

Version number: 1.27 Publication Date: 26/03/2018 Effective Date: 09/04/2018

LuxTrust S.A

IVY Building | 13-15, Parc d'activités | L-8308 Capellen

Luxembourg | VAT LU 20976985 | RCS B112233

Business Number N°00135240/0

Phone: +352 26 68 15 – 1 Fax: +352 26 68 15 – 789





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



	T	1						
1.19	YNU	11/11/2014	Update AIA in CP under the SSL CA since SSL CA 2					
1.20	YNU	19/12/2014	Add Integration CP for eID					
			Update eID CP with pseudonym					
			Update Global Root CA CP with OID attribute					
			Update SSL CA profile since SSL CA 3					
4.04	000	0=/00/00/-	Update lifetime of SSL Server/Object/SSL Client auth to 24 months					
1.21	CSP	25/03/2015	Update LT CA					
	Board		- lifetime up to 20 years					
			- AIA Update Display text					
			- EV SSL CP					
			Update eID CP					
			Update ILNAS Logo					
1.22	YNU	03/11/2015	Update Common Names in non SSL certificates					
1.22	TINO	03/11/2013	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					
			Soop Hoohook, ac actiniou by the Ozoco					
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					
			<ul> <li>Qualified/Advanced eSeal certificate profiles</li> </ul>					
			elDAS qualified certificate profiles					
			Signing Server Signature and eSeal certificates and QWAC					
			certificate and signing stick certificates					
1.25	DEL	30/08/2017	Add Microsoft OIDs in SSL certificates profiles to ensure					
			alignement with Microsoft Trusted Root certificate Program					
			requirements (https://technet.microsoft.com/en-					
			us/library/cc751157.aspx).					
1.26	NDE	24/11/2017	Increase CRL validity from 4h30min to 8h30min for SSL certificates					
	DEL	15/12/2017	Update hash functions in accordance with normative requirements					
	DEL	01/01/2018	Add Advanced eSeal certificate profile					
4.0=	55:	10/00/00/-						
1.27	DEL	19/03/2018	Add LuxTrust Corporate CA & Corporate certificate profile					
			Update SSL certificates profiles to support Certificate					
			Transparency					



## **Table of content**

DOCUMEN	IT INFORMATION	2
VERSION I	HISTORY	2
TABLE OF	CONTENT	4
INTELLEC	TUAL PROPERTY RIGHTS	7
REFEREN	CES	8
INTRODUC	CTION	9
1.1	THE LUXTRUST PROJECT	9
1.2	GOAL OF THE LUXTRUST PKI	9
1.3	LuxTrust PKI Hierarchy	9
LUXTRUS	T CERTIFICATION AUTHORITIES	10
1.4	TWO-LEVEL CA HIERARCHY	10
CERTIFICA	ATE AND CRL PROFILES	12
1.5	CERTIFICATE TYPES	12
1.6	LuxTrust Certification Authorities – Certificates profiles	23
1.7	LuxTrust Global Root CA	23
1.8	LuxTrust Global Qualified CA	24
1.9	LuxTrust SSL CA	25
1.10	LUXTRUST TSA (TIMESTAMPING) CA	27
1.11	LUXTRUST CORPORATE CA	28
1.11.1	Certificate extensions	30
1.11.2	Algorithm object identifiers	30
1.11.3	Name forms	30
1.11.4	Name constraints	30
1.11.5	Certificate policy object identifier	30
1.11.6	Usage of Policy Constraints extension	30
1.11.7	Policy qualifiers syntax and semantics	30
1.12	LuxTrust End-entity – Certificates profiles	30
1.12.1	Certificate profiles	30
1.12.2	Version number(s)	31
1.12.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	31
1.12.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	33
1.12.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	35
1.12.6	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	38
1.12.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	40
1.12.8	LuxTrust NCP+ Certificates supporting Mass Signature Services	42
1.12.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	43
1.12.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	45
1.12.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for in	-
1.12.12	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	
1.12.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	



1.12.14	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures	52
1.12.15	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures	54
1.12.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	56
1.12.17	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures	58
1.12.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	60
1.12.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	61
1.12.20	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authenticate Encryption	
1.12.21	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentica Encryption	
1.12.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Authentica Encryption	
1.12.23	LuxTrust Object (or Code) Signing Certificates	75
1.12.24	LuxTrust SSL/TLS Certificate for Client Authentication	77
1.12.25	SSL/TLS QCP-w Extended Validation Server Certificates	79
1.12.26	LuxTrust SPARE Signing Server LCP Certificate Profile	82
1.12.27	LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature	85
1.12.28	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	87
1.12.29	LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature	89
1.12.30	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	91
1.12.31	LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature	93
1.12.32	LuxTrust Smart Card QCP-n-qscd Certificate Profile	95
1.12.33	LuxTrust Smart Card NCP+ Certificate Profile	97
1.12.34	LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature	99
1.12.35	LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purposes	. 101
1.12.36	QCP-n-qscd supporting Qualified Electronic Signature for eID smart cards	. 102
1.12.37	NCP+ supporting Authentication & Encryption for eID smart cards	. 104
1.12.38	LuxTrust Signing Server QCP-n-qscd Certificate Profile	. 106
1.12.39	LuxTrust Signing Server QCP-I-qscd Certificate Profile	. 108
1.12.40	LuxTrust Signing Stick QCP-n-qscd certificate profile	. 110
1.12.41	LuxTrust Signing Stick NCP+ Certificate Profile	. 112
1.12.42	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	. 114
1.12.43	LuxTrust Corporate LCP Certificate Profile	. 118
1.13	TIMESTAMPING CERTIFICATE PROFILE	.120
1.13.1	Normalized Certificate Policy for LuxTrust Qualified Timestamping	. 122
1.13.2	Qualified Timestamping Certificate Profile	. 123
1.13.3	TimeStamp Request and Response Format	. 125
1.14	CERTIFICATE EXTENSIONS	.126
1.15	ALGORITHM OBJECT IDENTIFIERS	.126
1.16	NAME FORMS	.126
1.17	NAME CONSTRAINTS	.126
1.18	CERTIFICATE POLICY OBJECT IDENTIFIER	.126
1.19	USAGE OF POLICY CONSTRAINTS EXTENSION.	.126
1.20	POLICY QUALIFIERS SYNTAX AND SEMANTICS	.127
1.21	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES	.127
1.22	CRL PROFILE	.127
1.22.1	Version number(s)	. 127
1.22.2	CRL entry extensions	. 127
1.23	OCSP PROFILE	.127





1.23.1	Version number(s)	127
1.23.2	OCSP extensions	128

VERSION 1.27



## **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.



### 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 protection of individuals with regards to the processing of personal data and on the free movement of such data.
- [3] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- [4] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- [6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 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 e-applications and accelerate eLuxembourg. Within this context, LuxTrust will form the catalyser of such services and applications.

#### 1.3 LuxTrust PKI Hierarchy

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

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

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



### **LuxTrust Certification Authorities**

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

#### 1.4 Two-level CA hierarchy

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

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

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

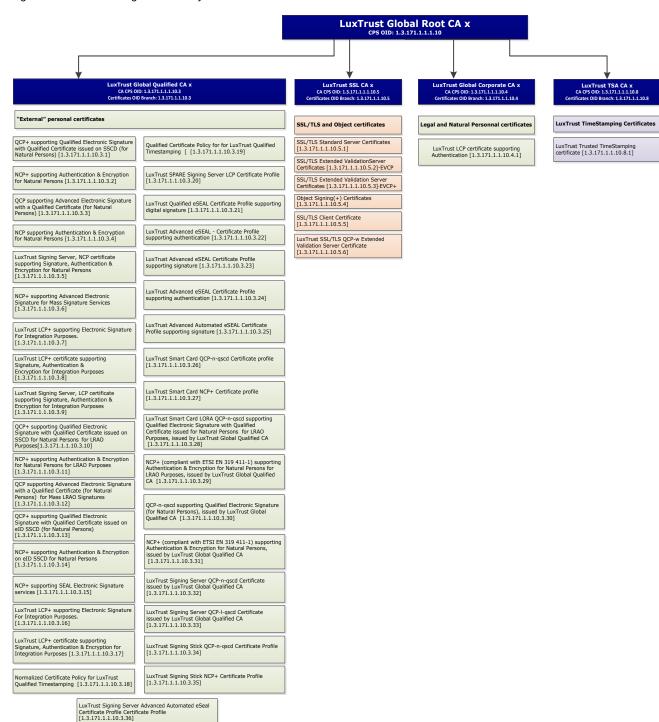
Subordinate CAs are operating within a grant of authority for issuing certificates under the LuxTrust CPS and the applicable CP. This grant has been provided by the "LuxTrust Global Root CA" (hereafter "LTGRCA") under the responsibility and authority of LuxTrust S.A. acting as CSP.

