name(s) as on ID card
	5					
	Cumpanya.					Surname(s) as on ID card without indication
	Surname	~		М	D	"épouse", "ép." or similar and the subsequent name(s)
						name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	~		М	D	Constructed by LuxTrust
						,
	le colitu Nome	~			_	Country of DA
	localityName	v		М	D	Country of RA
	organizationalUnitName	~		М	D	RA code Constructed by LuxTrust
	1	÷		IVI	D	
	organizationalUnitName					
	2	✓		M	D	RAO code Constructed by LuxTrust
subjectPubli		√	Foloo			
Subjectrubi	Algorithm	▼ ✓	False			Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	▼ ✓		М	+	exponent: Fermat-4 (=010001).
Extensions				IVI		
Authority						
Properties						
	/Identifier	✓	False			



VERSION 1.25

	LuxT	rust SS		RA NCP+	Certific	cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu	tionPoint	✓	False			
-	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyl	dentifier keyldentifier	✓ ✓	False		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
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.11
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	~			S	Id-qt-2 (User Notice)
	noticeNumbers DisplayText	×				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage : Data or Entity Authentication and Data Encryption for LRAO purposes.
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

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

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate for Mass LRAO Signature purposes. These Certificates include the corresponding LuxTrust QCP OID, i.e., < OID 1.3.171.1.10.3.12>.

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

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



LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
SerialNumb	er	✓	False						
					FDV	Validated on duplicates.			
signatureAl	gorithm	✓	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVa	alue	~	False						
					D	Issuing CA Signature.			
Issuer		\checkmark	False		S				
	countryName	✓			S	LU			
	commonName	\checkmark			S	LuxTrust Global Qualified CA x ¹⁷			
	organizationName	\checkmark			S	LuxTrust S.A.			
Validity	•	✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	~			D	Certificate generation process date/time + 30 Months			
Subject		\checkmark	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	~		М	D	Concatenation of given name(s) and surname(s as on ID card separated by a "Space" character			
	givenName	✓		М	D	Given name(s) as on ID card			
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequer name(s)			
	countryName	✓		М	D	Nationality of holder (ISO3166)			
	emailAddress	✓		0	D	Subject's email address			
	Title	✓		М	D	"LuxTrust RA officer – LRS"			
	organizationName	✓		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA			
	localityName	~		М	D	Country of RA (as in articles of association)			
	organizationalUnitName 1	~		м	D	RA code Constructed by LuxTrust			
	organizationalUnitName 2	\checkmark		0	D	RAO code Constructed by LuxTrust			
sub	ojectPublicKeyInfo	✓	False						
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public			
	subjectPublicKey	\checkmark		М		exponent: Fermat-4 (=010001).			
Extensions									
Authority P	roperties								
authorityKe	yldentifier	✓	False						
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key			
authorityInf	oAccess	\checkmark	False						
	AccessMethod	✓				ld-ad-2			
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt			
	AccessMethod	\checkmark				Id-ad-1			



VERSION 1.25

	LuxTrust non S	SCD Q	CP Ma	ss LRAO	Signat	ures Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
cRLDistribu	utionPoint	✓	False			
	distributionPoint	~			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Pro	perties					
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	Identifier	✓	False			
	keyldentifier	~			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 Prop	erties					
keyUsage		~	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.12
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	~			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	~				LuxTrust Qualified Certificate not SSCD compliant with ETSI TS101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Support of Advanced Electronic Signature for Mass LRAO purposes
	Policyldentifier	✓				0.4.0.1456.1.2
QualifiedCe	ertificateStat					
	QcCompliance	~		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	~				NOT SET

1.9.15 LuxTrust elD SSCD QCP+ Certificates supporting Qualified Signatures

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

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



VERSION 1.25

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 1.3.171.1.10.3.13>.

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

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

The certificate re-key is not allowed.

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

	LuxT	rust elD	SSCD C	CP+ Ce	ertificat	te Profile
Attribute	Field	IN ¹⁹	CE ²⁰	O/M ²¹	CO ²²	Value
Base Profile						
Version	•	✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
		✓	= 1		FDV	Validated on duplicates.
signatureAl	Algorithm	~	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x ²³
	organizationName	✓			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	~		М	D	LU
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"Private Person"
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubl		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit
_	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						

 $^{^{19}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{20}\,\}mathrm{CE}$ = Critical Extension.

²¹ O/M: O = Optional, M = Mandatory.

 $^{^{22}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $^{^{23}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

				CP+ Ce		
Attribute	Field	IN ¹⁹	CE ²⁰	O/M ²¹	CO ²²	Value
Authority						
Properties						
authorityKey		✓ ✓	False			Old Allesh of the low Truck Olehel Overlife
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified
		✓	F alaa			CA x public key
authorityInfo	AccessMethod	v 	False			Id-ad-2
	accessLocation	✓ ✓				
						http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu		✓	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	Subject email address
subjectKeyle	dentifier	✓	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit fiel with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, no 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
certificatePo	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.13
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers				1	
	DisplayText	~				LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. Sole Authorised Usage : Support of Qualifie Electronic Signature.
	Policyldentifier	✓			_	0.4.0.1456.1.1
QualifiedCer	rtificateStat					
	QcCompliance	✓		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in complianc with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in complianc with [3]
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

1.9.16 LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption

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

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

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD NCP+ OID, i.e., **<OID 1.3.171.1.10.3.14>**.

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

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



VERSION 1.25

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

The certificate re-key is not allowed.

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

	LuxTrust SSCD NCP+ Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile				C/III							
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	r	\checkmark	False								
					FDV	Validated on duplicates.					
signatureAlg		✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVal	ue	✓	False								
					D	Issuing CA Signature.					
issuer		√	False		S						
	countryName	✓			S	LU					
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	~			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate					
subject		✓	False								
	serialNumber	~		М	D	Serial Number as constructed by LRAO					
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character					
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID					
	surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID					
	countryName	✓		М	D	LU					
	emailAddress	~		0	D	Subject's email address					
	title	~		М	D	"Private Person"					
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).					
subjectPublic	cKeyInfo	✓	False								
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit					
	subjectPublicKey	~		М		(RSA); public exponent: Fermat-4 (=010001).					
Extensions											
Authority											
Properties											
authorityKey		✓	False								
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA x public key					
authorityInfo		~	False								
	AccessMethod	✓				Id-ad-2					
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt					
	AccessMethod	✓	1		1	Id-ad-1					
	accessLocation	✓	1		1	http://gca.ocsp.luxtrust.lu/ ¹⁸					
cRLDistributi		~	False								
SILEISUIDUI	distributionPoint	· ~	1 0130		S						
	fullName	· •			5	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl					
Subject											
Subject Properties											



VERSION 1.25

	LuxTrust SSCD NCP+ Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
subjectAltNa	me	✓	False								
	Rfc822Name	✓		0	D	Subject email address					
subjectKeyld		✓	False								
	keyldentifier	~			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					
certificatePo	licies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.14					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText					LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage : Data or Entity Authentication and Data Encryption.					
	Policyldentifier	\checkmark				0.4.0.2042.1.2					

1.9.17 LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures

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

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

The usage purpose of these LuxTrust SSCD LCP+ Certificates is limited to sole authorised usage of supporting the creation of Integration electronic signatures for system integration purposes with non-repudiation signatures. The LuxTrust SSCD LCP+ Certificates include the corresponding LuxTrust LCP+ OID, i.e., < OID 1.3.171.1.10.3.16>.

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

- 1. Pseudonym certificates are issued due to the laws on data protection and national register
- 2. The Given name and the Surname are encrypted alphanumeric strings

3. The pseudonym certificates are immediately revoked as the citizen will not use his certificates

The certificate re-key is not allowed.

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



	LuxTrust eID S		Integra	ation Sig	gnature	e Certificate Profile
Attribute	Field	IN ²⁴	CE ²⁵	O/M ²⁶	CO ²⁷	Value
Base						
Profile						
Version		√	False			
<u> </u>					S	Version 3 Value = "2"
SerialNumb	er	✓	False		501/	
signatureAl	acrithm	✓	False		FDV	Validated on duplicates.
SignatureAl	Algorithm	v	Faise		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	Algorithm				3	RSA Encryption.
signatureVa	lue	√	False			
					D	Issuing CA Signature.
Issuer	-	✓	False		S	
	countryName	✓			S	LU
	commonName	\checkmark			S	LuxTrust Global Qualified CA x ²⁸
	organizationName	√			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	\checkmark			D	Certificate generation process date/time + 12
						Months;
						Certificate generation process date/time + * day for PSEUDONYM Certificate
Subject		✓	False			
Canjeet	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	Senandumber	•		IVI	D	Senar Number as constructed by ENAO
	commonName	\checkmark		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	√		м	D	specimen-x provided by the RNCID
	-				_	
	surname	✓	_	М	D	specimen-x as provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	~		0	D	specimen-x Subject's email address as provided by the RNCID
	title	✓		М	D	"Private Person"
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubl	icKeyInfo	√	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties	Identifier		- Color			
authorityKe	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualified
	regiuentinei	v				CA x public key
authorityInfo	oAccess	✓	False			
	AccessMethod	√				ld-ad-2
	accessLocation	√	1	1	1	http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓	+		1	Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu		✓	False			<u>nup.//qca.ocop.iu/urust.iu/</u>
CITEDISTIDU	distributionPoint	· ✓	1 0130		S	
	fullName	· ✓	1			http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	ame	\checkmark	False			

 $^{^{24}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{25}}$ CE = Critical Extension.

 $^{^{26}}$ O/M: O = Optional, M = Mandatory.

 $^{^{27}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

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



VERSION 1.25

			LuxTrust eID SSCD LCP Integration Signature Certificate Profile										
Attribute	Field	IN ²⁴	CE ²⁵	O/M ²⁶	CO ²⁷								
	Rfc822Name	~		0	D	specimen-x Subject's email address a provided by the RNCID							
subjectKey	Identifier	✓	False										
	keyldentifier	✓ 			Fixed	The Key Identifier comprises a four-bit fiel with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of th value or subjectPublicKey bit string (tag, no 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							
certificateP	olicies	\checkmark	False										
	Policyldentifier	\checkmark				1.3.171.1.1.10.3.16							
	policyQualifierID	\checkmark			S	Id-qt-1 (CPS)							
	qualifier	✓			S	https://repository.luxtrust.lu							
	policyQualifierID	✓			S	Id-qt-2 (User Notice)							
	noticeNumbers												
	DisplayText	~				LuxTrust INTEGRATION CERTIFICATE of eID SSCD compliant with ETSI TS 102 04: LCP certificate policy. Key Generation by CSF Sole Authorised Usage : Electronic signature for Integration Purposes.							
	Policyldentifier	√				0.4.0.1456.1.1							
QualifiedCe	ertificateStat												
	QcCompliance	✓		М	S	0.4.0.1862.1.1							
	QcLimitValue			0	D	As provided by LuxTrust S.A. in complianc with [3]							
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in complianc with [3]							

1.9.18 LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption

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

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

The usage purpose of these LuxTrust SSCD LCP+ Certificates is for the combined purpose of authentication and encryption for system integration. These Certificates include the corresponding LuxTrust SSCD LCP+ OID, i.e., **<OID 1.3.171.1.10.3.17>**.

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

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

The certificate re-key is not allowed.

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

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



	LuxTrust ell	D SSCI		ntegratio	n AE Ce	ertificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
SerialNumbe	r	~	False		501/	
signatureAlg	orithm	~	False		FDV	Validated on duplicates.
SignatureAig	algorithm	-	1 0130		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVal	ue	√	False		D	Issuing CA Signature.
issuer		~	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷
Validity	organizationName	\checkmark	Falas		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12
						Months;
						Certificate generation process date/time + 1 day for PSEUDONYM Certificate
subject		~	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
					-	
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	niven Neme		}		_	
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	~		М	D	specimen-x provided by the RNCID
	countryName	~		М	D	LU
	-					specimen-x Subject's email address as
	emailAddress	~		0	D	provided by the RNCID
	title	√		М	D	"Private Person"
					_	
	organizationalUnitName	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPublic	cKevInfo	✓	False			
	algorithm	~				Public Key: Key length: 2048 bit up to 4096bit
	subjectPublicKey	~		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified
authorityInfo	Access	✓	False			CA x public key
,	AccessMethod	~				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓ ✓	- ·			http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	ionPoint distributionPoint	✓ ✓	False		S	
	fullName	✓			0	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	me Rfc822Name	✓ ✓	False	0	D	specimen-x Subject's email address as
	RICOZZINAIIIE	ľ		0		provided by the RNCID
subjectKeyld		√	False	-		
	keyldentifier	~			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
Dellass						bit-string bits).
Policy Properties						
Policy Properties keyUsage		√	True			



VERSION 1.25

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

1.9.19 LuxTrust NCP+ Certificates supporting SEAL Signature Services

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

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

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a normalised certificate for Seal Signature purposes. These Certificates include the corresponding LuxTrust NCP+ OID, i.e., < OID 1.3.171.1.10.3.15>.

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

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



LuxTrust	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	countryName	~		М	D	Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	emailAddress	~		0	D	Subject's email address if available
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	localityName	~		М	D	Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	~		0	D	As provided by Subscriber
	organizationalUnitName 2	~		0	D	As provided by Subscriber
subjectPublicKeyInfo		✓	False			
	algorithm	\checkmark				Public Key: Key length: 2048 bit (RSA);
Extensions	subjectPublicKey	~		M		public exponent: Fermat-4 (=010001).
Authority Properties						
authorityKeyldentifier		✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global
authorityInfoAccess		✓	False			Qualified CA public key
uullontyillortoooo	AccessMethod	✓	1 0.00			ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	17
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties		 ✓ 				
subjectAltName	Rfc822Name	▼ ✓	False	0	D	Certificate Holder's email address
subjectKeyldentifier	RIGOZZINANIC	✓	False			
	keyldentifier	~			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	digitalSignature	\checkmark	True		S	True
		×				True
	nonRepudiation	✓			S S	True
	keyEncipherment	✓ ✓			S S	False
	dataEncipherment				5	False
certificatePolicies	Dellevides (10 - s	✓ ✓	False			
	Policyldentifier policyQualifierID	✓ ✓			S	1.3.171.1.1.10.3.15 Id-qt-1 (CPS)
	qualifier	✓ ✓			S	https://repository.luxtrust.lu
	policyQualifierID	· ✓	1		S	Id-qt-2 (User Notice)
	-					



VERSION 1.25

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

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

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

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

The usage purpose of these LuxTrust SSL/TLS Standard Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding LuxTrust LCP OID for SSL/TLS server certificates, i.e., <1.3.171.1.10.5.1>.

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

	LuxTrust SSL Server LCP Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg		✓	False		-					
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	✓	False							
					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	~			S	LuxTrust SSL CA x ¹⁷				
	organizationName	✓			S	LuxTrust S.A.				
Validity	-	✓	False							
	NotBefore	~			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 12;24;36 Months				
subject		✓	False							
	countryName	~		М	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	~		0	D					
	localityName	~		М	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	~		М	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	✓		0	D	As provided by Subscriber				



	LuxTrus	t SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	organizationalUnitName2	~		0	D	As provided by Subscriber
	commonName	~		М	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	~		0	D	Serial Number as provided by subscriber
	emailAddress	~		0	D	Subject's email address
subjectPubli	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	l /Identifier	✓	False			
<u></u>	keyldentifier	✓ 	_			SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo		✓ ✓	False			
	AccessMethod accessLocation	✓ ✓				Id-ad-1
	AccessMethod	· ·		-		http://ssl.ocsp.luxtrust.lu ²⁹ Id-ad-2
	accessLocation	▼ ✓				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
cRLDistribut		 ✓	False			nttp://ca.iuxtrust.iu/LISSLCAX .cn
UNEDISTINU	distributionPoint	√	1 0150		S	
	fullName	✓			-	http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.

²⁹ Since SSL CA 2



	LuxTrus	t SSL S	erver LC	P Certifi	cate Pr	ofile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0		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	✓		0		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	~		0		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	~		0		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	~		0		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	✓		0		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	✓		0		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	✓		0		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	~		0		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	~		0		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.
subjectKeylo	dentifier keyldentifier	✓ ✓	False			
	Keyldentiner	v			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 dataEncipherment	✓ ✓			S S	True True
					5	1140
certificatePo		✓ ✓	False			
	Policyldentifier policyQualifierID	✓ ✓			S	1.3.171.1.1.10.5.1 Id-qt-1 (CPS)
	qualifier	▼ ✓			S	https://repository.luxtrust.lu
	Policyldentifier	~			-	0.4.0.2042.1.3



VERSION 1.25

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

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

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

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

The usage purpose of these LuxTrust SSL/TLS Extended Validation Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust EVCP Server Certificates include the corresponding LuxTrust EVCP OID for SSL/TLS extended validation server certificates, i.e., <1.3.171.1.10.5.2>.

Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

Prohibited Certificate uses:

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

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

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

Verification of Applicant's Legal Existence and Identity:

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

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



VERSION 1.25

- i. Verify the Applicant's Legal Existence as stipulated in the EV Guidelines [13]);
- ii. Verify the Applicant's Entity name as stipulated in the EV Guidelines [13]);
- iii. Verify the Applicant's Registration Number as stipulated in the EV Guidelines [13]);

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

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

	SSL/TLS Exte	ended \	/alidatio	on Serv	er Cert	ificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
CarialNumba		~	False		S	Version 3 Value = "2"
SerialNumbe		•	Faise		FDV	Validated on duplicates.
signatureAlg	lorithm	√	False		TDV	Validated off duplicates.
Signatarerag	algorithm	-	1 0100		S	OID = "1.2.840.113549.1.1.11" -
					-	SHA256 with RSA Encryption.
signatureVal	lue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust SSL CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		√	False		_	
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 12;24 Months
subject		✓	False			
	countryName			М	D	Country in which the company's or
	(OID: 2.5.4.6)	~				institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	~		М	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)	~		М	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)
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	~		0	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)	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)



	SSL/TLS Ext	ended V	/alidatic	on Serv	er Cert	ificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	~		0	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)	~		М	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)	~		М	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	~		М	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	~		0	D	Number and Street of the physical location of the subject
subjectPublic		✓	False			
	algorithm subjectPublicKey	\checkmark		М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions Authority		•				
Properties						
authorityKeyl		✓ ✓	False			
authorityInfo	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo	Access AccessMethod	✓ ✓	raise			ld-ad-1
	accessLocation	▼ ✓				http://ssl.ocsp.luxtrust.lu ²⁹
	AccessMethod	· ✓				Id-ad-2
	accessLocation	✓ ✓				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
cRLDistributi		√	False			Intp://ca.iuxtrust.iu/ETSSECAX .cit
on a pionibuti	distributionPoint	· ✓	1 0100		S	
		✓	1		-	http://orl.luxtruct.lu/LTSSLCAv ¹⁷ orl
	fullName	v				I NUD.//CIT.IUXUUSU.IU/LISSLCAX .CI
Subject	fullName	•				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject Properties subjectAltNar		✓ ✓	False			



SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	SubjectAltName-dNSName			М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a			
						Web Server or IP address or unique			
		~				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		✓				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		✓				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		\checkmark				name of server, owned or controlled by			
						the subject and to be associated with the			
						Subject's server. Wildcard name not allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		~				name of server, owned or controlled by			
						the subject and to be associated with the			
						Subject's server. Wildcard name not allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		✓				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		✓				name of server, owned or controlled by			
						the subject and to be associated with the			
						Subject's server. Wildcard name not allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		~				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		~				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of			
						application/server – Exact DNS for a Web Server or IP address or unique			
		~				name of server, owned or controlled by			
						the subject and to be associated with the Subject's server. Wildcard name not			
						allowed for EV SSL Certificates.			
subjectKeyld	entifier	✓	False						



VERSION 1.25

SSL/TLS Extended Validation Server Certificates								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value		
	keyldentifier	~			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								
keyÜsage		✓	True					
	digitalSignature	~			S	True		
	nonRepudiation	~			S	False		
	keyEncipherment	~			S	True		
	dataEncipherment	~			S	True		
certificatePo	licies	√	False					
	Policyldentifier	✓				1.3.171.1.1.10.5.2		
	policyQualifierID	\checkmark			S	ld-qt-1 (CPS)		
	qualifier	\checkmark			S	https://repository.luxtrust.lu		
	Policyldentifier	\checkmark				0.4.0.2042.1.4		
	Policyldentifier	✓				2.23.140.1.1		
Extended Ke	ey Usage	~	False					
	serverAuth	\checkmark			S	True		
	clientAuth	✓			S	True		
	emailProtection	\checkmark			S	False		

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

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

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

The usage purpose of these LuxTrust SSL/TLS Extended Validation+ Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust EVCP+ Certificates include the corresponding LuxTrust EVCP+ OID for SSL/TLS extended validation+ server certificates, i.e., <1.3.171.1.10.5.3>.

Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

Prohibited Certificate uses:



VERSION 1.25

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

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

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

Verification of Applicant's Legal Existence and Identity:

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

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

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

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

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

Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" -
						SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		\checkmark	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust SSL CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	✓			D	
	NotAfter	v			D	Certificate generation process date/time + 12;24 Months
Subject		\checkmark	False			
	countryName			М	D	Country in which the company's or
	(OID: 2.5.4.6)				_	institution's registered office is
	(010. 2.3.4.0)	✓				established (as specified in the
						memorandum and articles of
						association). (ISO3166)



	SSL/TLS Extended Validation Server Certificates on Secure User Device					
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	¥		М	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)	~		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	¥		0	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)	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	~		0	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)	~		М	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)	~		М	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity



	SSL/TLS Extended Validation	n Serve	er Certif	icates	on Sec	ure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	serialNumber (OID: 2.5.4.5)	×		M	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration Agency in its Jurisdiction of Incorporation or Registration Agency in its Jurisdiction of Incorporation or Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	~		0	D	Number and Street of the physical location of the subject
subjectPublic	cKeyInfo	✓	False			
	Algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo	Access AccessMethod	✓ ✓	False			ld-ad-1
	accessLocation	✓ ✓				20
	AccessMethod	~				http://ssl.ocsp.luxtrust.lu
	accessLocation	· ✓				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
cRLDistribut		✓	False			http://da.iuxitust.iu/ETOSEOAX .CIT
	distributionPoint	~			S	
	fullName	~				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject						
Properties subjectAltNa	me	✓	False			
	SubjectAltName-dNSName	×		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.



	SSL/TLS Extended Validation	n Serve	er Certif	icates	on Sec	ure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be
						associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	V		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	¥		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
subjectKeylo		 ✓ 	False			
	keyldentifier	✓ 			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).



VERSION 1.25

	SSL/TLS Extended Validati	on Serve	er Certi	ficates	on Sec	ure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Policy Properties						
keyUsage		✓	True			
	digitalSignature	~			S	True
	nonRepudiation	~			S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePol	licies	✓	False			
-	Policyldentifier	✓				1.3.171.1.1.10.5.3
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	✓				0.4.0.2042.1.5
Extended Ke	Extended Key Usage		False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

1.9.23 LuxTrust Object (or Code) Signing Certificates

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

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

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., <1.3.171.1.10.5.4>. This profile is not currently implemented.