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

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



Figure 1- LuxTrust running CA Hierarchy





## **CERTIFICATE AND CRL PROFILES**

## 1.5 Certificate 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	1.3.171.1.1.10.3	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.9	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for INTEGRATION PURPOSES.	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes
QCP+ supporting Qualified Electronic Signature with Qualified Certificate issued on SSCD for Natural Persons for LRAO Purposes issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.10	1.3.171.1.1.10.3	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	1.3.171.1.1.10.3	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	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.	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	1.3.171.1.1.10.3	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	1.3.171.1.1.10.3	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	1.3.171.1.1.10.3	Signing Stick QCP-n-qscd Certificate Profile	Signing Stick QCP-n-qscd Certificate Profile
LuxTrust Signing Stick NCP+ Certificate Profile	1.3.171.1.1.10.3.35	1.3.171.1.1.1.10.3	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile
LuxTrust Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	1.3.171.1.1.10.3.36	1.3.171.1.1.1.10.3	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile
LuxTrust SSL Certification Authority				



CP identification	CP OID	CPS OID	Short Description	Ref.
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 <b>LCP</b> 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
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 <b>EVCP</b> 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 <b>LCP</b> 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
*	mping) Certification Author	ority		
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
LuxTrust Global Corpo	rate CA			





CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Corporate LCP Certificate Profile issued by Corporate CA	1.3.171.1.1.10.4.1	1.3.171.1.1.10.4	LuxTrust Corporate LCP Certificate Profile	LuxTrust Corporate LCP Certificate Profile

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

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

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

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

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

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

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



VERSION 1.27

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	o			x	у	1.3.171.1 <b>.1.1.1.0.x.y</b>	N/A
		<b>2</b> Not Used		Not Used		-	-	not used	N/A
		10 CPS LuxTrust		LuxTrust Global Root CA		-	-	1.3.171.1 <b>.1.1.10</b>	N/A
		Global Root Chain	3	LuxTrust Global Qualified CA		-	-	1.3.171.1 <b>.1.1.10.3</b>	N/A
			5	LuxTrust SSL CA		-	-	1.3.171.1. <b>1.1.10.5</b>	N/A
			8	LuxTrust Global Timestamping CA		-	-	1.3.171.1. <b>1.1.10.8</b>	N/A
1 LuxTrust	LuxTrust Certi	ficate Policies							
PKI	10 CP's LuxTrust Global Chain	xTrust LuxTrust Global	1	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1. <b>1.10.3.1</b>	0.4.0.1456.1.1
		Certificates	2	NCP+ supporting Authentication & Encryption for Natural Persons	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.2</b>	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. <b>1.10.3.3</b>	0.4.0.1456.1.2
			4	NCP Authentication & Encryption	Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.4</b>	0.4.0.2042.1.1
			5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1 <b>.1.10.3.5</b>	0.4.0.2042.1.1
			6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-	-	1.3.171.1. <b>1.10.3.6</b>	0.4.0.2042.1.1
	<u> </u>	LuxTrus	t pror	prietary and confidential				Page 19	

VERSION 1.27

7	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration SmartCard Signature Certificate	-	-	1.3.171.1. <b>1.10.3.7</b>	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. <b>1.10.3.8</b>	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 <b>.1.10.3.9</b>	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. <b>1.10.3.10</b>	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. <b>1.10.3.11</b>	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. <b>1.10.3.12</b>	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. <b>1.10.3.13</b>	0.4.0.1456.1.1
14	NCP+ supporting Authentication & Encryption for Natural Persons	eID SmartCard Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.14</b>	0.4.0.2042.1.2
15	NCP+ supporting Advanced Electronic Seal Signature Services	Seal Signature Services	-	-	1.3.171.1 <b>.1.10.3.15</b>	0.4.0.1456.1.2
16	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration eID SmartCard Signature Certificate	-	-	1.3.171.1. <b>1.10.3.16</b>	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 <b>.1.10.3.17</b>	0.4.0.2042.1.3
18	Normalized Certificate Policy for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1. <b>1.10.3.18</b>	0.4.0.2042.1.2
19	Qualified Certificate Policy for for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1. <b>1.10.3.19</b>	0.4.0.194112.1.1
20	LuxTrust SPARE Signing Server LCP Certificate	LuxTrust SPARE Signing Server LCP Certificate	-	-	1.3.171.1 <b>.1.10.3.20</b>	0.4.0.2042.1.3
21	LuxTrust Qualified eSEAL Certificate supporting digital signature	LuxTrust Qualified eSeal	-	-	1.3.171.1. <b>1.10.3.21</b>	0.4.0.194112.1.3
22	LuxTrust Advanced eSeal NCP+ Certificate for authentication	LuxTrust Qualified eSeal	-	-	1.3.171.1. <b>1.10.3.22</b>	0.4.0.2042.1.2



VERSION 1.27

	23	LuxTrust Advanced eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.23</b>	0.4.0.2042.1.2
	24	LuxTrust Advanced eSEAL Certificate supporting authentication	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.24</b>	0.4.0.2042.1.2
	25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.25</b>	0.4.0.2042.1.2
	26	LuxTrust Smart Card QCP-n-gscd Certificate Profile	SmartCard PRI/PRO			1.3.171.1 <b>.1.10.3.26</b>	0.4.0.194112.1.2
	20	Lux rust Smart Card QCF-11-qscd Certificate Frome	Signature Certificate	-	-	1.3.171.1.11.10.3.20	0.4.0.194112.1.2
	07	Les Trans Ocean Ocean NODe Confiference Destite	SmartCard PRI/PRO			4 2 474 4 4 40 2 27	0.4.0.0040.4.0
	27	LuxTrust Smart Card NCP+ Certificate Profile	Authentication Certificate	1-	-	1.3.171.1 <b>.1.10.3.27</b>	0.4.0.2042.1.2
	28	LuxTrust Smart Card LORA NCP+ - Signature	SmartCard LORA			4 2 474 4 4 40 2 20	0.4.0.0040.4.0
	28	Certificate for LRAO Purposes	Signature Certificate	]	-	1.3.171.1 <b>.1.10.3.28</b>	0.4.0.2042.1.2
		LuxTrust Smart Card LORA NCP+ - authentication	SmartCard LORA				0.4.0.2042.1.2
	29	Certificate for LRAO Purposes	Authentication Certificate	-	-	1.3.171.1 <b>.1.10.3.29</b>	
	30	LuxTrust eID Smart Card QCP-n-qscd Certificate	eID SmartCard			1.3.171.1 <b>.1.10.3.30</b>	0.4.0.194112.1.2
	30	Lux riust eid Smart Card QCF-II-qScd Certificate	Signature Certificate		-	1.3.171.1.11.10.3.30	0.7.0.134112.1.2
	31	LuxTrust elD Smart card NCP+ Certificate	eID SmartCard			4 2 474 4 4 40 2 24	0.4.0.2042.1.2
	31	Lux rrust eid Smart card NCP+ Certificate	Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.31</b>	0.4.0.2042.1.2
	32	LuxTrust Signing Server QCP-n-qscd Certificate	Signing Server certificate for qualified signature	-	-	1.3.171.1. <b>1.10.3.32</b>	0.4.0.194112.1.2
	33	LuxTrust Signing Server QCP-I-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1. <b>1.10.3.33</b>	0.4.0.194112.1.3
	34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171. <b>1.1.10.3.34</b>	0.4.0.194112.1.2
	35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171. <b>1.1.10.3.35</b>	0.4.0.2042.1.2
	36	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile			1.3.171.1.1.10.3.36	0.4.0.2042.1.3
5 LuxTrust SSL CA	1	SSL/TLS Standard Server Certificates	SSL/TLS Standard Server Certificates		-	1.3.171.1 <b>.1.10.5.1</b>	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. <b>1.10.5.2</b>	0.4.0.2042.1.4



VERSION 1.27

	3	SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	-	-	1.3.171.1. <b>1.10.5.3</b>	0.4.0.2042.1.5
	4	Object Signing(+) Certificates	Object Signing(+) Certificates	-	-	1.3.171.1. <b>1.10.5.4</b>	0.4.0.2042.1.3
	5	SSL/TLS Client Certificate	SSL/TLS Client Certificate	-	-	1.3.171.1. <b>1.10.5.5</b>	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. <b>1.10.5.6</b>	0.4.0.194112.1.4
8 LuxTrust Global Timestamping CA Certificates	1	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate	-	-	1.3.171.1 <b>.1.10.8.1</b>	0.4.0.2042.1.3
<b>4</b> LuxTrust Corporate CA	1	LuxTrust Corporate LCP Certificate Profile	LCP Corporate Certificate used for authentication purposes	-	-	1.3.171.1.1.10.4.1	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	xTrust Gl	obal Root	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 CA Signature	
Validity					
NotBefore		Х		Key Generation Process Date/Time	
NotAfter		Х		Key Generation Process Date/Time + 10;20 years	Fixed
SubjectPublicKeyInf o		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 <sup>1</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Root x <sup>1</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies <sup>2</sup>	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.1.10	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 <sup>6</sup>		

 $<sup>^{1}</sup>$  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.

<sup>&</sup>lt;sup>2</sup> Since LuxTrust Global Root 2



	Lu	xTrust 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		X		SHA-1 Hash	
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE <sup>6</sup>		
CA		X		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		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 <sup>1</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA x <sup>3</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		

<sup>&</sup>lt;sup>3</sup> 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.



	L	uxTrust Glob	al Qualifie	ed CA	
Base Profile	OID	Include d	Critical	Value	
policyldentifier		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 <sup>6</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyldentifie 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 <sup>5</sup> .crl	Fixed
BasicConstraints	{id-ce 19}	Х	TRUE <sup>6</sup>	N/A	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

### 1.9LuxTrust SSL CA

	LuxTrust SSL CA							
Base Profile	OID	Included	Critical	Value				
Version		X		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				

<sup>&</sup>lt;sup>4</sup> Since LuxTrust Global Qualified CA 3

 $<sup>^{5}</sup>$  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

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



LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value				
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 <sup>1</sup>	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
Subject								
CountryName	{ id-at-6 }	Х		LU	Fixed			
CommonName	{ id-at-3 }			LuxTrust SSL CA x <sup>7</sup>	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
CertificatePolicies	{id-ce 32}	Х	FALSE					
policyldentifier (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			
policyldentifier (2)	{ anyPolicy }	Х		2.5.29.32.0	Fixed			
policyQualifiers (2)				N/a				
policyQualifierId (2)								
Qualifier (2)								
KeyUsage	{id-ce 15}	Х	TRUE <sup>6</sup>					
keyCertSign				Set	Fixed			
crlSign				Set	Fixed			
authorityKeyldentifier	{id-ce 35}	Х	FALSE		1			
Keyldentifier		Х		SHA-1 Hash of Authority public key	1			
authorityInfoAccess <sup>8</sup>	{id-pe 1}		False					
AccessMethod accessLocation	{Id-ad-1}	Х		http://ltgroot.ocsp.luxtrust.lu	Fixed			
AccessMethod	{Id-ad-2}	^	False		i ixeu			
accessLocation		Х		http://ca.luxtrust.lu/LTGRCAx17.crt	Fixed			
subjectKeyldentifier	{id-ce 14}	Х	FALSE					
Keyldentifier		Х		SHA-1 Hash of Subject public key				
cRLDistributionPoints	{id-ce 31}	Х	FALSE					

 $<sup>^{7}</sup>$  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.