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

	LuxTrust LCP Code Signing Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
Base Prof	Base Profile									
Version		~	False							
					s	Version 3 Value = "2"				
SerialNum	nber	~	False							
					FDV	Validated on duplicates.				
signature	Algorithm	~	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signature	Value	~	False							
					D	Issuing CA Signature.				
Issuer		~	False		s					
	countryName	~			s	LU				
	commonName	\checkmark			S	LuxTrust SSL CA x ¹⁷				
	organizationName	~			s	LuxTrust S.A.				
Validity		~	False							
	NotBefore	~			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 12; 24; 36 months				



	l	_uxTrust	LCP Code	Signing C	ertificate P	Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Subject		✓	False			
	countryName	~		М	D	Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	~		0	D	
	localityName	~		М	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	V		М	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	✓		0	D	As provided by Subscriber
	organizationalUnitName2	~		0	D	As provided by Subscriber
	commonName	V		М	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	~		0	D	NA or Serial Number as provided by subscriber
	emailAddress	✓		0	D	Subject's email address if available
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extension						
	Properties					
authorityK	Keyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust SSL CA public key
authorityli	nfoAccess	✓	False			
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu ²⁹
	AccessMethod	✓				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
CRLDistri	butionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject Pr	roperties	1		1		· · · · · · · · · · · · · · · · · · ·
subjectAlt	Name	✓	False			
	Rfc822Name	~		0	D	Subject's email address
subjectKe	yldentifier	✓	False			
	keyldentifier	~			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 Pro	perties					



VERSION 1.25

	LuxTrust LCP Code Signing Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
keyUsage		~	True								
	digitalSignature	~			S	True					
	nonRepudiation	~			S	False					
	keyEncipherment	~			S	False					
	dataEncipherment	~			s	False					
certificate	Policies	~	False								
	Policyldentifier	~			s	1.3.171.1.1.10.5.4					
	policyQualifierID	~			s	ld-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 <u>http://repository.luxtrust.lu</u> . Signed by an SSL CA.					
	Policyldentifier	~			S	0.4.0.2042.1.3					
Extended	Key Usage	✓	False								
	Object Signing	✓			s	Set					

1.9.24 LuxTrust SSL/TLS Certificate for Client Authentication

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

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

The usage purpose of these LuxTrust SSL/TLS Client Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding LuxTrust LCP OID for SSL/TLS client certificates, i.e., <1.3.171.1.10.5.5>.

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

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



	LuxTrus	st SSL	Client L	CP Cert	tificate I	Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	countryName	~		М	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	✓		0	D	
	localityName	~		М	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	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	~		0	D	As provided by Subscriber
	organizationalUnitName 2	~		0	D	As provided by Subscriber
	commonName	~		М	D	As provided by Subscriber
	serialNumber	✓		0	D	Serial Number as provided by subscriber
	emailAddress	~		0	D	Subject's email address
subjectPubli		✓	False			
	Algorithm subjectPublicKey	✓ ✓	-	М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	Subjecti ublicitey			101		
Authority Properties			- Falsa			
authorityKey	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo		✓ ✓	False			
	AccessMethod accessLocation	✓ ✓				Id-ad-1 http://ssl.ocsp.luxtrust.lu ²⁹
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
cRLDistribut	ionPoint distributionPoint	✓ ✓	False		S	
	fullName	~			0	http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	me Rfc822Name	✓	False	0	D	Certificate Holder's email address
aubication		✓ ✓	E-la -	0		
subjectKeyld	keyldentifier	v v	False		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			- T			
keyUsage	digitalSignature	✓ ✓	True		S	True
	nonRepudiation	✓			S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo	licies Policyldentifier	✓ ✓	False			1.3.171.1.1.10.5.5
	policyQualifierID	✓ ✓	1		S	Id-qt-1 (CPS)



VERSION 1.25

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

1.9.25 SSL/TLS QCP-w Extended Validation Server Certificates

QCP-w: certificate policy for European Union (EU) qualified website authentication certificates, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key encryption as well as extended key usage for server and client authentication. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.5.6>.

Attribute	Field	IN ¹³		O/M ¹⁵	CO ¹⁶	Value
Base	11010			0,111		, Tuldo
Profile						
Version		√	False			
					S	Version 3 Value = "2"
SerialNumbe	er	~	False			
					FDV	Validated on duplicates.
signatureAlg		~	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust SSL CA x ¹⁷
	organizationName	~			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time
	NotAfter	✓			D	Certificate generation process date/tim + 12;24 Months
subject		✓	False			
countryName (OID: 2.5.4.6)	-	V		М	D	Country in which the company's constitution's registered office is established (as specified in the memorandum and articles constructed association). (ISO3166)
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	*		М	D	Contains the country informatio specified using the applicable ISC country code for the jurisdiction of Incorporation for the Incorporatin Agency or Jurisdiction of Registration for a Registration Agency that operates a the country level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	*		М	D	State or Province in which th company's registered office i established (as specified in th memorandum and articles of associatio or an equivalent document)
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	~		0	D	Contains the jurisdiction for th applicable Incorporating Agency of Registration Agency at the state of province level MUST include bot country and state or province information,
	localityName (2.5.4.7)	✓		М	D	Location in which the company registered office is established (a specified in the memorandum an articles of association or an equivaler document)



	SSL/TLS QCP-w	Extend	ed Valio	lation S	Server (Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	V		0	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)	✓		М	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)	~		М	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	~		М	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	~		0	D	Number and Street of the physical location of the subject
subjectPublic		✓ ✓	False			Public Key: Key length: 2048 bit (RSA);
	algorithm subjectPublicKey	✓ ✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey		✓	False			
authorityInfo	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust SSL CA public key
autionityinfo	Access AccessMethod	✓ ✓	i aise			ld-ad-1
	accessLocation	· ✓				http://ssl.ocsp.luxtrust.lu ²⁹
	AccessMethod	✓				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt
cRLDistribut	ionPoint	√	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject						
Properties			Felsi			
subjectAltNa	me	~	False			



	SSL/TLS QCP-w	Extend	ed Valic	ation S	Server (Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName	~		М		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
	SubjectAltName-dNSName			0		the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates. FQDN (Fully Qualified Domain Name) of
		V				application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	¥		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyld	entifier	✓	False			



VERSION 1.25

	SSL/TLS QCP-	w Extend	led Valio	lation S	Server (Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	keyldentifier	V			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	1	✓	True			
	digitalSignature	~			S	True
	nonRepudiation	~			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	~			S	False
certificatePo		~	False			
	Policyldentifier	~				1.3.171.1.1.10.5.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	~				0.4.0.194112.1.4
	Policyldentifier	~				0.4.0.2042.1.4
	Policyldentifier	~			S	2.23.140.1.1
Extended Ke	y Usage	~	False			
	serverAuth	\checkmark			S	True
	clientAuth	✓			S	True
	emailProtection	\checkmark			S	False
QualifiedCer		~	False			
	QcCompliance (0.4.0.1862.1.1)	~		М	S	True
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repos itory/PDS.pdf
	QcType (0.4.0.1862.1.6)	√		М	S	id-etsi-qct-web (0.4.0.1862.1.6.3)

1.9.26 LuxTrust SPARE Signing Server LCP Certificate Profile

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

These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]). The usage purpose of these Certificates is only authentication <OID 1.3.171.1.1.0.3.20>.

The LuxTrust SPARE Signing Server LCP Certificate Profile include the corresponding SPARE Signing Server LCP Certificate, i.e., <1.3.171.1.1.10.3.20>.

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



Attribute	Field	IN ¹⁸	CE ¹⁹	O/M ²⁰	CO ²¹	Value
					FDV	Validated on duplicates.
signatureAlg	orithm		False			
SignatureAig			1 0130			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.
signatureVal	ue		False			
	Т				D	Issuing CA Signature.
					D	issuing CA Signature.
Issuer			False		S	
	countryName				S	LU
	commonName				S	LuxTrust Global Qualified CA x
	organizationName				S	LuxTrust S.A.
	organizationname				3	
Validity			False			
	NotBefore				D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time
						36 Months
Subject			False			
	serialNumber			М	D	Serial Number as constructed by LRAO
	commonName				D	LGQCA XX CSS (XX a number selected internally by LuxTrust) or Concatenation of
	commonname			М		given name(s) and surname(s) separated b a "Space" character.
	givenName			м	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s
	gitterinterine					as on ID document
	Surname			м	D	CSS or Surname(s) as on ID documer without indication "épouse", "ép." or simila
	ourname					and the subsequent name(s)
	countryName			М	D	LU or Nationality of holder (ISO3166)
	emailAddress			0	D	N/A
	Title			М	D	Private Person
cubicat Dub!			Folor			
subjectPublic	-		False			
	Algorithm					Public Key: Key length: 2048 bit (RSA) public exponent: Fermat-4 (=010001).
	subjectPublicKey			М		-
Extensions						



	SPA	RE LuxTru	st Signin	g Server L	.CP Certifi	cate Profile
Attribute	Field	IN ¹⁸	CE ¹⁹	O/M ²⁰	CO ²¹	Value
Authority Properties						
authorityKeyl	dentifier		False			
	keyldentifier					SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access		False			
	AccessMethod					ld-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx ²² .crt
	AccessMethod					ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/23
cRLDistributi	onPoint		False			
	distributionPoint				S	
	fullName					http://crl.luxtrust.lu/LTGQCAx ²² .crl
Subject Properties						
subjectAltNa	ne		False			
	Rfc822Name			0	D	N/A
subjectKeyId	entifier		False			
	keyldentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, no including the length and number of unused bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
certificatePol	icies		False			
	Policyldentifier					1.3.171.1.1.10.3.20
	policyQualifierID				S	Id-qt-1 (CPS)
	Qualifier				S	https://repository.luxtrust.lu
	Policyldentifier					0.4.0.2042.1.3



VERSION 1.25

1.9.27 LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature

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

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

	LuxTrust Qualified eSEAL Certificate Profile											
Attribute	Field	IN ³⁰	CE ³¹	O/M ³²	CO ³³	Value						
Base Profile												
Version		\checkmark	False									
					S	Version 3 Value = "2"						
SerialNumbe	er	✓	False									
					FDV	Validated on duplicates.						
signatureAlg	jorithm	✓	False									
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.						
signatureVal	ue	✓	False									
					D	Issuing CA Signature.						
Issuer	•	√	False		S							
	countryName	✓			S	LU						
	commonName	✓			S	LuxTrust Global Qualified CA x ³⁴						

Certificates is limited to sole authorised usage of supporting the creation of qualified eseals supported by Qualified Certificate compliant with ETSI EN 319 411-2 [20] QCP-I-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.21>.

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

 $^{^{30}}$ IN = Included: Attribute / field included within the certify

cate profile.

 $^{^{31}\,\}mathrm{CE}$ = Critical Extension.

³² O/M: O = Optional, M = Mandatory.

 $^{^{33}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $^{^{34}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	organizationName	✓			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	\checkmark			D	Certificate generation process date/time.
	NotAfter	\checkmark			D	Certificate generation process date/time + 24 Months
Subject		\checkmark	False			
	commonName	\checkmark		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	✓		М	D	 Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		Ο	D	Company/institution department or other information item
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
subjectPubl	icKeyInfo	\checkmark	False			
-	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	✓		М	1	public exponent: Fermat-4 (=010001).
Extensions	,,					
Authority						
Properties						
authorityKe	vldentifier	✓	False			
autiontyne	keyldentifier	• ✓	raise			SHA-1 Hash of the LuxTrust Global Qualified CA public
authorityInf	0400055	✓	Folos			key
autiontyint			False			Id ad 2
	AccessMethod	-				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	√	L			http://qca.ocsp.luxtrust.lu/ ³⁵
cRLDistribu		√	False			
	distributionPoint	\checkmark			S	

³⁵ SINCE LTGQCA3



VERSION 1.25

	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject						
Properties						
subjectKeylo		√	False			
	keyldentifier	~			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	\checkmark			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	\checkmark			S	False
certificatePo		✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.21
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.194112.1.3
QualifiedCer	tificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	~		Μ	S	True
	QcSSCD (0.4.0.1862.1.4)	~		Μ	S	True
	QcPDS (0.4.0.1862.1.5)	~		Μ	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	~		Μ	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

1.9.28 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

Keys are generated on Secure User Device, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eseals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.22>.



	LuxTrust NCP+ Certificate Profile for authentication										
Attribute Field IN ³⁶ CE ³⁷ O/M ³⁸ CO ³⁹ Value											
Base											
Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								

 $^{^{36}}$ IN = Included: Attribute / field included within the certify cate profile.

 $^{^{37}}$ CE = Critical Extension.

 $^{^{38}}$ O/M: O = Optional, M = Mandatory.

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



					FDV	Validated on duplicates.
signatureAl		\checkmark	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	√	False			
-					D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	√			S	LU
	commonName	\checkmark			S	LuxTrust Global Qualified CA x ⁴⁰
	organizationName	\checkmark			S	LuxTrust S.A.
Validity		\checkmark	False			
	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	~		М	D	 Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: "VAT" for identification based on a national value added tax identification number. "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPub	licKeyInfo	\checkmark	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	√		М		public exponent: Fermat-4 (=010001).
Extensions				141		
Authority Properties			- ·			
authorityKe	yldentifier	✓	False			

 $^{^{40}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	oAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/41
cRLDistribu	tionPoint	✓	False			
				vanced e	SEAL C	Certificate Profile
Attribute	Field	IN ⁴²		O/M ⁴⁴	CO ⁴⁵	Value
Base Profile						
Version		✓	False			
	Reyldentiner				Ś	Version 3 Value = the least significant 60 bits of the SHA-
						1 hash of the value or subjectPublicKey bit string (tag, not
						including the length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		√	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePo	olicies	✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.22
	policyQualifierID	✓			S	Id-gt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

1.9.29 LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature

This profile aims at issuing advanced electronic eSeals. The usage purpose of these Certificates is limited to the creation of advanced eseals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Keys are generated on QSCD, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.23>.

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

⁴⁴ O/M: O = Optional, M = Mandatory.

⁴¹ SINCE LTGQCA3

cate profile.

 $^{^{43}}$ CE = Critical Extension.

 $^{^{45}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

VERSION 1.25



SerialNumbe	<u>a</u> r	✓	False			
oonantanibe			1 0150		FDV	Validated on duplicates.
signatureAlg	orithm	√	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	ue	√	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	~			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁴⁶
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
-	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	✓		М	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPubli	cKeyInfo	√	False			
	Algorithm	√				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	√		М	1	public exponent: Fermat-4 (= 010001).
Extensions				IVI		
Authority Properties						

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



VERSION 1.25

	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public
	hoylaonnoi					key
authorityInf	oAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/47
cRLDistribu	ıtionPoint	✓	False			
		LuxT	rust Adv	vanced e	SEAL C	Certificate Profile
Attribute	Field	IN ⁴⁸	CE ⁴⁹	O/M ⁵⁰	CO ⁵¹	Value
Base Profile						
Version		✓	False			
	Regidentinei				Ś	Valsion of Value by the least significant 60 bits of the SHA-
SerialNumb	er	✓	False			ו המסור סו נווס זמומס סו סמסוסטו מסווסונסץ את סנווווק (נמק, ווסר
						including the length and number of unused bit-string bits).
Policy Properties						
keyÜsage	·	✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	~			S	False
certificateP	olicies	✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.23
	policyQualifierID	✓	1		S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.2042.1.2

1.9.30 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

LuxTrust Certificates for Advanced Seal Signature Services are Advanced Certificates certified with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eseals supported by Advanced Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.24>. The following table provides the description of the fields for LuxTrust Advanced Certificates for authentication purpose.

 48 IN = Included: Attribute / field included within the certify

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

⁴⁷ SINCE LTGQCA3

cate profile.

 $^{^{49}}$ CE = Critical Extension.

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



					FDV	Validated on duplicates.
signatureAlg		\checkmark	False			
·	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	\checkmark	False			
·					D	Issuing CA Signature.
Issuer		\checkmark	False		S	
	countryName	\checkmark			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x ⁵²
	organizationName	~			S	LuxTrust S.A.
Validity	· =	✓	False			
č	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	~	1 0.00	М	D	Shall contain the full registered name of the subject (legal person).
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	~		М	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPubli	icKeyInfo	✓	False			
-	Algorithm	√				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	✓		М	1	public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties	d de se tiller					
authorityKey	ldentifier	\checkmark	False			

 $^{^{52}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	keyldentifier	1	<u> </u>			SHA-1 Hash of the LuxTrust Global Qualified CA public
	Regidentinei	•				kev
authorityInf	oAccess	✓	False			
j	AccessMethod	√				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	√				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/53
cRLDistribu	tionPoint	✓	False			
	Lu	xTrust A	dvance	d Autom	ated eS	EAL Certificate Profile
Attribute	Field	IN ⁵⁴	CE ⁵⁵	O/M ⁵⁶	CO ⁵⁷	Value
Base Profile				-		
Version	Keyldentinei	✓	False		I IXEU	
						value, followed by the least significant 60 bits of the SHA- 1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	√			S	True
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.24
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

1.9.31 LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature

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

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

 54 IN = Included: Attribute / field included within the certify

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

⁵³ SINCE LTGQCA3

cate profile.

 $^{^{55}}$ CE = Critical Extension.

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



					S	Version 3 Value = "2"
SerialNum	ber	✓	False			
					FDV	Validated on duplicates.
signatureA		\checkmark	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RS
						Encryption.
signatureV	alue	\checkmark	False		-	
		1			D	Issuing CA Signature.
Issuer	1	✓	False		S	
	countryName	✓			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x ⁵⁸
	organizationName	✓			S	LuxTrust S.A.
Validity		\checkmark	False			
	NotBefore	\checkmark			D	Certificate generation process date/time.
	NotAfter	\checkmark			D	Certificate generation process date/time + 24 Months
Subject		~	False			
	commonName	~		М	D	Shall contain the full registered name of the subject (lega
				101		person).
	countryName	~		М	D	the country in which the subject (legal person) established (ISO3166)
	organisationIdentifier (2.5.4.97)	~		М	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that i considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	~		М	D	Shall contain the full registered name of the subject (lega person).
	organizationalUnitName	✓		Ο	D	Company/institution department or other information item
subjectPub	licKeyInfo	√	False			
	Algorithm	√				Public Key: Key length: 2048bit up to 4096bit (RSA
	subjectPublicKey	√		М	1	public exponent: Fermat-4 (=010001).
Extensions	,				1	
Authority						
Properties	eyldentifier	√	Falsa			
	Synachunici	v	False			
autiontyra	keyldentifier	\checkmark				SHA-1 Hash of the LuxTrust Global Qualified CA publ

 $^{^{58}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

authorityInfo	oAccess	✓	False		
	AccessMethod	✓			ld-ad-2
	accessLocation	✓			http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓			ld-ad-1
	accessLocation	✓			http://qca.ocsp.luxtrust.lu/ ⁵⁹
cRLDistribu	tionPoint	✓	False		
	distributionPoint	✓		S	
	fullName	✓			http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties					
subjectKeyl		\checkmark	False		
	keyldentifier	~		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
certificatePo		✓	False		
	Policyldentifier	~			1.3.171.1.1.10.3.25
	policyQualifierID	✓		S	Id-qt-1 (CPS)
	qualifier	✓		S	https://repository.luxtrust.lu
	policyQualifierID	✓		S	Id-qt-2 (User Notice)
	Policyldentifier	✓			0.4.0.2042.1.2

1.9.32 LuxTrust Smart Card QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.26>.

⁵⁹ SINCE LTGQCA3



Attribute	Field	IN ⁶⁰	CE ⁶¹		-	Iscd Certificate Profile Value
Allinbule	Field	IN	CE	O/M ⁶²	CO 63	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False			
signature	Algorithm	✓	False		FDV	Validated on duplicates.
signature	Algorithm	•	1 8136		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RS/
					Ū.	Encryption.
signature	Value	✓	False			
					D	Issuing CA Signature.
ssuer	a a contro Al a ma a	\checkmark	False		S	
	countryName commonName	✓ ✓			S S	
						LuxTrust Global Qualified CA x ⁶⁴
1-1:4:4.4	organizationName	\checkmark	Falsa		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Certificate generation process date/time.
	NotAfter	• •			D	Certificate generation process date/time.
Subject	NOLAILEI	· ·	False		0	Certificate generation process date/time + 30 Month's
	serialNumber	~	1 0.00	м	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of give name(s) and surname(s) as on ID card separated by "Space" character.
	givenName	~		м	D	PRO and PRIVATE products : Given name(s) as on li card
	surname	~		м	D	PRO and PRIVATE products : Surname(s) as on la card without indication "épouse", "ép." or similar and th subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		М	D	Subject's email address
	title	*		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		м	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including th legal form.
	localityName	~		м	D	PRO products only : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	¥		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).

 $^{^{60}\,\}mathrm{IN}$ = Included: Attribute / field included within the certificate profile.

 $^{^{61}}$ CE = Critical Extension.

 $^{^{62}}$ O/M: O = Optional, M = Mandatory.

 $^{^{63}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $^{^{64}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	Luz					ascd Certificate Profile
Attribute	Field	IN ⁶⁰	CE ⁶¹	O/M ⁶²	CO 63	Value
						PRO products only:
	organizationalUnit	~		0	D	Company/institution department or other information
	Name 2			Ŭ	D	item
subjectPu	blicKeyInfo	√	False			
	Algorithm	√				Public Key: Key length: 2048bit (RSA); public exponent
	subjectPublicKey	~		М		Fermat-4 (=010001).
Extensio						
ns Authorit						
y Properti						
es						
	eyldentifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authoritylr		\checkmark	False			
	AccessMethod	~				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓	İ	İ		Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ⁶⁵
cRLDistrik	outionPoint	\checkmark	False			
ONEDIOUN	distributionPoint	~	1 0.00		S	
	fullName	√			-	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properti es						
subjectAlt	Name	✓	False			
•	Rfc822Name	√		0	D	Certificate Holder's email address
subjectKe	yldentifier	✓	False			
-	keyldentifier	✓			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
Dellara						string bits).
Policy						
Properti						
es keyUsage		✓	True			
ReyUsage	digitalSignature	· •	nue		S	False
	nonRepudiation	v √			S	True
	keyEncipherment	· •			S	False
	dataEncipherment	✓			S	False
certificate		√	False			
	Policyldentifier	✓	. 0.00			1.3.171.1.1.10.3.26
	policyQualifierI	✓	1	1	S	Id-qt-1 (CPS)
	D				_	
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				
						0.4.0.194112.1.2
QualifiedC	ertificateStat	✓	False			-
	QcCompliance	\checkmark		M	S	True
	(0.4.0.1862.1.1)					
	QcSSCD			М	S	True
	(0.4.0.1862.1.4)					
	QcPDS	\checkmark		М	S	https://www.luxtrust.lu/upload/data/repository/PD
	(0.4.0.1862.1.5)					S.pdf
	QcType	✓		М	S	id-etsi-qct-esign
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-esign

⁶⁵ SINCE LTGQCA3



VERSION 1.25

1.9.33 LuxTrust Smart Card NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.27>.

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

 $^{^{66}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{67}}$ CE = Critical Extension.

⁶⁸ O/M: O = Optional, M = Mandatory.

 $^{^{69}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $^{^{70}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	LuxTrust Smart Card NCP+ Certificate Profile												
Attribute	Field	IN 66	CE ⁶⁷	O/M ⁶⁸	CO ₆₉	Value							
	organizationalUnit Name 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).							
	organizationalUnit Name 2	~		0	D	PRO products only: Company/institution department or other information item							
subjectPul	blicKeyInfo	✓	False										
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public							
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).							
Extensio ns													
Authorit y Properti es													
authorityK	eyldentifier	✓	False										
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key							
authorityIn		√	False										
	AccessMethod	✓				Id-ad-2							
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt							
	AccessMethod	✓				ld-ad-1							
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/1							
cRLDistrib	outionPoint	✓	False										
	distributionPoint	√			S								
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl							
Subject Properti es													
subjectAlt	Name	✓	False										
	Rfc822Name	√		0	D	Certificate Holder's email address							
subjectKe		√	False										
Policy	keyldentifier	✓ 			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).							
Properti es			_										
keyUsage	11 1/ 1/61	✓	True			-							
	digitalSignature	✓ ✓			S								
	nonRepudiation	✓ ✓			S	False							
	keyEncipherment dataEncipherment	✓ ✓			S	True False							
certificate		✓ ✓	False		S								
Certificater	Policyldentifier	▼ ✓	1 2150			1.3.171.1.1.10.3.27							
	policyQualifierID	▼ ✓			S	Id-qt-1 (CPS)							
	gualifier	· •			S	https://repository.luxtrust.lu							
	policyQualifierID	· •			S	Id-qt-2 (User Notice)							
	Policyldentifier	✓			5								
	. Shoylaontinoi					0.4.0.2042.1.2							

1.9.34 LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature

⁷¹ SINCE LTGQCA3



VERSION 1.25

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

These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.0.3.28>.