<sup>&</sup>lt;sup>8</sup> Since LuxTrust SSL CA 4



	LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value					
distributionPoint									
FullName		X		http://crl.luxtrust.lu/LTGRCAx1.crl	Fixed				
BasicConstraints	{id-ce 19}	X	TRUE <sup>6</sup>	N/a					
CA		X		TRUE	Fixed				
pathLenConstraint		X		0 (Zero)	Fixed				

## 1.10 LuxTrust TSA (Timestamping) CA

	LuxTru	st Global 1	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 <sup>1</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA x <sup>9</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.10.8	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier		Х		https://repository.luxtrust.lu	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.



	LuxTru	ust Global 1	Timestamp	ping CA	
Base Profile	OID	Included	Critical	Value	
KeyUsage	{id-ce 15}	Х	TRUE <sup>6</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyldentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess10	{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/LTGRCAx1.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 <sup>5</sup> .crl	Fixed
Basic Constraints	{id-ce 19}	Х	TRUE <sup>6</sup>	N/a	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

## 1.11 LuxTrust Corporate CA

	LuxTrust Corporate CA							
Base Profile	OID	Included	Critical	Value				
Version		Х		V3				
SerialNumber		Х		Random CSN				
SignatureAlgorithm								
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed			
SignatureValue		Х		Issuing LTGRCA2 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).				

 $<sup>^{10}\,\</sup>mathrm{Since}\,\mathrm{LuxTrust}\,\mathrm{Global}\,\mathrm{Timestamping}\,\,\mathrm{CA}\,\mathrm{2}$ 



	Lu	xTrust Co	orporate	: CA	
Base Profile	OID	Included	Critical	Value	
				20 years certificate requires a 4096 key length.	
Issuer					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }	Х		LuxTrust Global Root 2	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Corporate CA x	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.1.10.4	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 <sup>6</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{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/LTGRCA2.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/LTGRCA2.crl	Fixed
BasicConstraints	{id-ce 19}	Х	TRUE	N/A	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed



#### 1.11.1 Certificate extensions

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

## 1.11.2 Algorithm object identifiers

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

#### 1.11.3 Name forms

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

#### 1.11.4 Name constraints

Name constraints are supported as per RFC 5280.

#### 1.11.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

#### 1.11.6 Usage of Policy Constraints extension

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

#### 1.11.7 Policy qualifiers syntax and semantics

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

#### 1.12 LuxTrust End-entity - Certificates profiles

#### 1.12.1 Certificate profiles

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

For the purpose of integration with current devices such as the smartcard, the signing stick and signing server, the following five types of LuxTrust Certificates will be issued under the 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+<sup>11</sup> Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy QID 1.3.171.1.10.3.1, and
  - signatures, under the Certificate Policy OID 1.3.171.1.1.10.3.1, and

    One LuxTrust NCP+<sup>12</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.2.

Under eIDAs regulation, those profiles are updated to the following certificate policies:

- LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.26.
- LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1]
  (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key
  pairs, according to two certificate policies
  - One LuxTrust QCP<sup>11</sup> 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 NCP<sup>12</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.10.3.4.
- LuxTrust Signing Server Accounts (Virtual Smartcards): These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy
   One LuxTrust NCP<sup>12</sup> certificate for Natural Persons for the combined purposes of electronic signature,
  - One LuxTrust NCP<sup>12</sup> 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 1.3.171.1.10.3.21

<sup>&</sup>lt;sup>11</sup> As defined by ETSI TS 101 456 (cf. [3]).

 $<sup>^{12}</sup>$  As defined in ETSI TS 102 042 (cf. [4]).





 LuxTrust Advanced eSeal - Certificate Profile supporting authentication under the Certificate Policy OID 1.3.171.1.10.3.22

#### The advanced eSeal product is based on two certificate policies:

- LuxTrust Advanced eSeal Certificate Profile supporting signature under the Certificate Policy OID 1.3.171.1.10.3.23.
- LuxTrust Advanced eSeal Certificate Profile supporting authentication under the Certificate Policy OID 1.3.171.1.10.3.24.

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 1.3.171.1.10.5.1.
- 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 1.3.171.1.10.5.2.
- 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.

#### 1.12.2 Version number(s)

X.509 v3 is supported and used.

## 1.12.3 LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures

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

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

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

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

	LuxTrust SSCD QCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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 Global Qualified CA x <sup>17</sup>			
	organizationName	✓			S	LuxTrust S.A.			

<sup>&</sup>lt;sup>13</sup> IN = Included: Attribute / field included within the certificate profile.

 $^{15}$  O/M: O = Optional, M = Mandatory.

 $<sup>^{14}</sup>$  CE = Critical Extension.

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

 $<sup>^{17}</sup>$  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.



	Lux	Trust SS	CD QC	P+ Cert	tificate	e Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Validity		✓	False			
	NotBefore	<u>√</u>			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		<b>√</b>	False			IVIOLITIS
	serialNumber	<b>√</b>	. 4.00	М	D	Serial Number as constructed by LRAO
	Schantaniber			101		, ,
	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	<b>√</b>		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	<b>√</b>		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	dentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified
authorityInfo	Access	<b>√</b>	False			CA public key
addiontyiiil	AccessMethod	<u>√</u>	1 4130			Id-ad-2
	accessLocation	<b>√</b>			<u> </u>	http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓	<u> </u>		<del>                                     </del>	Id-ad-1
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribut		✓	False			mapar qualitud pilaki dutilar
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
	l		1		1	p.,, ormani domar E i Odor in Ton

<sup>18</sup> SINCE LTGQCA3



	LuxTrust SSCD QCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
Subject									
Properties									
subjectAltNa		✓	False						
	Rfc822Name	✓		0	D	Certificate Holder's email address			
subjectKeylo		✓	False						
	keyldentifier	<b>~</b>			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 bitstring bits).			
Policy						-			
Properties									
keyUsage		✓	True						
	digitalSignature	✓			S	False			
	nonRepudiation	✓			S	True			
	keyEncipherment	✓			S	False			
	dataEncipherment	✓			S	False			
certificatePo	licies	✓	False						
	Policyldentifier	✓				1.3.171.1.1.10.3.1			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	<b>√</b>				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	✓				0.4.0.1456.1.1			
QualifiedCer	tificateStat								
	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	✓		М	D	0.4.0.1862.1.4			

#### 1.12.4 LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption

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

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

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

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

	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
,					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
,					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.				



	Lux	xTrust	SSCDI	NCP+ Cer	tificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	1= .	<b>√</b>	False			
	NotBefore NotAfter	<b>√</b>			D D	Certificate generation process date/time.
	NotArter	•			ט	Certificate generation process date/time + 36 Months
subject		✓	False			World
	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
	- Contantantico	-		IVI		,
	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	<b>✓</b>		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	<b>√</b>		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	<b>√</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<b>*</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	<b>~</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPubli		✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA); public
Extensions	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Authority						
Properties						
authorityKey	dentifier	<b>✓</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust Global
	<b>A</b>					Qualified CA public key
authorityInfo		<b>√</b>	False			ld od 2
	AccessMethod accessLocation	<b>✓</b>				Id-ad-2 http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
		· ·				
	AccessMethod accessLocation	<b>✓</b>				Id-ad-1
cRLDistribut		· ·	Eoloo			http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
CKLDISTIDUT	distributionPoint	<b>✓</b>	False		S	
	arati ibuti On F On it		<u> </u>	l	_ S	



	Lu	ıxTrust	SSCD N	NCP+ Ce	rtificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ime	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		✓	False			
	keyldentifier	<b>*</b>			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	✓				1.3.171.1.1.10.3.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers	<b>_</b>				
	DisplayText	<b>V</b>				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

#### 1.12.5 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 1.3.171.1.110.3.3>.

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

	LuxTrust non SSCD QCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile	e									
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	alue	✓	False							
					D	Issuing CA Signature.				



LuxTrust non SSCD QCP Certificate Profile						
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x 17
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity		<b>√</b>	False			
	NotBefore	<b>√</b>			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	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>✓</b>		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	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>✓</b>		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	<b>~</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitName 2	<b>~</b>		0	D	PRO products only: Company/institution department or other information item
subjectPublicKeyInfo		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyldentifier		✓	False			



	Lu	xTrust	non SS	CD QCP	Certific	cate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key
authorityIn	foAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistrib	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Pro	pperties					
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	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 Prop	perties					
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP	Policies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	<b>✓</b>				LuxTrust Qualified Certificate not on SSCE 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





#### 1.12.6 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

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

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

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

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

	LuxT	rust non	SSCD 1	NCP Cert	tificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile						
Version	T	✓	False		S	Version 3 Value = "2"
SerialNumb	er	<b>✓</b>	False		3	Version 3 value = 2
Ochaniani	T	•	i aise		FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
-:	I					with RSA Encryption.
signatureVa	liue 	· ·	False		D	Issuing CA Signature.
issuer		<b>√</b>	False		S	issuing CA Signature.
100001	countryName	<b>√</b>	1 4130		S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	<b>√</b>	1		S	LuxTrust S.A.
Validity		✓	False	_		
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	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	<b>✓</b>		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	<b>✓</b>		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)