	LuxTrust Sr	nart C	ard LOF		⊦ - Sign	ature Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base				0/101		Value
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	\checkmark	False			
	L				FDV	Validated on duplicates.
signatureAl		√	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa		~	False			
Signature ve			1 0.00		D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity	· • •	✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
						on in card separated by a space character.
	givenName	✓		М	D	Given name(s) as on ID card
						Surname(s) as on ID card without indication
	Surname	~		м	D	"épouse", "ép." or similar and the subsequent
	Gurname	•		IVI		name(s)
						17
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	~		М	D	Constructed by LuxTrust
	organizationitanie			IVI		
					_	
	localityName	~		М	D	Country of RA
	organizationalUnitNam	~		м	D	RA code Constructed by LuxTrust
	e 1	•		IVI		TA code constructed by Eux Trast
	organizationalUnitNam					
	e 2	✓		M	D	RAO code Constructed by LuxTrust
subjectBuck		✓	False			
subjectPub	Algorithm	✓ ✓	Faise			Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	▼ ✓		М		exponent: Fermat-4 (=010001).
Extension	Subject unioney			IVI		
S						
Authority						
Properties						
authorityKe		~	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInf		√	False			
	AccessMethod	 ✓ 				Id-ad-2 17
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	\checkmark				Id-ad-1



VERSION 1.25

	LuxTrust S	mart C	ard LOF		⊦ - Sign	ature Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu	itionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltN		~	False			
	Rfc822Name	√		0	D	Certificate Holder's email address
subjectKeyl		✓	False			
	keyldentifier	~			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
certificateP		√	False			
	Policyldentifier	√				1.3.171.1.1.10.3.28
	policyQualifierID	√			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.2042.1.2

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

LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.29>.

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



VERSION 1.25

	LuxTrust Sma	rt Ca	rd LOR	A NCP+	- authent	tication Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"LuxTrust RA Officer"
	organizationName	~		М	D	Constructed by LuxTrust
	localityName	~		М	D	Country of RA
	organizationalUnitNam e 1	~		М	D	RA code Constructed by LuxTrust
	organizationalUnitNam e 2	~		М	D	RAO code Constructed by LuxTrust
subjectPubl		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
F	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Extension s						
Authority Properties						
authorityKe	yldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		√	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu		\checkmark	False			
	distributionPoint fullName	▼ ✓			S	17
Subject Properties	Tuinvaine	•				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
subjectAltNa	ame	√	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyl		✓	False			
	keyldentifier	~			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
certificatePo	dataEncipherment	√ √	Folor		S	False
certificatePC	Policyldentifier	\checkmark	False			1.3.171.1.1.10.3.29
	policyQualifierID	▼ ✓			S	Id-qt-1 (CPS)
	Qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.2042.1.2

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

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



VERSION 1.25

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

	LuxTrus					cd Certificate Profile
Attribute	Field	IN ⁷²	CE ⁷³	O/M 74	CO ⁷⁵	Value
Base Profile						
Version		 ✓ 	False			
VC131011		-	T disc		S	Version 3 Value = "2"
SerialNumb	ber	✓	False		-	
					FDV	Validated on duplicates.
signatureAl		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RS/ Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer	1	✓	False		S	
	countryName	 ✓ 			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁷⁶
	organizationName	✓	L		S	LuxTrust S.A.
Validity		 ✓ 	False		-	
	NotBefore	✓ ✓			D	Certificate generation process date/time.
	NotAfter	v			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day fo PSEUDONYM Certificate
Subject		√	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		м	D	Concatenation of given name(s) and surname(s separated by the space character
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse" "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	~		М	D	LU
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"Private Person"
	organizationalUnitName	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date o birth + 18 years).
subjectPub		✓	False			
	Algorithm	 ✓ 				Public Key: Key length: 2048bit up to 4096bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extension s						
Authority Properties						
authorityKe	vldentifier	✓	False			
_	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA : public key
authorityInf	oAccess	✓	False			
.,	AccessMethod	✓				Id-ad-2
	accessLocation	✓	İ			http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓		1		http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu		✓	False			
C. LEIGHIDU	distributionPoint	· ·	1 4.00		S	

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

⁷³ CE = Critical Extension.

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

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

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



VERSION 1.25

Policy value, followed by the least significant 60 bits of th Second String value, followed by the least significant 60 bits of th Properties value, followed by the least significant 60 bits of th Properties value, followed by the least significant 60 bits of th KeyUsage value, followed by the least significant 60 bits of th digitalSignature value, followed by the least significant 60 bits of th keyUsage value, followed by the least significant 60 bits of th digitalSignature value, followed by the least significant 60 bits of th keyEncipherment value, followed by the least significant 60 bits of the value or subjectPublicKey bit string bits). certificatePolicies value, followed by the least significant 60 bits of the value or subjectPublicKey bit string bits). certificatePolicies value, followed by the least significant 60 bits of the value or subjectPublicKey bit string bits). policyQualifierID value S qcCompliance value M S qualifiedCertificateStat		LuxTru	st elD	Smart C	ard Q(CP-n-qs	cd Certificate Profile
Subject Properties ✓ False ✓ subjectAltName ✓ False ✓ O D Subject email address subjectKeyldentifier ✓ False ✓ O D Subject email address keyldentifier ✓ False ✓ The Key Identifier comprises a four-bit field with a 010 value, followed by the least significant 60 bits of the stude or subject/bublicKey bit stir (tag, not including the length and number of unused bits, string bits). Policy Properties ✓ S False keyUsage ✓ True ✓ S False digitalSignature ✓ S False ✓ S False certificatePolicies ✓ S False ✓ S False certificatePolicies ✓ False ✓ S Id-qt-1 (CPS) O QualifierD ✓ S Id-qt-1 (CPS) O <	Attribute	Field	IN ⁷²	CE ⁷³	O/M 74	CO ⁷⁵	Value
Subject Properties ✓ False ✓ subjectAltName ✓ False ✓ O D Subject email address subjectKeyldentifier ✓ False ✓ O D Subject email address keyldentifier ✓ False ✓ The Key Identifier comprises a four-bit field with a 010 value, followed by the least significant 60 bits of th SHL, on the or subject/bublicKey bit stir (tag, not including the length and number of unused bits). Policy Properties ✓ S False keyUsage ✓ True ✓ S False digitalSignature ✓ ✓ S False ✓ dataEncipherment ✓ S False ✓ S False certificatePolicies ✓ False ✓ S Id-qt-1 (CPS) QualifierID ✓ S Id-qt-2 (User Notice) ✓ policyQualifierID ✓ S Id-qt-2 (User Notice) ✓ O.4.0.194112.1.2 QualifierCertificateStat ✓ False ✓ O.4.0.194112.1.2 O.4.0.1862.1.4) Qcopplance		fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Rtc822Name ✓ O D Subject email address subjectKeyldentifier ✓ False Fixed The Key Identifier comprises a four-bit field with a 010 value, followed by the least significant 60 bits of th SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused b) string bits). Policy ✓ True S False digitalSignature ✓ ✓ S False digitalSignature ✓ S False S dataEncipherment ✓ S False S dataEncipherment ✓ S False S PolicyUsualifierID ✓ S Its:/repository.luxtrust.lu policyQualifierID ✓ S Its:/repository.luxtrust.lu QualifiedCertificateStat ✓ False S QualifiedCertificateStat ✓ False<							
subject Keyldentifier ✓ False ✓ False ✓ subject Keyldentifier ✓ False ✓ The Key Identifier comprises a four-bit field with a 010 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit stirr (tag, not including the length and number of unused bits string bits). Policy ✓ True ✓ S False ✓ keyUsage ✓ True S False ✓ S False digitalSignature ✓ ✓ S False ✓ S False digitalSignature ✓ ✓ S False ✓ S False digitalSignature ✓ ✓ S False ✓ S False certificatePolicies ✓ S False ✓ S False ✓ Qualifier ✓ S Id-qt-1 (CPS) ✓ Outalifier ✓ S Id-qt-2 (User Notice) PolicyUdentifier ✓ S Id-qt-2 (User Notice) ✓ O.4.0.194112.1.2 OutalifiedCertificateStat ✓ False ✓	subjectAltNa	ame	✓	False			
keyldentifier ✓ Fixed The Key Identifier comprises a four-bit field with a 010 value, followed by the least significant 60 bits of th SHA-1 hash of the value or subjectPublicKey bit string tag, not including the length and number of unused bits of the value or subjectPublicKey bit string the value or subjectPublicKey bit string bits). Policy ✓ True S False digitalSignature ✓ True S False digitalSignature ✓ S False S digitalSignature ✓ S False S dataEncipherment ✓ S False S certificatePolicies ✓ False S Id-qt-1 (CPS) Qualifier ✓ S Id-qt-2 (User Notice) S policyQualifierID ✓ S Id-qt-2 (User Notice) S policyQualifierID ✓ S Id-qt-2 (User Notice) S policyQualifierID ✓ M S True QualifiedCertificateStat ✓ False S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False S Id-qt-2 (User Notice) QcACompliance		Rfc822Name	✓		0	D	Subject email address
Note Note	subjectKeyle	dentifier	√	False			
Properties ✓ True ✓ keyUsage ✓ True ✓ S False nonRepudiation ✓ S False ✓ S False dataEncipherment ✓ S False ✓ S False certificatePolicies ✓ False ✓ S False PolicyIdentifier ✓ S Id-qt-1 (CPS) ✓ Qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) O.4.0.194112.1.2 ✓ QualifiedCertificateStat ✓ False ✓ O.4.0.194112.1.2 QualifiedCertificateStat ✓ False ✓ O.4.0.194112.1.2 QualifiedCertificateStat ✓ False ✓ O.4.0.194112.1.2 QualifiedCertificateStat ✓ M S True QcCompliance ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE QcType ✓ M S		keyldentifier	✓ 			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).
digitalSignature ✓ S False nonRepudiation ✓ S True keyEncipherment ✓ S False dataEncipherment ✓ S False certificatePolicies ✓ False PolicyQualifierID ✓ S Id-qt-1 (CPS) Qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S QualifiedCertificateStat ✓ False Qccompliance ✓ M S (0.4.0.1862.1.1) ✓ M S QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE QcType ✓ M S id-etsi-qct-esign	Properties						
Do Repudiation ✓ S True keyEncipherment ✓ S False dataEncipherment ✓ S False certificatePolicies ✓ False I.3.171.1.1.10.3.30 policyQualifierID ✓ S Id-qt-1 (CPS) Qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ M S QualifiedCertificateStat ✓ False O.4.0.194112.1.2 QualifiedCertificateStat ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE QcType ✓ M S id-etsi-qct-esign	keyUsage			True			
$\begin{tabular}{ c c c c c c c c c c c c c c c c c c c$			-				
dataEncipherment ✓ S False certificatePolicies ✓ False 1.3.171.1.10.3.30 Policyldentifier ✓ S Id-qt-1 (CPS) Qualifier ✓ S https://repository.luxtrust.lu policyQualifierID ✓ S Id-qt-2 (User Notice) Policyldentifier ✓ S Id-qt-2 (User Notice) Policyldentifier ✓ S Id-qt-2 (User Notice) Policyldentifier ✓ M S QualifiedCertificateStat ✓ False 0.4.0.194112.1.2 QualifiedCertificateStat ✓ M S QcCompliance ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE QcType ✓ M S id-etsi-qct-esign							
CertificatePolicies ✓ False ✓ PolicyIdentifier ✓ S Id-qt-1 (CPS) Qualifier ✓ S Id-qt-1 (CPS) Qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ False 0.4.0.194112.1.2 QualifiedCertificateStat ✓ False False QCCompliance ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PI QcType ✓ M S id-etsi-qct-esign							False
Policyldentifier ✓ 1.3.171.1.1.10.3.30 policyQualifierID ✓ S Id-qt-1 (CPS) Qualifier ✓ S https://repository.luxtrust.lu policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S QualifiedCertificateStat ✓ False 0.4.0.194112.1.2 QualifiedCertificateStat ✓ False Intue QcCompliance ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PI (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PI QcType ✓ M S id-etsi-qct-esign			✓			S	False
PolicyQualifierID ✓ S Id-qt-1 (CPS) Qualifier ✓ S <u>https://repository.luxtrust.lu</u> policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False 0.4.0.194112.1.2 QualifiedCertificateStat ✓ False True QcCompliance ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PE QcType ✓ M S id-etsi-qct-esign	certificatePc	licies	\checkmark	False			
Qualifier ✓ S https://repository.luxtrust.lu policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False 0.4.0.194112.1.2 QcCompliance ✓ M S True QcSSCD ✓ M S True QcPDS ✓ M S S.pdf QcType ✓ M S id-etsi-qct-esign		PolicyIdentifier	✓				
policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ 0.4.0.194112.1.2 QualifiedCertificateStat ✓ False QcCompliance ✓ M S (0.4.0.1862.1.1) ✓ M S QcSSCD ✓ M S (0.4.0.1862.1.4) ✓ M S QcPDS ✓ M S (0.4.0.1862.1.5) ✓ M S QcType ✓ M S		policyQualifierID	✓			S	
Policyldentifier ✓ Image: Construction of the quarter of the quar		Qualifier	√			S	https://repository.luxtrust.lu
QualifiedCertificateStat ✓ False 0.4.0.194112.1.2 QualifiedCertificateStat ✓ False QcCompliance (0.4.0.1862.1.1) ✓ M S QcSSCD (0.4.0.1862.1.4) ✓ M S QcPDS (0.4.0.1862.1.5) ✓ M S True QcType ✓ M S id-etsi-qct-esign		policyQualifierID	√			S	Id-qt-2 (User Notice)
QcCompliance (0.4.0.1862.1.1) ✓ M S True QcSSCD (0.4.0.1862.1.4) ✓ M S True QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PE S.pdf QcType ✓ M S id-etsi-qct-esign		PolicyIdentifier	~				0.4.0.194112.1.2
QcCompliance (0.4.0.1862.1.1) ✓ M S True QcSSCD (0.4.0.1862.1.4) ✓ M S True QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PE S.pdf QcType ✓ M S id-etsi-qct-esign	QualifiedCe	rtificateStat	√	False			
QcSSCD ✓ M S True (0.4.0.1862.1.4) M S https://www.luxtrust.lu/upload/data/repository/PE QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PE (0.4.0.1862.1.5) ✓ M S id-etsi-qct-esign			~		М	S	True
QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PE S.pdf QcType ✓ M S id-etsi-qct-esign		QcSSCD	~		М	S	True
		QcPDS	~		М	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf
			~		М	S	id-etsi-qct-esign

1.9.37 NCP+ supporting Authentication & Encryption for eID smart cards

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.31>.

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

 $^{^{77}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{78}}$ CE = Critical Extension.

 $^{^{79}}$ O/M: O = Optional, M = Mandatory.

 $^{^{80}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	LuxTrust eID Smart card NCP+ Certificate Profile									
Attribute	Field	IN″	CE ⁷⁸	O/M 79	CO ⁸⁰	Value				
	countryName	✓			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x ⁸¹				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False		_					
	NotBefore NotAfter	\checkmark			D	Certificate generation process date/time.				
	NOTATTER	v			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate				
Subject		~	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character				
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID				
	Surname	~		м	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID				
	countryName	~		М	D	LU				
	emailAddress	~		ο	D	Subject's email address				
	Title	~		М	D	"Private Person"				
	organizationalUnitNam e 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).				
subjectPub		~	False							
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);				
Extension	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).				
s Authority										
Properties authorityKe	videntifier		Foloo							
authorityke	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualified CA x public key				
authorityInf	oAccess	✓	False							
	AccessMethod	\checkmark				ld-ad-2				
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt				
	AccessMethod	~				Id-ad-1				
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ ¹⁸				
cRLDistribu		√	False							
	distributionPoint	√	ļ		S	17				
Cukingt	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl				
Subject Properties										
subjectAltN		✓	False							
	Rfc822Name	✓		0	D	Subject email address				
subjectKeyl		✓	False							
	keyldentifier	~			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	✓	ļ	<u> </u>	S	False				
	keyEncipherment	√			S	True				
	dataEncipherment	\checkmark		1	S	False				

 $^{^{81}}$ X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.25

	LuxTrust eID Smart card NCP+ Certificate Profile									
Attribute	Field	IN″	CE ⁷⁸	O/M 79	CO ⁸⁰	Value				
certificatePo	certificatePolicies									
	Policyldentifier	✓				1.3.171.1.1.10.3.31				
	policyQualifierID	√			S	Id-qt-1 (CPS)				
	Qualifier	√			S	https://repository.luxtrust.lu				
	policyQualifierID	√			S	Id-qt-2 (User Notice)				
	Policyldentifier	~				0.4.0.2042.1.2				

1.9.38 LuxTrust Signing Server QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by LuxTrust, up to 4096 bit key size and with a key usage limited to the support of qualified electronic signature.

	LuxTru	st Signir	ng Serve	er QCP	-n-qsco	d Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹ 5	CO ¹⁶	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	False			
signatureA	laorithm	✓	False		FDV	Validated on duplicates.
SignatureA	algorithm		I dise		S	
	algonam				Ű	OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
-			_		D	Issuing CA Signature.
Issuer		~	False		S	
	countryName	✓ ✓			S	LU 17
	commonName				S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	~	E 1		S	LuxTrust S.A.
Validity	NatDafara	✓ ✓	False	-		Contificate proposition process data (time
	NotBefore NotAfter	✓ ✓			D	Certificate generation process date/time. Certificate generation process date/time + 36
	NotAlter	,			U	Months
subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	title	~		м	D	PRIVATE products:Fixed value: "Private Person"PRO products:"Professional Person" (default) or"Professional Administrator"(Other titles possible for special purpose certificates)
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.



	LuxTrust	Signir	ng Serve	er QCP	-n-ascd	Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹	CO ¹⁶	Value
				5		
	localityName	~		м	D	PRO products only : Company/institution country of HQ (as in articles of association)
	organizationalUnitNa me 1	~		M for PRO prod ., cond i- tiona I (O) for PRI V 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).
	organizationalUnitNa me 2	~		0	D	PRO products only : Company/institution department or other information item
subjectPub		✓	False			
	algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extension s						
Authority Properties						
authorityKe	vldentifier	 ✓ 	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf		✓	False			
	AccessMethod accessLocation	\checkmark	-			Id-ad-2
	AccessMethod	· ✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt Id-ad-1
	accessLocation	· •				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu	ItionPoint	~	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl
Subject Properties						
subjectAltN	ame Rfc822Name	\checkmark	False	0	D	Certificate Holder's email address
subjectKey		· ✓	False			
	keyldentifier	~			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	digitalSignature	✓ ✓	True		S	True
	nonRepudiation				s	True
	keyEncipherment	~			S	True
	dataEncipherment	~			S	False
certificateP	olicies	√	False			
	Policyldentifier	✓ 				1.3.171.1.1.10.3.32
	policyQualifierID gualifier	✓ ✓			S S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	policyQualifierID	▼ ✓			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.194112.1.2
QualifiedCe	rtificateStat	✓	False			



VERSION 1.25

	LuxTrust Signing Server QCP-n-qscd Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹	CO ¹⁶	Value				
	QcCompliance (0.4.0.1862.1.1)	√		М	S	True				
	QcSSCD (0.4.0.1862.1.4)	~		М	S	True				
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS. pdf				
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)				

1.9.39 LuxTrust Signing Server QCP-I-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy with creation of the keys by LuxTrust, up to 4096 bit key size and with a key usage limited to the support of qualified electronic eSeals.

	LuxTrust Signing Server QCP-I-qscd Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNum	per	✓	False							
					FDV	Validated on duplicates.				
signatureA	Igorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.				
signatureV	alue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x ¹⁷				
	organizationName	√			S	LuxTrust S.A.				
Validity		√	False							
	NotBefore	√			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 36 Months				
subject		√	False							
	serialNumber	~		М	D	Serial Number as constructed by LRAO				
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).				
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)				



	LuxTru	st Sigr	ning Ser	ver QCF	P-I-qscd	Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Attribute	organisationIdentif ier (2.5.4.97)	IN ↓	CE	M	D	 Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitNa me	~		о	D	Company/institution department or other information item
subjectPub		√	False			
	algorithm	✓ ✓		N 4		Public Key: Key length: up to 4096 bit (RSA);
Extensio ns	subjectPublicKey	~		M		public exponent: Fermat-4 (=010001).
Authority Propertie s						
authorityKe		√	False			
authorityInf	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualified CA public key
autiontyini	AccessMethod	▼ ✓	1 alse			Id-ad-2
	accessLocation	· ·			-	http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	· √				Id-ad-1
	accessLocation	▼ ✓				
oBI Distrik			Felac			http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu		✓ ✓	False		S	
	distributionPoint fullName	✓ ✓			5	http://ard.hustmict.hu// TOOOA 17
Subject Propertie s		•				http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl
subjectKey	Identifier	√	False			



VERSION 1.25

LuxTrust Signing Server QCP-I-qscd Certificate Profile											
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
	keyldentifier	~			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 Propertie s											
keyUsage		✓	True								
	digitalSignature	~			S	True					
	nonRepudiation				S	False					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificateP	certificatePolicies		False								
	Policyldentifier	~				1.3.171.1.1.10.3.33					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	√			S	Id-qt-2 (User Notice)					
	Policyldentifier	~				0.4.0.194112.1.3					
Qualifie	edCertificateStat	✓	False								
L	QcCompliance (0.4.0.1862.1.1)	~		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	~		Μ	S	True					
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS. pdf					
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)					

1.9.40 LuxTrust Signing Stick QCP-n-qscd certificate profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.34>.

	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								
					FDV	Validated on duplicates.					
signature	Algorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signature	/alue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	~			S	LuxTrust Global Qualified CA x ⁸⁶					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								

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

 83 CE = Critical Extension.

⁸⁴ O/M: O = Optional, M = Mandatory.

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

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



VERSION 1.25

	Lux	Frust S	Signing	Stick Q	CP-n-c	gscd Certificate Profile
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value
	NotBefore NotAfter	\checkmark			D D	Certificate generation process date/time. Certificate generation process date/time + 36 Months
Subject	NOLAILEI	✓ ✓	False			Certificate generation process date/time + 30 Months
	serialNumber	✓		м	D	Serial Number as constructed by LRAO
						-
	commonName	~		М	D	PRO and PRIVATE products : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	~		м	D	PRO and PRIVATE products : Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	~		М	D	"Professional Person" (default) or "Professional Administrator"
						(Other titles possible for special purpose certificates)
						PRO products only:
	organizationName	✓		М	D	Name of company/institution as in articles of association
						or equivalent documents, including the legal form.
	localityName	~		М	D	PRO products only : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	 PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnit Name 2	~		о	D	PRO products only : Company/institution department or other information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent:
	subjectPublicKey	✓		М		Fermat-4 (=010001).
Extensio ns						
Authorit						
y Properti es						
authorityK	eyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public
authoritylr	nfoAccess	✓	False			key
aanontyn	AccessMethod	· ✓				Id-ad-2
	accessLocation	✓			1	http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ⁸⁷
cRLDistrik	outionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
	L		1	1		