	LuxTrus	t non	SSCDI	NCP Cert	ificate l	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationalUnitName 1	~		M for PRO prod., conditional (O) for PRIV	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:
	organizationalUnitName 2	<b>✓</b>		prod.)	D	" & (Date of birth + 18 years).  PRO products only:  Company/institution department or other information item
subjectPubli	icKeyInfo	✓	False			
	algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey	yldentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key
authorityInfo		✓ ✓	False			14 - 4 0
	AccessMethod accessLocation	<b>∨</b>				Id-ad-2
						http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓ ✓				Id-ad-1
	accessLocation		L			http://qca.ocsp.luxtrust.lu/18
cRLDistribut		<b>√</b>	False			
	distributionPoint fullName	✓ ✓			S	
	tuliname	· ·				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties subjectAltNa	ama ama	<b>✓</b>	Foloo			
SubjectAitina	Rfc822Name	<b>V</b> ✓	False	0	D	Certificate Holder's email address
subjectKeylo		·	False	- 0		Certificate Floider's email address
oubjectivey.	keyldentifier	<b>√</b>	T disc		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			
neyosaye	digitalSignature	<b>√</b>	True		S	True
	nonRepudiation				S	False
	keyEncipherment	<b>√</b>			S	True
oortific-t-D	dataEncipherment	✓ ✓	Folse		S	True
certificatePo	Policyldentifier	<b>∨</b>	False			1.3.171.1.1.10.3.4
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>		<del>                                     </del>	S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					, \
	DisplayText	<b>√</b>				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption.
	Policyldentifier	✓				0.4.0.2042.1.1





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

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

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

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

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

	LuxTrus	st Signing	Serve	r NCP C	ertificat	e Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version	•	<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlo		✓	False			
oign oturo Vo	algorithm		False		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	-	raise		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	133ung OA Signature.
.50401	countryName	<b>√</b>	1 4130		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	ga=a	✓	False			Edit 1 dot 0.7 ti
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		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	<b>√</b>		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	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)



	LuxTrust	Signin	g Serve	r NCP C	ertificat	te Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
				0,111		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)
	organizationalUnitName 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à"  & (Date of birth + 18 years).
	organizationalUnitName 2	✓		0	D	PRO products only:  Company/institution department or other
						information item
subjectPubli	icKeyInfo	✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA)
Futanciana	subjectPublicKey	<b>✓</b>		M		public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey	/Identifier	<b>✓</b>	False			
uu.iioiiiyitoj	keyldentifier	<b>√</b>	1 0.00			SHA-1 Hash of the LuxTrust Globa
						Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint	✓			S	17
	fullName	✓				http://crl.luxtrust.lu/LTGQCA 17.crl
Subject Properties			F-1			
subjectAltNa	Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
subjectKeylo		\ \ \	False	U	U	Certificate Holder's email address
Subjectivelyi	keyldentifier	· ·	i dise		Fixed	The Key Identifier comprises a four-bifield with a 0100 value, followed by the least significant 60 bits of the SHA-1 hast of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy						
Properties keyUsage		<b>✓</b>	True			
neyusaye	digitalSignature	<b>√</b>	ilue		S	True
	nonRepudiation				S	True
	keyEncipherment	<b>✓</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo		✓	False			
·	Policyldentifier	✓				1.3.171.1.1.10.3.5
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers				1	



	LuxTrust Signing Server NCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
	DisplayText	<b>✓</b>				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Signature, Data or Entity Authentication and Data Encryption.				
	Policyldentifier	✓				0.4.0.2042.1.1				

#### 1.12.8 LuxTrust NCP+ Certificates supporting Mass Signature Services

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

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

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

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

LuxTrust	non SSCD NCP+ Publi	c Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		<b>√</b>	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	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	T	<b>√</b>	False			
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + <b>36</b> Months
subject		✓	False			
	commonName	<b>✓</b>		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	<b>✓</b>		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)



LuxTrust	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationalUnitName 1	✓		0	D	As provided by Subscriber
						,
	organizationalUnitName 2	<b>✓</b>		0	D	As provided by Subscriber
	gaa =					The provided by Gabbelines
subjectPublicKeyInfo		<b>✓</b>	False			
casjoon associations	algorithm	<b>√</b>	. 4.00			Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
<b>Authority Properties</b>						
authorityKeyldentifier		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global
						Qualified CA public key
authorityInfoAccess	A a a a a BA - db - d	✓ ✓	False			11 - 10
	AccessMethod	✓ ✓				ld-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint		✓	False		_	
	distributionPoint	<b>√</b>			S	17
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx 17.crl
Subject Properties						
subjectAltName	I	<b>√</b>	False		_	
1: 45 11 45	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKeyldentifier	least dentifier	<b>✓</b>	False		F	The Manual description of the bit
	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		<b>√</b>	True		_	
	digitalSignature	✓			S	False
	nonDonudiction				S	True
	nonRepudiation				3	True
	keyEncipherment	<b>√</b>			S	False
	y=noipnoimont					1 4.00
	dataEncipherment	✓			S	False
	•					
certificatePolicies		✓	False			
	Policyldentifier	✓				1.3.171.1.10.3.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers	<b>✓</b>				Lui Truck Contification of Continue
	DisplayText	<b>'</b>				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	<b>✓</b>	İ	ĺ	İ	0.4.0.2042.1.2

## 1.12.9 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]).

## **LuxTrust Global Root CA Certificate Specifications**





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

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

Astribute   Field   Nt   CE*   O/M   CO*		table provides the description					icate Profile
Profition	Attribute						
SerialNumber							
SerialNumber			<b>√</b>	Falso			
SerialNumber	VCISION			1 alse		S	Version 3 Value = "2"
SignatureAlgorithm	SerialNumbe	r	✓	False			
Algorithm   S   D(D = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.		tab				FDV	Validated on duplicates.
SignatureValue	signatureAig		<b>V</b>	Faise		S	OID = "1 2 840 113549 1 1 11" - SHA256 with RSA
Ssuer		Aigorium					
Salur	signatureVal	ue	✓	False			
CountryName	laguer		-/	Folos			Issuing CA Signature.
CommonName	issuer	countryName		Faise			111
Validity   Validity							<del></del>
Validity		organizationName	<b>√</b>			S	
NotAfter	Validity	<b>J</b>	✓	False		_	
Subject   SerialNumber   V   False   M   D   Serial Number as constructed by LRAO							
SerialNumber   V   M   D   Serial Number as constructed by LRAO	Cubicat	NotAfter		Folos		D	Certificate generation process date/time + 36 Months
commonName  commonName  divenName   Subject	a a wi a l N la sua la a u		raise	N.4	_	Contal Number on an according to deliver DAO	
givenName		seriainumber	<b>v</b>		IVI	D	Senai Number as constructed by LRAU
surname		commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s)
CountryName		givenName	<b>✓</b>		M	D	TEST ONLY + " " + As provided by Subscriber
emailAddress  Title  M  D  Reprovided by Subscriber  PRIVATE products:  Fixed value: "Private Person" PRO products:  "Professional Person" (default) or "Professional Administrator" PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.  IocalityName  M  D  PRO products only: Company/institution country of HQ (as in articles of association)  PRO products only: Company/institution country of HQ (as in articles of association)  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  organizationalUnitName 3  O  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).  PRO products only: Company/institution department or other information item  SubjectPublicKey		surname	✓		М	D	As provided by Subscriber
emailAddress		countryName	✓		М	D	LU
Title  Title  M  D  PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator"  Name of company/institution as in articles of association or equivalent documents, including the legal form.  IocalityName  M  D  PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.  PRO products only: Company/institution country of HQ (as in articles of association)  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).  PRO products only: Company/institution department or other information item  SubjectPublicKey  Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).		-	./				As provided by Subscriber
Title    M		emanaduress	•		0	D	As provided by Subscriber
organizationName  ✓ M D Name of company/institution as in articles of association or equivalent documents, including the legal form.  IocalityName  ✓ M D PRO products only: Company/institution country of HQ (as in articles of association)  FRO 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  organizationalUnitName 2  O D PRO products only: Company/institution department or other information item  subjectPublicKeyInfo Algorithm Algorithm Algorithm Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm Algorithm SubjectPublicKey Algorithm Algo		Title	<b>√</b>		М	D	Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional
organizationName  ✓ M D Name of company/institution as in articles of association or equivalent documents, including the legal form.  IocalityName  ✓ M D PRO products only: Company/institution country of HQ (as in articles of association)  FRO 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  organizationalUnitName 2  O D PRO products only: Company/institution department or other information item  subjectPublicKeyInfo Algorithm Algorithm Algorithm Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm SubjectPublicKey Algorithm Algorithm SubjectPublicKey Algorithm Algo							PRO products only:
organizationalUnitName 1  OrganizationalUnitName 1  OrganizationalUnitName 1  OrganizationalUnitName 1  OrganizationalUnitName 2  OrganizationalUnitName 2  OrganizationalUnitName 2  OrganizationalUnitName 3  OrganizationalUnitName 4  OrganizationalUnitName 5  OrganizationalUnitName 7  OrganizationalUnitName 8  OrganizationalUnitName 9  OrganizationalUnit		organizationName	<b>√</b>		М	D	Name of company/institution as in articles of association or equivalent documents, including the
organizationalUnitName 1  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).  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).  PRO products only: Company/institution department or other information item  subjectPublicKeyInfo Algorithm Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).		localityName	✓		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
organizationalUnitName 2			<b>~</b>		PRO prod., conditional (O) for PRIV	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
Algorithm     ✓     Public Key: Key length: 2048bit (RSA); public subjectPublicKey     ✓     M     exponent: Fermat-4 (=010001).		2			0	D	Company/institution department or other information
subjectPublicKey   ✓   M   exponent: Fermat-4 (=010001).	subjectPubli			False			Dubling Kong Kong Inggeling CO (CC) (CC)
					N/I		
EXTERNIORS	Extensions	aubjectrublichey	· ·		IVI		охронени т еннас <del>ч</del> (=010001).



	Lu	ıxTru	st Integ	gration	Certif	icate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	N/A
subjectKeylo		✓	False			
	keyldentifier	<b>✓</b>			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	<b>✓</b>				1.3.171.1.1.10.3.7
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.3

#### 1.12.10 LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption

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

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

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

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

	LuxTrust SSCD LCP+ Integration Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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	signatureValue										
					D	Issuing CA Signature.					