⁸⁷ SINCE LTGQCA3



VERSION 1.25

Policy Properti es SHA-1 hash of the value or subjectPublicKey bit st (tag, not including the length and number of unused string bits). Policy Properti es M True S keyUsage ✓ True S digitalSignature ✓ S False nonRepudiation ✓ S False dataEncipherment ✓ S False dataEncipherment ✓ S False Policydentifier ✓ S Id-qt-1 (CPS) policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S True QualifiedCertificateStat ✓ False M S QualifiedCertificateStat ✓ False M S True QualifiedCertificateStat ✓ False M S True QualifiedCertificateStat ✓	Lux			Stick Q	CP-n-c	scd Certificate Profile
Properti es v False D SubjectAltName ✓ False D Rt622Name ✓ False D SubjectKeyldentifier ✓ False D keyldentifier ✓ False D keyldentifier ✓ False D keyldentifier ✓ False D keyldentifier ✓ False D Value, followed by the least significant 60 bits of Value, followed by the least significant 60 b	Attribute Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value
Rfc822Name ✓ O D Certificate Holder's email address subjectKeyldentifier ✓ False Fixed The Key Identifier comprises a four-bit field with a 0 value, followed by the least significant 60 bits of SHA-1 hash of the value or subjectPublicKey bit st (tag. not including the length and number of unused string bits). Policy Properties S False False digitalSignature ✓ S False S keyUsage ✓ True S False dataEncipherment ✓ S False certificatePolicies ✓ False S PolicyUdentifier ✓ S Id-qt-1 (CPS) galifier ✓ S Id-qt-1 (CPS) galifier ✓ S Id-qt-2 (User Notice) PolicyUdentifier ✓ S Id-qt-2 (User Notice) policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyUdentifier ✓ S Id-qt-2 (User Notice) PolicyUdentifier ✓ S Id-qt-2 (User Notice)	Properti es					
subjectKeyldentifier ✓ False O D Output Diversion subjectKeyldentifier ✓ False Fixed The Key Identifier comprises a four-bit field with a O value, followed by the least significant 60 bits of value, followed by the least significant 60 bits of value, followed by the length and number of unused string bits). Policy Properties ✓ True S False digitalSignature ✓ True S False digitalSignature ✓ S False S nonRepudiation ✓ S False S certificatePolicies ✓ False S False certificatePolicies ✓ False S False policyQualifierI ✓ S Id-qt-1 (CPS) S qualifier ✓ S Id-qt-2 (User Notice) S policyQualifierID ✓ S Id-qt-2 (User Notice) S qualifiedCertificateStat ✓ False S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False S Id-qt-2 (User Notice) QcCompliance ✓			False			
keyldentifier ✓ Fixed The Key Identifier comprises a four-bit field with a 0 value, followed by the least significant 60 bits of SHA-1 hash of the value or subject/bublicKey bit st (tag, not including the length and number of unused string bits). Policy Properti es ✓ S False digitalSignature ✓ S False monRepudiation ✓ S False dataEncipherment ✓ S False dataEncipherment ✓ S False policyQualifierI ✓ S Id-qt-1 (CPS) qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S True QualifiedCertificateStat ✓ False QualifiedCertificateStat ✓ False QcCompliance ✓ M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc				0	D	Certificate Holder's email address
Policy value, followed by the least significant 60 bits of SHA-1 hash of the value or subjectPublicKey bit st (rag, not including the length and number of unused string bits). Policy rone Properti es value digitalSignature v test value digitalSignature v test value digitalSignature v test s formation v test s			False			
Properti es Image: second	keyldentifier	~			Fixed	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-
digitalSignature ✓ S False nonRepudiation ✓ S True keyEncipherment ✓ S False dataEncipherment ✓ S False certificatePolicies ✓ False Image: Sector of Constraints PolicyIdentifier ✓ S Id-qt-1 (CPS) qualifier ✓ S Id-qt-2 (User Notice) policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S True QcCompliance ✓ M S True (0.4.0.1862.1.1) M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign	Properti es					
Ingritude Image nonRepudiation V keyEncipherment V dataEncipherment V dataEncipherment V S False certificatePolicies V PolicyIdentifier V policyQualifierl V D S Id-qt-1 (CPS) Qualifier V S Id-qt-2 (User Notice) PolicyIdentifier V S Id-qt-2 (User Notice) PolicyIdentifier V S Id-qt-2 (User Notice) PolicyIdentifier V V S Id-qt-2 (User Notice) PolicyIdentifier V V S Id-qt-2 (User Notice) PolicyIdentifier V V S Id-qt-2 (User Notice) PolicyIdentifier V V S Id-qt-2 (User Notice) PolicyIdentifier V V M QcCompliance V (0.4.0.1862.1.4) N QcPDS V (0.4.0.1862.1.5) M QcType V	keyUsage		True			
keyEncipherment ✓ S False dataEncipherment ✓ S False certificatePolicies ✓ False PolicyIdentifier ✓ 1.3.171.1.1.0.3.34 policyQualifierl ✓ S Id-qt-1 (CPS) qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierlD ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ M S True QualifiedCertificateStat ✓ False QcCompliance ✓ M S True (0.4.0.1862.1.1) M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign	digitalSignature					
dataEncipherment ✓ S False certificatePolicies ✓ False Image: Constraint of the structure		-				
certificatePolicies ✓ False Image: state sta						
Policyldentifier ✓ 1.0.0 1.3.171.1.1.10.3.34 policyQualifierI ✓ S Id-qt-1 (CPS) qualifier ✓ S https://repository.luxtrust.lu policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ False O.4.0.194112.1.2 QualifiedCertificateStat ✓ False O.4.0.194112.1.2 QualifiedCertificateStat ✓ M S True QcCompliance ✓ M S True QcSSCD M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign					S	False
PolicyQualifierI ✓ S Id-qt-1 (CPS) qualifier ✓ S Id-qt-1 (CPS) qualifier ✓ S Id-qt-2 (User Notice) PolicyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False Output QcCompliance ✓ M S True QcSSCD M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign			False			
D Image: Second system Image: Second system <thimage: second="" system<="" th=""> Image: Second syste</thimage:>						
policyQualifierID ✓ S Id-qt-2 (User Notice) PolicyIdentifier ✓ S Id-qt-2 (User Notice) QualifiedCertificateStat ✓ False O.4.0.194112.1.2 QualifiedCertificateStat ✓ False False QcCompliance ✓ M S True QcSSCD M S True QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign	D				-	
Policyldentifier ✓ ✓ Image: Constraint of the second		✓				https://repository.luxtrust.lu
QualifiedCertificateStat ✓ False QcCompliance (0.4.0.1862.1.1) ✓ M S True QcSSCD (0.4.0.1862.1.4) M S True QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign	policyQualifierID				S	Id-qt-2 (User Notice)
QcCompliance (0.4.0.1862.1.1) ✓ M S True QcSSCD (0.4.0.1862.1.4) M S True QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign	Policyldentifier	~				0.4.0.194112.1.2
(0.4.0.1862.1.1) M S True QcSSCD M S True (0.4.0.1862.1.4) M S https://www.luxtrust.lu/upload/data/repository/PDS.pd QcPDS ✓ M S id-etsi-qct-esign QcType ✓ M S id-etsi-qct-esign	QualifiedCertificateStat	✓	False			
(0.4.0.1862.1.4) ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcPDS ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pc QcType ✓ M S id-etsi-qct-esign		~		М	S	True
QcPDS (0.4.0.1862.1.5) ✓ M S https://www.luxtrust.lu/upload/data/repository/PDS.pd QcType ✓ M S id-etsi-qct-esign	QcSSCD			М	S	True
	QcPDS	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
		~		М	S	id-etsi-qct-esign

1.9.41 LuxTrust Signing Stick NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.35>.

	LuxTrust Signing Stick NCP+ Certificate Profile										
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	CO ⁹¹	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								
					FDV	Validated on duplicates.					
signatureA	lgorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureV	/alue	✓	False								

 $^{^{88}}$ IN = Included: Attribute / field included within the certificate profile.

 $^{^{89}}$ CE = Critical Extension.

 $^{^{90}}$ O/M: O = Optional, M = Mandatory.

 $^{^{91}}$ CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



VERSION 1.25

Assailante	Field	INI	89	90	91	Value
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	C0 ⁹¹	Value
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	\checkmark			S	LuxTrust Global Qualified CA x ⁹²
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓ ✓			D D	Certificate generation process date/time.
	NotAfter	v			D	Certificate generation process date/time + 3 Months
Subject	L	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						DDO and DDI/(ATE and ductor Consectance)
	commonName	~		М	D	PRO and PRIVATE products : Concatenation given name(s) and surname(s) as on ID ca separated by a "Space" character.
	givenName	~		М	D	PRO and PRIVATE products : Given name(s) a on ID card
	surname	~		М	D	PRO and PRIVATE products : Surname(s) as of ID card without indication "épouse", "ép." or simile and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) "Professional Administrator" (Other titles possible for special purpos certificates)
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles association or equivalent documents, including th legal form.
	localityName	~		М	D	PRO products only : Company/institution count of HQ (as in articles of association)
	organizationalUnit Name 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VA number available, other unique nation company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " (Date of birth + 18 years).
	organizationalUnit Name 2	~		0	D	PRO products only : Company/institution department or oth information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); publ
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensio						
ns Authorit y Properti						
es authorityK	Ceyldentifier	 ✓ 	False			
autiontyn	keyldentifier	• ✓	1 0150			SHA-1 Hash of the LuxTrust Global Qualified C
		1				public key

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



VERSION 1.25

	LuxTrust Signing Stick NCP+ Certificate Profile										
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	CO ⁹¹	Value					
authoritylr	authorityInfoAccess		False								
	AccessMethod	✓				Id-ad-2					
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt					
	AccessMethod	✓				Id-ad-1					
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/93					
cRLDistrib	outionPoint	✓	False								
	distributionPoint	✓		-	S						
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl					
Subject Properti es											
subjectAlt		✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKe		\checkmark	False								
	keyldentifier	~			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 Properti es											
keyUsage		✓	True			_					
	digitalSignature	 ✓ 			S	True					
	nonRepudiation	\checkmark			S	False					
	keyEncipherment	v √			S S	True					
certificate	dataEncipherment	v √	False		5	False					
certificate	Policyldentifier	▼ ✓	raise			1.3.171.1.1.10.3.35					
	policyQualifierID	· ·			S	Id-qt-1 (CPS)					
	qualifier	√	1		S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	Policyldentifier	~				0.4.0.2042.1.2					

1.10 Timestamping Certificate Profile

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

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

	LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
Base										
Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	✓	False							

⁹³ SINCE LTGQCA3



VERSION 1.25

					ificate F	
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU 17
	commonName	~			S	LuxTrust Global Timestamping CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time
		✓			-	60 Months
subject			False			
	commonName	~		М	D	tts.luxtrust.lu
	localityName	✓		М	D	Capellen
	localityName	-		IVI		Capenen
	organizationName	✓		М	D	LuxTrust S.A.
	organizational InitName 1	~		М	D	DKI Entity
	organizationalUnitName 1	v		IVI	U	PKI Entity
	countryName	\checkmark		0	D	LU
subjectPubli		✓	False			
	algorithm	· ·	1 0.00		1	Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	✓	1	М	1	public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	yldentifier	✓	False			
,	keyldentifier	√				SHA-1 Hash of the LuxTru
						Timestamping CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGTSACAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistribut		✓	False			
	distributionPoint	✓		1	S	
	fullName	✓			_	http://crl.luxtrust.lu/LTGTSACAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓	1 0.00	0	D	info@luxtrust.lu
subjectKeylo		✓	False			
· · · · , · · · · · , · ·	keyldentifier	✓			Fixed	The Key Identifier comprises a four-t
						field with a 0100 value, followed by the least significant 60 bits of the SHA-1 has of the value or subjectPublicKey bit strir (tag, not including the length and numb of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	√			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
_	dataEncipherment	✓			S	False
Extended Ke		✓	False			
	TimeStamping	~			S	Set
	(1.3.6.1.5.5.7.3.8)	1 .	I			
Private Key	Usage Period	✓	False			
	Usage period (2.5.29.16)	~		М	D	Certificate generation process date/time
		1 .	I			12 Months
		✓	False			
ertificatePo	blicies		1 0.00			
certificatePo	Policyldentifier	✓	1 0.00			1.3.171.1.1.10.8.1
certificatePo	Policyldentifier policyQualifierID	✓ ✓			S	Id-qt-1 (CPS)
certificatePo	Policyldentifier	✓			S S S	



VERSION 1.25

	LuxTrust Timestamping Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
	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.					
	Policyldentifier	✓				0.4.0.2042.1.3					

1.10.1 Normalized Certificate Policy for LuxTrust Qualified Timestamping

LuxTrust Qualified Timestamping Certificates are issued by the LuxTrust Qualified CA with keys located on HSM devices, with generation by LuxTrust CSP according to the processes and procedures described in the applicable CP, with a key size up to 4096 and 5 years validity from issuing start date.

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 and RFC5816. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles.

This profile complies to the requirements of the standard ETSI EN 319 411-1 describing the Requirements for trust service providers issuing Extended Normalized Certificate Policy.

Normalized Certificate Policy for LuxTrust Qualified Timestamping										
Attribute	Field	IN ¹³		O/M ¹⁵	CO ¹⁶					
Base			-							
Profile										
Version		✓	False							
			1 0.00		S	Version 3 Value = "2"				
SerialNumbe	ar	✓	False							
Senanumbe		-	1 0130		FDV	Validated on duplicates.				
cianoturo Ala	vorithm	✓	False		TDV					
signatureAlg	jorithm	v	Faise			OID = "1.2.840.113549.1.1.11" - SHA256 with RSA				
	algorithm				S					
• • •						Encryption.				
signatureVa	lue	√	False		_					
-					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	√			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
					_	Certificate generation process date/time + 60				
	NotAfter	~			D	Months				
subject		✓	False							
300,000	organisationIdentifier		1 0130							
	(2.5.4.97)	\checkmark		M	D	VATLU-20976985				
	commonName	~		М	D	LuxTrust Qualified Timestamping				
		▼ ✓			_					
	organizationName			M	D	LuxTrust S.A.				
	countryName	✓		М	D	LU				
subjectPubli		✓	False							
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA)				
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).				
Extensions										
Authority										
Properties										
authorityKey		✓	False							
	keyldentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA				
authorityInfo		√	False							
	AccessMethod	✓			1	ld-ad-2				
	accessLocation	~	1	İ	1	http://ca.luxtrust.lu/LTGQCAx.crt				
	AccessMethod	√ 	1	†	1	Id-ad-1				
	accessLocation	· ·	-		-	http://gca.ocsp.luxtrust.lu/				
cRLDistribut		▼ ✓	False			<u>niip.//yea.ocop.iuxii.uoi.iu/</u>				
CILDISTIDU	distributionPoint	▼ ✓	raise		S					
		✓ ✓			3					
0.1.	fullName	~				http://crl.luxtrust.lu/LTGQCAx.crl				
Subject										
Properties										
subjectAltNa		✓	False			-				
	Rfc822Name	\checkmark		0	D	<u>info@luxtrust.lu</u>				



VERSION 1.25

	Normalized (Certific	ate Poli	cy for Lu	uxTrust (Qualified Timestamping
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
subjectKeylo	dentifier	✓	False			
	keyldentifier	~			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 Ke	ey Usage	✓	True			
	TimeStamping (1.3.6.1.5.5.7.3.8)	~			S	Set
Private Key	Usage Period	~	False			
	Usage period (2.5.29.16)	~		М	D	Certificate generation process date/time + 12 Months
certificatePo	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.18
	policyQualifierID	~			S	ld-qt-1 (CPS)
	qualifier	~			S	https://repository.luxtrust.lu
	policyQualifierID	~			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

1.10.2 Qualified Timestamping Certificate Profile

LuxTrust Qualified Timestamping Certificates are issuesd by the LuxTrust Qualified CA with keys located on HSM devices, with generation by LuxTrust CSP according to the processes and procedures described in the applicable CP, with a key size up to 4096 and 5 years validity from issuing start date.

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 and RFC5816. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [21] and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles [22].

This profile complies to the requirements of the standard ETSI EN 319 411-2 [20] describing the Requirements for trust service providers issuing EU qualified certificates.

Qualified Certificate Policy for for LuxTrust Qualified Timestamping								
Attribute	Field	IN1 3	CE1 4	O/M1 5	CO1 6	Value		
Base Profile								
Version		~	Fals e					
					S	Version 3 Value = "2"		
SerialNumber		~	Fals e					
					FDV	Validated on duplicates.		
signatureAlgorithm		~	Fals e					
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.		
signatureV	alue	~	Fals e					
					D	Issuing CA Signature.		
issuer		~	Fals e		S			
	countryName	✓			S	LU		
commonName		✓			S	LuxTrust Global Qualified CA x		
	organizationName	✓			S	LuxTrust S.A.		
Validity	·	~	Fals e					
	NotBefore	✓			D	Certificate generation process date/time.		
NotAfter		✓			D	Certificate generation process date/time + 60 Months		



VERSION 1.25

	Qualifie	d Certi	ificate P	olicy for	for Lux	Trust Qualified Timestamping
Attribute	Field	IN1	CE1		CO1	Value
, the instate		3	4	5	6	
subject		✓	Fals			
			е			
	organisationIdentifi) (ATI 11 00070005
	er	✓		М	D	VATLU-20976985
	(2.5.4.97)					
					-	
	commonName	✓		М	D	LuxTrust Qualified Timestamping
	organizationName	✓		М	D	LuxTrust S.A.
	countryName	✓		М	D	LU
subjectPub	licKeyInfo	~	Fals			
			е			
	algorithm	\checkmark				Public Key: Key length: up to 3072 bit (RSA)
Extension	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).
S						
Authority						
Propertie						
S						
authorityKe	eyldentifier	✓	Fals			
	Level de 199		е			
	keyldentifier	~				SHA 1 back of the Lux Truct Clobal Qualified CA
authorityInf	o Access	✓	Fals			SHA-1 hash of the LuxTrust Global Qualified CA
autiontyilli	CAUCUSS		e			
	AccessMethod	√	Ŭ			Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	\checkmark				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/
cRLDistribu	utionPoint	✓	Fals			
	distribution Daint		е			
	distributionPoint fullName	\checkmark			S	http://crl.luxtrust.lu/LTGQCAx.crl
	Tullivallie	ľ				http://cilluxilusillu/ETGQCAX.cil
Subject						
Propertie						
S						
subjectAltN	lame	~	Fals			
	D(000)		е		_	
aubiaatKau	Rfc822Name	\checkmark	Fala	0	D	info@luxtrust.lu
subjectKey	Identifier	Ň	Fals e			
	keyldentifier	✓	e		Fixe	The Key Identifier comprises a four-bit field with a 0100
	Reylacitation				d	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						
Propertie						
s keyUsage		 ✓ 	True			
пеуизауе	digitalSignature	▼ ✓	nue		S	True
	nonRepudiation	· •	1	1	S	False
	keyEncipherment	✓	1	1	S	False
	dataEncipherment	✓	1	1	S	False
Extended K	ey Usage	✓	True			
	TimeStamping	✓			S	Set
	(1.3.6.1.5.5.7.3.8)				-	
Private Key	Usage Period	✓	Fals			
	Usage period	✓	е	M	D	Certificate generation process date/time + 12 Months
	(2.5.29.16)	1		IVI		Certificate generation process date/time + 12 Months
certificateP		✓	Fals			
			e			
	Policyldentifier	✓				1.3.171.1.1.10.3.19
	policyQualifierID	\checkmark			S	Id-qt-1 (CPS)
	qualifier	\checkmark			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
		✓ ✓			S	Id-qt-2 (User Notice) 0.4.0.194112.1.1



VERSION 1.25

	Qualified Certificate Policy for for LuxTrust Qualified Timestamping									
Attribute Field		IN1	I1 CE1 O/M1		CO1	Value				
		3	4	5	6					
certificateP	certificatePolicies									
	QcType	✓		М	S	id-etsi-qct-eseal				
	(0.4.0.1862.1.6)					(0.4.0.1862.1.6.2)				
	QcCompliance (0.4.0.1862.1.1)	~		М	S	True				
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/GTC_F_v2 _4.pdf				

1.10.3 TimeStamp Request and Response Format

1.10.3.1 TimeStamp Request Format

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

LuxTrust Time Stamp Request									
Field	Value / comment								
Document Hash	Hash of the document on which the TimeStamp must be computed								
Hash OID	(SHA-1/SHA-256/SHA-512)								
	Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.								
Policy OID	1.3.171.1.10.3.18.1								
	The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.								
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.								
Should TSA Certificate be included?	TRUE/FALSE								
Request Extensions	Value *								
None	None								

*no extension is required to be supported

1.10.3.2 TimeStamp Response Format

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

LuxTrust Time Stamp Response								
Field	Value / comment							
Generation Time	The time at which the time-stamp token has been created by the TSA. It is expressed as UTC time (Coordinated Universal Time).							
Document Hash	Hash of the document on which the TimeStamp response has been computed							
Hash OID	(SHA-1/SHA-256/SHA-512) Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.							



VERSION 1.25

LuxTrust Time Stamp Response								
Field	Value / comment							
Serial Number	Serial Number of the current TSU certificate (unique, up to 160 bits)							
Policy OID	1.3.171.1.1.10.3.18.1 / Qualified timestamp token 1.3.171.1.1.10.8.1.1 / Non-qualified timestamp token							
	The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.							
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.							
Accuracy	1 second							
TSA Certificate Information	Current TSU Certificate							
Request Extensions	Value *							
None	None							

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

1.11 Certificate extensions

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

1.12 Algorithm object identifiers

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

1.13 Name forms

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

1.14 Name constraints

Name constraints are supported as per RFC 5280.

1.15 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

1.16 Usage of Policy Constraints extension

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

1.17 Policy qualifiers syntax and semantics

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



VERSION 1.25

1.18 Processing semantics for the critical Certificate Policies

Not applicable.

1.19 CRL profile

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

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

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

LuxTrust CRL Profile								
Field	Comments							
Version	v2							
Signature	Same signature algorithm as related CA							
Issuer	<subjectca></subjectca>							
thisUpdate	<creation time=""></creation>							
nextUpdate	<creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" subordinate<br="" time="">Qualified and SSL CAs> <creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></creation></creation>							
revokedCertificates								
userCertificate	<certificate number="" serial=""></certificate>							
revocationDate	<revocation time=""></revocation>							
crlEntryExtensions								
reasonCode	<insert code="" list="" of="" reason="" revocation="" used=""></insert>							
crlExtensions								
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>							
authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>							

1.19.1 Version number(s)

See section 3.4.

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

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

1.19.2 CRL entry extensions

See section 3.4.

1.20 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 OCSP v1 and v2. The LuxTrust CAs support signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA.

1.20.1 Version number(s)

See section 3.5.

1.20.2 OCSP extensions

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

LuxTrust OCSP Certificate Profile								
Attribute	Field	IN18	CE19	O/M20	CO21	Value		
Base Profile								
Version	Version							
					S	Version 3 Value = "2"		
SerialNumbe		False						



VERSION 1.25

	LuxTrust OCSP Certificate Profile								
Attribute	Field	IN18	CE10	O/M20	CO21	Value			
Attribute	Field	INTO	CE19	0/10/20	FDV				
		_	E de s		FDV	Validated on duplicates.			
signatureAl			False		-	OID = "1.2.840.113549.1.1.11" - SHA256			
	algorithm				S				
alamaturaVa						with RSA Encryption.			
signatureVa			False						
			L Calas		D	Issuing LTGRCA Signature			
issuer			False		S				
	countryName				S	LU			
	commonName				S	LuxTrust Global Root x			
	organizationName				S	LuxTrust S.A.			
Validity			False		_				
	NotBefore				D	Certificate generation process date/time.			
	NotAfter				D	Certificate generation process date/time +			
						maximum 12 Months			
subject			False		-				
	countryName			М	D	LU			
	organizationName			М	D	LuxTrust S.A.			
	organizationalUnitName 1			0	D	Pki entity			
	commonName			М	D	LuxTrust S.A. OCSP Server 2			
subjectPubl			False						
	algorithm					Public Key: Key length: 2048 bit (RSA);			
	subjectPublicKey			М		public exponent: Fermat-4 (=010001).			
Extensions									
Authority									
Properties									
authorityKe	yldentifier		False						
	keyldentifier					SHA-1 Hash of the LuxTrust LTGR x CA			
		_				public key			
id-ocsp-noc	heck		False						
					S	NULL			
Subject									
Properties									
subjectKeyl	dentifier		False						
	keyldentifier				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			
		<u> </u>			<u> </u>				
	nonRepudiation				S	False			
	keyEncipherment				S	False			
				L					
	dataEncipherment				S	False			
certificatePo	certificatePolicies		False						
	PolicyIdentifier					1.3.171.1.1.1.0.1.0			
	policyQualifierID				S	Id-qt-1 (CPS)			
	qualifier				S	https://repository.luxtrust.lu			
	policyQualifierID				S	Id-qt-2 (User Notice)			
	noticeNumbers			I					
	DisplayText		Ī			LuxTrust S.A. Online Certificate Status			
						Server. IETF PKIX RFC 2560 OCSP v1			
						and v2. No OCSP extensions are			
						supported.			
	Policyldentifier					0.4.0.2042.1.3			
Extended K			False						
	OCSPSigning				S	True			
						•			