	LuxTru					
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 3
						Months
Subject		✓	False			
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
						LGQCA XX SC PRI V3 (XX a numb
	commonName	✓		M	D	selected internally by LuxTrust)
	givenName	✓		М	D	LGQCA XX (XX a number selected internal
						by LuxTrust)
	Surname	✓		М	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	✓	1	0	D	N/A
		-	1		<u> </u>	Britania Barrara
	Title	✓	<u></u>	М	D	Private Person
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); publ
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust Global Qualifie
						CA public key
authorityInfo		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>✓</b>				http://qca.ocsp.luxtrust.lu/
cRLDistribut	tionPoint	✓	False			
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						TREAT CHILDREN TO COLOR
Properties subjectAltNa		<b>✓</b>	False			
SubjectAlliva	Rfc822Name	\ \ \ \	raise	0	D	N/A
subjectKeylo		<b>V</b> ✓	Foloo	U	<u> </u>	IV/A
	keyldentifier	<u> </u>	False		Fixed	The Key Identifier comprises a four-bit field wi a 0100 value, followed by the least significa 60 bits of the SHA-1 hash of the value subjectPublicKey bit string (tag, not includir the length and number of unused bit-strir bits).
Policy Properties						
keyUsage		<b>√</b>	True			
, osage	dinital@:		Tiue		_	T
	digitalSignature	<b>✓</b>	1		S	True
	nonRepudiation		ļ		S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓	<u>L</u>		S	True
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.8
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE
						SSCD compliant with ETSI TS 102 042 LCF certificate policy. Key Generation by CSP. Sc Authorised Usage: Authentication at



LuxTrust SSCD LCP+ Integration Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value		
						Encryption for Integration Purposes.		
	Policyldentifier	✓				0.4.0.2042.1.3		

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

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

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

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

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

	Luxiii	aot Olgiiii	_			te Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
	L				FDV	Validated on duplicates.
signatureAl		✓	False			010
	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	ilue	✓	False			
laguer		<b>✓</b>	False		D S	Issuing CA Signature.
Issuer	countryName	<b>✓</b>	Faise		S	LU
	commonName	· ·			S	LuxTrust Global Qualified CA x <sup>17</sup>
		· ·			S	
organizationName		<b>✓</b>	False		5	LuxTrust S.A.
Validity	NotBefore	V	raise		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	<b>✓</b>		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	<b>✓</b>		М	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s) as on ID document
	Surname	<b>✓</b>		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
subjectPubl		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).



	LuxTru	st Signin	_	r LCP C	ertificat	
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Extensions						
Authority						
Properties						
authorityKey		<b>√</b>	False			CIIA 4 Hash of the LuxTrust Clabel
	keyldentifier					SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ume.	<b>√</b>	False			
SubjectAitiva	Rfc822Name	-	i aise	0	D	N/A
subjectKeylo		· ·	False			I IVA
	keyldentifier	<b>*</b>			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	<b>√</b>			S	True
	nonRepudiation				S	True
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.9
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>*</b>				INTEGRATION Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Signature, Data or Entity Auth. and Data Enc. for integration purposes
	Policyldentifier	✓				0.4.0.2042.1.3

## 1.12.12 LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes

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

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

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

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

	LuxTrust SSCD LORA QCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			



	LuxTrı	ıst SSCD	LORA	QCP+	Certific	ate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base	1 1010			· · · · · · · · · · · · · · · · · · ·		7 3.1 3.0
Profile						
Version		✓	False			
0 : 11					S	Version 3 Value = "2"
SerialNumbe	er I	✓	False		FDV	Validated on dunlinates
signatureAlg	orithm	<b>√</b>	False		FDV	Validated on duplicates.
SignatureAig	Algorithm		i alsc		S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer	oountryNomo	<b>√</b>	False		S	LU
	countryName commonName	<b>→</b>			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName				S	LuxTrust Global Qualified CA x  LuxTrust S.A.
Validity	Organizationivanie	<b>→</b>	False		3	Lux Tiust S.A.
validity	NotBefore	✓	i alsc		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
						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
	Surname	<b>√</b>		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	<b>√</b>		М	D	"LuxTrust RA Officer"
	organizationName	<b>√</b>		M	D	Constructed by LuxTrust
	organizationitanic			141		Constructed by EaxTract
	localityName	✓		M	D	Country of RA
	organizationalUnitName 1	<b>√</b>		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	✓		М	D	RAO code Constructed by LuxTrust
subjectPubli		✓	False			
	Algorithm	✓			ļ	Public Key: Key length: 2048bit (RSA); public
Evtersion	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey	Identifier	✓	False			
,,	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistribut		✓	False			
	distributionPoint	<b>√</b>			S	17
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						
Properties subjectAltNa	uma .	<b>√</b>	False			
SubjectAitNa	Rfc822Name	<b>✓</b>	i alse	0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False			Standard Horder & Chian address
Sasjootitoyic			i aloc			



	LuxTrust SSCD LORA QCP+ Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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	False				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificatePo	olicies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.10				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>~</b>				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Support of Qualified Electronic Signature for LRAO purposes				
	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 compliance with [3]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }				

## 1.12.13 LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes

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

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

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

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

	LuxTrust SSCD LORA NCP+ Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	r	✓	False							
					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 <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				



	LuxTrı	ıst SS	CD LOF	RA NCP+	Certific	ate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Validity	2 27	✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36
						Months
Subject	Γ	✓	False			
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		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
	localityName	✓		М	D	Country of RA
	organizationalUnitName 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	✓		М	D	RAO code Constructed by LuxTrust
subjectPubli		✓	False			
	Algorithm	<b>√</b>		N 4		Public Key: Key length: 2048 bit (RSA); public
Extensions	subjectPublicKey	<u> </u>		M		exponent: Fermat-4 (=010001).
Authority						
Properties authorityKey	Idontifior	<b>√</b>	False			
authoritykey	keyldentifier	√ ·	i aise			SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	<b>√</b>	False			Qualifica Cry public Key
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>✓</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	ionPoint	<b>√</b>	False			THE TY QUAL COOP TO ALL COLORS
OI (EDIOLIDA)	distributionPoint	<b>√</b>	1 0100		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx 17.crl
Subject Properties						110000000000000000000000000000000000000
subjectAltNa	me	<b>√</b>	False			
	Rfc822Name	<b>√</b>	. 2.50	0	D	Certificate Holder's email address
subjectKeylo	lentifier	✓	False			
	keyldentifier	<b>√</b>			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	True
certificatePo	licies	✓	False			
_						



	LuxTrust SSCD LORA NCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
	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	<b>✓</b>				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			

#### 1.12.14 LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures

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

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

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

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

	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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	alue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust <b>Global Qualified</b> CA x <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	<b>✓</b>			D	Certificate generation process date/time.				
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 36 Months				
Subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		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				



	LuxTrust non SS	SCD Q	CP Mas	ss LRAO	Signat	ures Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	Surname	<b>√</b>		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 – LRS"
	organizationName	✓		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA
	localityName	<b>~</b>		М	D	Country of RA (as in articles of association)
	organizationalUnitName 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	✓		0	D	RAO code Constructed by LuxTrust
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 Global Qualified CA public key
authorityInf	oAccess	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribu	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Pro	perties					
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyl	Identifier	✓	False			
	keyldentifier	<b>✓</b>			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			



	LuxTrust non S	SCD Q	CP Mas	ss LRAO	Signat	tures Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	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	<b>✓</b>				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	rtificateStat					
	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

## 1.12.15 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]).

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust elD SSCD QCP+ Certificate Profile										
Attribute	Field	IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>	CO <sup>22</sup>	Value					
Base											
Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg	jorithm	✓	False								

 $<sup>^{19}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certificate profile.

 $<sup>^{20}\,\</sup>mathrm{CE}$  = Critical Extension.

 $<sup>^{21}</sup>$  O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>22</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



SignatureValue	LuxTrust elD SSCD QCP+ Certificate Profile										
signature/alue	Attribute		IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>						
Super		Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with				
Saurance	-:	June 1		Falsa			RSA Encryption.				
Second   S	signatureva	liue 	<b>V</b>	Faise		D	Issuing CA Signature				
CountryName	Issuer		<b>√</b>	False			issuing CA Signature.				
CommonName	100001	countryName	<b>√</b>	1 0.00			LU				
Validity			✓				LuxTrust Global Qualified CA x <sup>23</sup>				
Validity		organizationName	<b>√</b>			S					
NotAfter	Validity	, , , , , , , , , , , , , , , , , , , ,	✓	False		_					
Subject											
SerialNumber		NotAfter				D	maximum 120 Months; Certificate generation process date/time + 1				
commonName	Subject	T		False							
Surname   V		serialNumber	✓		М	D	-				
Surname  Subject's email address  If the holder is underage: 'Mineur jusqu'à : ' & (Date of birth + 18 years).  Subject's email address  Mineur jusqu'à : ' & (Date of birth + 18 years).  Subject's email address  Suphiect Key: Key length: 2048bit up to 4096bit (Date of birth + 18 years).  Subject Reyldentifier  SHA-1 Hash of the LuxTrust Global Qualified  CRA y public exponent: Fermat-4 (=010001).  SHA-1 Hash of the LuxTrust Global Qualified  CRA y public key  SHA-1 Hash of the LuxTrust Global Qualified  CRA y public key  SHA-1 Hash of the LuxTrust Global Qualified  CRA y public key  Subject key  Subject Reyldentifier  SHA-1 Hash of the SHA-1 Hash of the LuxTrust Liu/LTGQCAx 17 crt  Id-ad-1  Id-ad-2  http://cral.luxtrust.lu/LTGQCAx 17 crt  Subject Altiname  Subject Altiname  Subject Altiname  Fixed  The Key Identifier comprises a four-bit field with a 0100 value, followed by the leas significant Gots of the SHA-1 hash of the value or subject Public Key bit string (tag, no including the length and number of unused bit string bits).  Policy  Properties  Gigital Signature  S False		commonName	✓		М	D	surname(s) separated by the space character				
Surname  Surname  Surname  Surname  CountryName  CountryN		givenName	<b>✓</b>		М	D					
emailAddress		Surname	<b>√</b>		М	D	"épouse", 'ép." or similar and the subsequent				
Title		countryName	✓		М	D	LU				
organizationalUnitName 1		emailAddress			0	D	Subject's email address				
subjectPublicKeyInfo Algorithm SubjectPublicKey Algorithm SubjectPublicKey Authority Properties AuthorityKeyIdentifier AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessLocation AccessMethod AccessLocation AccessLocati		Title	✓		М	D	"Private Person"				
Algorithm		1			0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).				
SubjectPublicKey	subjectPubl			False							
Extensions Authority Properties authorityKeyldentifier    Value   False   SHA-1   Hash of the LuxTrust Global Qualified CA x public key					N 4						
Authority Properties authorityKeyldentifier    keyldentifier	Extensions	SubjectFublickey	<b>V</b>		IVI		(NSA), public exponent. Fermat-4 (=010001).				
Reyldentifier   V	Authority Properties										
authorityInfoAccess  AccessMethod accessLocation AccessMethod accessLocation AccessMethod accessLocation AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessLocation AccessMethod AccessLocation AccessMethod AccessLocation AccessMethod AccessMetho	authorityKe			False							
AccessMethod accessLocation   V		-	<b>√</b>								
AccessLocation AccessMethod accessLocation AccessMethod accessLocation Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Subject Brition AccessLocation Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  AccessLocation Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl  Antip://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crl	authorityInf		✓	False							
AccessMethod accessLocation   Id-ad-1   http://qca.ocsp.luxtrust.lu/ 18											
accessLocation    CRLDistributionPoint   False			,			ļ					
CRLDistributionPoint						<b>_</b>					
distributionPoint   v	-DI D'- ( ''			+			http://qca.ocsp.luxtrust.lu/				
Subject   Properties   Subject AltName   ✓ False   O D   Subject email address	CKLDISTRIBU			False		9					
Subject Properties subject AltName  Rfc822Name  ✓ False  SubjectKeyldentifier  Keyldentifier  ✓ False  Fixed  Fix				+		3	https://ord.hustrucht.ls/I.TCOCA17				
SubjectAltName	•	TullName	•				nttp://cri.luxtrust.lu/L1GQCAx .cri				
Rfc822Name ✓ False  subjectKeyldentifier ✓ False  keyldentifier ✓ False  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 False		ame	_	Falso							
subjectKeyldentifier  keyldentifier  ✓ False  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 False	SubjectAitiv			i aise	0	D	Subject email address				
Keyldentifier	subjectKeyl			False							
Properties     LeyUsage     ✓ True       digitalSignature     ✓ S False			<b>V</b>			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).				
keyUsage     ✓     True       digitalSignature     ✓     S     False	Policy Properties										
				True							
		digitalSignature nonRepudiation	✓ ✓			S	False True				

-

 $<sup>^{23}</sup>$  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.



	Lux	Trust eID	SSCD Q	CP+ Ce	rtifica	te Profile
Attribute	Field	IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>	CO <sup>22</sup>	Value
	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					
	DisplayText	<b>~</b>				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	✓				0.4.0.1456.1.1
QualifiedCer	tificateStat					
	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	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

#### 1.12.16 LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption

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

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

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust SSCD NCP+ Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg	orithm	✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVal	ue	✓	False			21					
					D	Issuing CA Signature.					
issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Global Qualified CA x17					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
•	NotBefore	✓			D	Certificate generation process date/time.					



	Lux	Trust	SSCD N	NCP+ Cer	tificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	NotAfter	<b>√</b>			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
subject	·	✓	False			0 : 44 4 500
	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	<b>√</b>		М	D	"Private Person"
		•		IVI		111 111
	organizationalUnitName 1	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli	cKeyInfo algorithm	<b>√</b>	False			Public Key: Key length: 2048 bit up to 4096bit
	subjectPublicKey	<i>'</i>		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties authorityKey	  dentifier	<b>√</b>	False			
	keyldentifier	✓	. 4.00			SHA-1 Hash of the LuxTrust Global Qualified
						CA x public key
authorityInfo	Access AccessMethod	<b>✓</b>	False			Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		<b>√</b>	False			
	distributionPoint fullName	<b>√</b>			S	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject	Tullivallic	-				nttp://cri.luxtrust.lu/LTGQCAX .cri
Properties						
subjectAltNa	-	<b>√</b>	False			Outriest amount and the
subjectKeyld	Rfc822Name	<b>√</b>	False	0	D	Subject email address
<u> </u>	keyldentifier	<b>√</b>	i alse		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		<b>√</b>	True			
, coage	digitalSignature	· ✓	Truc		S	True
	nonRepudiation				S	
	keyEncipherment	<b>√</b>			S	False True
		·	<del>                                     </del>			
	dataEncipherment		F='		S	True
certificatePo	Policyldentifier	<b>√</b>	False			1.3.171.1.1.10.3.14
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers			1		



	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	oute Field IN <sup>13</sup> CE <sup>14</sup> O/M <sup>15</sup> CO <sup>16</sup> Value									
	DisplayText	<b>√</b>				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				

### 1.12.17 LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures

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

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

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust elD SSCD LCP Integration Signature Certificate Profile										
Attribute	Field	IN <sup>24</sup>	CE <sup>25</sup>	O/M <sup>26</sup>	<b>co</b> <sup>27</sup>	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	<b>✓</b>			S	LuxTrust Global Qualified CA x <sup>28</sup>					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	<b>√</b>			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					

<sup>&</sup>lt;sup>24</sup> IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{25}</sup>$  CE = Critical Extension.

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

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

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



	LuxTrust eID S	SCD LCP	Integra	ation Sig	gnature	e Certificate Profile
Attribute	Field	IN <sup>24</sup>	CE <sup>25</sup>	O/M <sup>26</sup>	<b>CO</b> <sup>27</sup>	Value
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	<b>√</b>		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	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli		✓	False			
	Algorithm subjectPublicKey	✓ ✓	1	М		Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	SubjectFublicKey	V		IVI		(NOA), public exponent. Fermat-4 (=010001).
Authority						
Properties						
authorityKey		<b>√</b>	False			SHA-1 Hash of the LuxTrust Global Qualified
	keyldentifier	<b>'</b>				CA x public key
authorityInfo	Access	✓	False			Orth passe ney
•	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	distributionPoint	✓ ✓	False		S	
	fullName	<b>V</b> ✓			3	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						TILID://CIT.idxtrdst.id/ETGQCAX :CIT
Properties						
subjectAltNa		✓	False			
	Rfc822Name	<b>√</b>		0	D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo		✓	False			
	keyldentifier	<b>√</b>			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	T	✓	True			
	digitalSignature	✓ ✓	1		S	False
	nonRepudiation keyEncipherment	<b>✓</b>			S	True False
	dataEncipherment	<i>'</i>			S	False
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.16
	policyQualifierID qualifier	✓ ✓			S	Id-qt-1 (CPS)
	policyQualifierID	<b>∨</b>	1		S	https://repository.luxtrust.lu Id-qt-2 (User Notice)
	noticeNumbers					ia qi 2 (osci Nolloc)
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Electronic signature for Integration Purposes.
	Policyldentifier	✓				0.4.0.1456.1.1
QualifiedCer		,				0.4.0.4000.4.4
	QcCompliance QcLimitValue	<b>√</b>		<u>М</u> О	S D	O.4.0.1862.1.1  As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]

### **LuxTrust Global Root CA Certificate Specifications**





#### 1.12.18 LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption

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

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

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust ell	D SSCI	D LCP I	ntegratio	n AE Ce	ertificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	r	✓	False		ED) /	N P. L. L. P. J.
alamatuma Alam	a nith me	<b>✓</b>	Falsa		FDV	Validated on duplicates.
signatureAlg	algorithm	· ·	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	aigoritiiii				3	RSA Encryption.
signatureVal	ue	<b>√</b>	False			1 Contendigues.
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			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
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	<b>✓</b>		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).
subjectPublic		✓	False			
-	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						



	LuxTrust el	D SSCI			n AE Ce	ertificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified
						CA x public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx 17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						The profit of the control of the con
Properties						
subjectAltNa	me	<b>√</b>	False			
,	Rfc822Name	<b>✓</b>		0	D	specimen-x Subject's email address as
						provided by the RNCID
subjectKeylo	lentifier	✓	False			
	keyldentifier	<b>✓</b>			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		<b>√</b>	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.17
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					L T . INTEGRATION CERTIFICATE
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Authentication and Encryption for Integration Purposes
	Policyldentifier	✓				0.4.0.2042.1.2

### 1.12.19 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.



LuxTrust	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile	Tield	114	CL	O/IVI	- 00	Value
Version		<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" -
signatureValue		<b>√</b>	False			SHA256 with RSA Encryption
Signaturevalue			i aise		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	recarring on Congressions.
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process
aubiast		,	F-1			date/time + 36 Months
subject	T	✓	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	<b>✓</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>✓</b>		0	D	As provided by Subscriber
	organizationalUnitName 2	<b>✓</b>		0	D	As provided by Subscriber
subjectPublicKeyInfo	almanish m	<b>√</b>	False			Public Keep Keep Land Control to Control
	algorithm	<b>✓</b>		N //		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	subjectPublicKey	V		М		Public exponent. Fermat-4 (=010001).
Authority Properties						
authorityKeyldentifier		<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfoAccess		✓	False			
	AccessMethod	<b>√</b>				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint		✓	False			
	distributionPoint	<b>√</b>			S	47
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						



LuxTrust	LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
subjectAltName		✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKeyldentifier		✓	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	<b>✓</b>			S	False					
	dataEncipherment	<b>✓</b>			S	False					
certificatePolicies		✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.15					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	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					

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

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

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

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

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

LuxTrust SSL Server LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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 <b>SSL</b> CA x <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							



	LuxTrus	t SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
1 1101 110 1110	NotBefore	<b>√</b>			D	Certificate generation process
	NotAfter	<b>√</b>			D	date/time.  Certificate generation process date/time
	NotAiter	•				+ 12:24:36 Months
subject		✓	False			
	countryName	<b>✓</b>		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	<b>√</b>		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	<b>✓</b>		M	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName1	✓		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber
	commonName	<b>✓</b>		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	<b>√</b>		0	D	Serial Number as provided by subscriber
	emailAddress	<b>√</b>		0	D	Subject's email address
subjectPubli	icKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
Authority Properties	d do natifica	<b>✓</b>	Falsa			
authorityKey	keyldentifier	<b>V</b> ✓	False			SHA-1 Hash of the LuxTrust SSL CA
	-					public key
authorityInfo		✓	False			
	AccessMethod accessLocation	✓ ✓				ld-ad-1
	AccessMethod	·				http://ssl.ocsp.luxtrust.lu <sup>29</sup> Id-ad-2
	accessLocation	· ·				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt
cRLDistribut		<b>√</b>	False			nttp://ca.luxtrust.lu/L155LCAx .crt
O. (LDIOLIDA)	distributionPoint	<b>✓</b>	1 0.00		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl
SCTs		<b>✓</b>	False	М	D	Values returned by Log Servers
Subject						
Properties subjectAltNa	ame	<b>√</b>	False			
- Casjeotriiii	Rfc822Name	· ·	1 4100	0	D	Certificate Holder's email address
	SubjectAltName-dNSName	✓ <b>/</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.

<sup>&</sup>lt;sup>29</sup> Since SSL CA 2



	LuxTrus	t SSL S	erver LC	P Certif	icate Pro	ofile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	SubjectAltName-dNSName	<b>√</b>		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	<b>√</b>		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	<b>✓</b>		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	<b>√</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>√</b>		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	<b>√</b>		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	<b>✓</b>		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	<b>√</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>√</b>		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.



	LuxTrust SSL Server LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
	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		✓	False								
	keyldentifier	<b>*</b>			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	<b>√</b>			S	True					
	nonRepudiation	<b>√</b>			S	False					
	keyEncipherment	<b>√</b>			S	True					
	dataEncipherment	<b>√</b>			S	True					
certificatePo	licies	<b>√</b>	False								
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.5.1					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	Policyldentifier	✓				0.4.0.2042.1.3					
	Policyldentifier					2.23.140.1.2.2					
Extended Ke	Extended Key Usage		False								
	serverAuth	✓			S	True					
	clientAuth	✓			S	True					
	emailProtection	✓			S	True					

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

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

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

Prohibited Certificate uses:

### **LuxTrust Global Root CA Certificate Specifications**





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

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

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

### Verification of Applicant's Legal Existence and Identity:

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

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

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

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

	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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.				
signatureVal	ue	✓	False							
					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		<b>✓</b>	False							
•	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 12;24 Months				
subject		✓	False							
	countryName (OID: 2.5.4.6)	~		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)				



	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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)	<b>√</b>		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)	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)				
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>√</b>		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)	<b>√</b>		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)	<b>~</b>		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.				



	SSL/TLS Ex	tended \	/alidatio	on Serv	er Cert	tificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
7 ttt ibato	streetAddress		<u> </u>	0	D	Number and Street of the physical
	(OID: 2.5.4.9)	✓				location of the subject
	(OID. 2.3.4.9)					
subjectPublic	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
Futanciana	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA
auth aritudata	Access	<b>✓</b>	Folso			public key
authorityInfo	AccessMethod	<b>V</b> ✓	False			Id-ad-1
	accessLocation	<b>✓</b>				http://ssl.ocsp.luxtrust.lu <sup>29</sup>
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx 17.crt
cRLDistribut	ionPoint	<b>✓</b>	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx17.crl
F =			<u> </u>			
SCTs		✓	False	M	D	Values returned by Log Servers
Subject Properties						
subjectAltNa	me	<b>√</b>	False			
casjoon and	SubjectAltName-dNSName		1 4100	М		FQDN (Fully Qualified Domain Name) of
	•					application/server - Exact DNS for a
		<b>√</b>				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
		<b>√</b>				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
	O L : (AKA) INON					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
	SubjectAltName-dNSName		+	0	<del> </del>	allowed for EV SSL Certificates  FQDN (Fully Qualified Domain Name) of
	- Lasjood attaine artoriane					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		1	0		FQDN (Fully Qualified Domain Name) of
	_					application/server - Exact DNS for a
			1			Web Server or IP address or unique
		<b>√</b>	1			name of server, owned or controlled by the subject and to be associated with the
						Subject's server. Wildcard name not
			<u>L</u>		<u> </u>	allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
			1			application/server – Exact DNS for a
		<b>✓</b>				Web Server or IP address or unique name of server, owned or controlled by
		'				the subject and to be associated with the
			1			Subject's server. Wildcard name not
						allowed for EV SSL Certificates.



SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
	SubjectAltName-dNSName	<b>~</b>		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	<b>✓</b>		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	<b>✓</b>		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	<b>√</b>		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		✓	False						
	keyldentifier	<b>*</b>			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	<b>√</b>			S	True			
	nonRepudiation	<b>√</b>			S	False			
	keyEncipherment	✓			Ø	True			
	dataEncipherment	<b>✓</b>			S	True			
certificatePo		✓	False						
	Policyldentifier	✓				1.3.171.1.1.10.5.2			
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	Policyldentifier	✓				0.4.0.2042.1.4			
	Policyldentifier	✓	L			2.23.140.1.1			
Extended Ke		<b>√</b>	False						
	serverAuth	✓			S	True			
	clientAuth	<b>√</b>	ļ		S	True			
	emailProtection	✓	Ĺ		S	False			

# 1.12.22 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).

#### **LuxTrust Global Root CA Certificate Specifications**

**VERSION 1.27** 



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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

#### Prohibited Certificate uses:

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

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

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

#### Verification of Applicant's Legal Existence and Identity:

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

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

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

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

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

SSL/TLS Extended Validation Server Certificates on Secure User Device								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value		
Base								
Profile								
Version		✓	False					



	SSL/TLS Extended Validation	n Serv	er Certi	ficates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
					S	Version 3 Value = "2"
SerialNumbe	e <b>r</b> T	✓	False		ED) (	N E L C L L E L
signatureAlg	orithm	<b>√</b>	False		FDV	Validated on duplicates.
SignatureAig	Algorithm		raise		S	OID = "1.2.840.113549.1.1.11" -
	Algorium					SHA256 with RSA Encryption.
signatureVal	ue	✓	False			•
		ļ			D	Issuing CA Signature.
Issuer	I construction Allows	✓ ✓	False		S	
	countryName commonName	<b>✓</b>			S	LU 17 1991 OA 17
		· ·			S	LuxTrust <b>SSL</b> CA x <sup>17</sup> LuxTrust S.A.
Validity	organizationName	<b>✓</b>	False		3	Luxifust S.A.
validity	NotBefore	<i>'</i>	1 also		D	Certificate generation process
	1101201010					date/time.
	NotAfter	✓			D	Certificate generation process
						date/time + 12;24 Months
Subject	T	✓	False			
	countryName			M	D	Country in which the company's or
	(OID: 2.5.4.6)	<b>✓</b>				institution's registered office is established (as specified in the
		•				memorandum and articles of
						association). (ISO3166)
	jurisdictionCountryName			М	D	Contains the country information
	· ·			IVI	D	Contains the country information specified using the applicable ISO
	(OID: 1.3.6.1.4.1.311.60.2.1.3)					country code for the jurisdiction of
		<b>✓</b>				Incorporation for the Incorporating
						Agency or Jurisdiction of
						Registration for a Registration Agency that operates at the country
						level, at state/pr.
	stateOrProvinceName			М	D	State or Dravines in which the
				IVI	D	State or Province in which the company's registered office is
	(OID: 2.5.4.8)	<b>✓</b>				established (as specified in the
		•				memorandum and articles of
						association or an equivalent
						document)
	jurisdictionStateOrProvinceName			0	D	Contains the jurisdiction for the
	(OID: 1.3.6.1.4.1.311.60.2.1.2)					applicable Incorporating Agency or
		✓				Registration Agency at the state or province level MUST include both
						country and state or province
						information,
	localityName			М	D	Location in which the company's
	(2.5.4.7)			IVI		registered office is established (as
	(2.3.4.7)	✓				specified in the memorandum and
						articles of association or an
						equivalent document)
	jurisdictionLocalityName			0	D	Jurisdiction for the applicable
	(1.3.6.1.4.1.311.60.2.1.1)					Incorporating Agency or Registration
	,					Agency at the locality level MUST
		<b>✓</b>				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
		ļ				information.
	organizationName		1	М	D	Full legal organization name as
	(OID: 2.5.4.10)					listed in the official records of the
		<b>✓</b>	1			Incorporating or Registration Agency in the Subject's Jurisdiction of
						Incorporation or Registration or as
			1			otherwise verified by the CA as
						provided herein
		_	_			-



	SSL/TLS Extended Validation	Serve	er Certif	ficates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	businessCategory (OID: 2.5.4.15)	<b>~</b>		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)	<b>√</b>		M	D	See EV Guidelines [13]: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.  For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject
	postalCode (OID: 2.5.4.17)	<b>✓</b>		0	D	is a Government Entity.  Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	<b>✓</b>		0	D	Number and Street of the physical location of the subject
subjectPublic	- KeyInfo	<b>√</b>	False			
SubjectFubili	Algorithm	<b>√</b>	i aise			Public Key: Key length: 2048 bit
	subjectPublicKey	√ ·		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties	dead(Con		Falsa			
authorityKey	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-1
	accessLocation	✓		<u> </u>		http://ssl.ocsp.luxtrust.lu <sup>29</sup>
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx 17.crt
cRLDistributi		✓	False			
	distributionPoint	✓			S	
	fullName	✓		<u> </u>		http://crl.luxtrust.lu/LTSSLCAx17.crl
Subject Properties						
subjectAltNa	SubjectAltName-dNSName	✓	False	M		FQDN (Fully Qualified Domain Name) of application/server – Exact
		<b>✓</b>				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		er Certif	icates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	SubjectAltName-dNSName	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>✓</b>		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 Valid	dation Serv	er Certi	ficates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>✓</b>			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	<b>√</b>			S	True
	nonRepudiation	<b>✓</b>			S	False
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo	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	ey Usage	✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

# 1.12.23 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 <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	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	<b>✓</b>			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>					



	ı	_uxTrust	LCP Code	Signing C	ertificate F	Profile		
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value		
	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 registered office is established (as specified in the memorandum and articles of association). (ISO3166)		
	stateOrProvinceName	✓		0	D			
	localityName	<b>√</b>		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	<b>✓</b>		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	<b>✓</b>		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	s							
Authority	Properties							
authorityK	Keyldentifier	✓	False					
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key		
authoritylı	nfoAccess	✓	False					
	AccessMethod	✓				ld-ad-1		
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu <sup>29</sup>		
	AccessMethod	✓				Id-ad-2		
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt		
CRLDistril	butionPoint	✓	False					
	distributionPoint	✓			S			
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx17.crl		
Subject Pr	Subject Properties							
subjectAlt	Name	✓	False					
	Rfc822Name	✓		0	D	Subject's email address		
subjectKe	yldentifier	✓	False					
			l .					



	LuxTrust LCP Code Signing Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
	keyldentifier	<b>√</b>			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										
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	Id-qt-1 (CPS)					
	Qualifier	✓			S	http://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	~			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on <a href="http://repository.luxtrust.lu">http://repository.luxtrust.lu</a> . Signed by an SSL CA.					
	Policyldentifier	✓			S	0.4.0.2042.1.3					
Extended	Key Usage	✓	False								
	Object Signing	✓			S	Set					

### 1.12.24 LuxTrust SSL/TLS Certificate for Client Authentication

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

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

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

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

	LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		<b>√</b>	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	<b>✓</b>	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	<b>✓</b>	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	<b>√</b>			S	LuxTrust SSL CA				



	LuxTru	st SSL	Client I	LCP Cer	tificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationName	✓			S	LuxTrust S.A.
Validity	N-(D-fore	<b>√</b>	False			0 00 1
	NotBefore NotAfter	✓ ✓			D D	Certificate generation process date/time.  Certificate generation process date/time +
	Notate	'				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)
				_	_	atticles of association). (1303100)
	stateOrProvinceName	✓		0	D	
	localityName			M	D	Location in which the company's
		✓				registered office is established (as
						specified in the memorandum and articles of association or an equivalent document)
					<u> </u>	
	organizationName			M	D	Names as in articles of association, including the legal form (as specified in the
		✓				memorandum and articles of association
						or an equivalent document)
	organizationalUnitName 1			0	D	As provided by Subscriber
	. 9	<b>✓</b>			-	The provided by Cabbonics.
	organizationalUnitName 2	<b>✓</b>		0	D	As provided by Subscriber
	commonName	<b>✓</b>		М	D	As provided by Subscriber
	serialNumber	<b>√</b>		0	D	Serial Number as provided by subscriber
		+ -				, ,
	emailAddress	<b>✓</b>		0	D	Subject's email address
subjectPubli		✓	False			
	Algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA);
Extensions	subjectPublicKey	<b>√</b>		M		public exponent: Fermat-4 (=010001).
Authority						
Properties						
authorityKey		<b>√</b>	False			
	keyldentifier	<b>*</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfo	Access	✓	False			public key
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>✓</b>				http://ssl.ocsp.luxtrust.lu <sup>29</sup>
	AccessMethod	<b>√</b>				ld-ad-2
	accessLocation	<b>V</b>	<b>_</b>			http://ca.luxtrust.lu/LTSSLCAx17.crt
cRLDistribut	tionPoint distributionPoint	✓ ✓	False		S	
	fullName	· /			3	http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl
Subject						INDITIONAL USE IN LEGISLA CONTROL CONT
Properties						
subjectAltNa		✓	False		1	Contilionto Holdenia accessi.
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False			
	keyldentifier	<b>✓</b>			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
Policy						of unused bit-string bits).
Properties						
keyUsage	1	<b>√</b>	True			
	digitalSignature	<b>✓</b>		1	S	True
	nonRepudiation	<b>✓</b>	1		S	False
		1	Ī	1	1	1



	LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
	keyEncipherment	<b>√</b>			S	True				
	dataEncipherment	<b>✓</b>			S	True				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.5.5				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	Policyldentifier	✓				0.4.0.2042.1.3				
Extended Ke	y Usage	<b>√</b>	False							
	serverAuth	✓			S	False				
	clientAuth	✓			S	True				
	emailProtection	✓			S	True				

### 1.12.25 SSL/TLS QCP-w Extended Validation Server Certificates

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

	SSL/TLS QCP-w					Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile		<b>√</b>	Falsa			
Version		V	False		S	Version 3 Value = "2"
SerialNumbe	er	<b>√</b>	False		3	Version 3 value - 2
OCH I III I I I I I I I I I I I I I I I I			1 dioc		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 commonName	✓ ✓			S	LU 17
		-			_ ~	LuxTrust SSL CA x <sup>17</sup>
M = 11 -114	organizationName	✓ ✓	F-1		S	LuxTrust S.A.
Validity	NotBefore	<b>✓</b>	False		D	Cartificate generation process data/time
	NotAfter	<b>✓</b>			D	Certificate generation process date/time  Certificate generation process date/time
	Notatiei					+ 12:24 Months
subject	1	✓	False			,
	countryName (OID: 2.5.4.6)	<b>✓</b>		М	D	Country in which the company's constitution's registered office is established (as specified in the memorandum and articles association). (ISO3166)
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)  stateOrProvinceName (OID: 2.5.4.8)	1	<b>✓</b>		М	D	Contains the country information specified using the applicable ISC country code for the jurisdiction of Incorporation for the Incorporation Agency or Jurisdiction of Registration for a Registration Agency that operates a the country level, at state/pr.
	<b>√</b>		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)	<b>√</b>		0	D	Contains the jurisdiction for the applicable Incorporating Agency of Registration Agency at the state of province level MUST include bottountry and state or province information,



	SSL/TLS QCP-w	Extend	ed Valid	lation S	erver (	Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	localityName (2.5.4.7)	<b>√</b>		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>√</b>		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)	<b>~</b>		M	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	<b>√</b>		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)	<b>*</b>		M	D	See EV Guidelines [13]:  For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.  For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	<b>√</b>		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		<b>√</b>	False			Public Keep Keep II 00 10 11 (DO)
	algorithm subjectPublicKey	<b>√</b>		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	SubjectFubilities	· ·		IVI		Public expolicit. I eliliat-4 (=010001).
Authority Properties						
authorityKey		<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://ssl.ocsp.luxtrust.lu <sup>29</sup>
	AccessMethod	<b>√</b>				Id-ad-2
-DI D' - ''	accessLocation		F			http://ca.luxtrust.lu/LTSSLCAx17.crt
cRLDistributi	onPoint	✓	False			



	SSL/TLS QCP-w	Extend	ed Valid	dation S	Server	Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx17.crl
SCTs		✓	False	М	D	Values returned by Log Servers
Subject					_	
Properties						
subjectAltNa		✓	False			
	SubjectAltName-dNSName	<b>✓</b>		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	<b>√</b>		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	<b>√</b>		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	<b>√</b>		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	<b>~</b>		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	<b>~</b>		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	<b>*</b>		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	<b>✓</b>		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.



	SSL/TLS QCP-	w Extend	led Valid	dation S	Server (	Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	SubjectAltName-dNSName	<b>*</b>		O		FQDN (Fully Qualified Domain Name) of application/server — Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeylo	lentifier	✓	False			
	keyldentifier	<b>V</b>			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		<b>✓</b>	Terre			
keyUsage	di mital Ci ma atuma	· ·	True			T
	digitalSignature	v			S	True
	nonRepudiation	<b>✓</b>			S	False
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>✓</b>			S	False
certificatePo	licies	✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.5.6
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	<b>✓</b>			S	https://repository.luxtrust.lu
	Policyldentifier	<b>✓</b>				0.4.0.194112.1.4
	Policyldentifier	<b>√</b>				0.4.0.2042.1.4
	Policyldentifier	<b>✓</b>			S	2.23.140.1.1
Extended Ke	y Usage	✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓		1	S	False
QualifiedCer		<b>✓</b>	False			
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>✓</b>		М	S	https://www.luxtrust.lu/upload/data/repos itory/PDS.pdf
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-web (0.4.0.1862.1.6.3)

#### 1.12.26 LuxTrust SPARE Signing Server LCP Certificate Profile

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

These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]). The usage purpose of these Certificates is only authentication <OID 1.3.171.1.1.10.3.20>.

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

	SPARE LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value				
Base Profile										
Version			False							



						icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
					S	Version 3 Value = "2"
			<u> </u>			
SerialNumbe	r		False			
					FDV	Validated on duplicates.
signatureAlg	a vith va		Falsa			
SignatureAig	Orithin		False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA250 with RSA Encryption.
signatureVal	ue		False			
	T				D	Issuing CA Signature.
Issuer			False		S	
	countryName				S	LU
	commonName				S	LuxTrust Global Qualified CA x
	Commonwanie					Luxitusi Globai Qualified CA X
	organizationName				S	LuxTrust S.A.
Validity			False			
	NotBefore				D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time + 3 Months
Subject			False			
	serialNumber			М	D	Serial Number as constructed by LRAO
	commonName			М	D	LGQCA XX CSS (XX a number selecter 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 selecter internally by LuxTrust) or Given name(s as on ID document
	Surname			М	D	CSS or Surname(s) as on ID documer without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName			М	D	LU or Nationality of holder (ISO3166)
	emailAddress			0	D	N/A
	Title			M	D	Private Person
subjectPubli	cKeyInfo		False			
	Algorithm					Public Key: Key length: 2048 bit (RSA public exponent: Fermat-4 (=010001).
	subjectPublicKey		†	M		1



						cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Extensions						
A 41 14						
Authority Properties						
authorityKeyl	dentifier		False			
uuoy.toy.	uo		1 dioc			
	keyldentifier					SHA-1 Hash of the LuxTrust Globa Qualified CA public key
authorityInfo/	Access		False			
	AccessMethod					ld-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod					ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>23</sup>
cRLDistribution	<u> </u> onPoint		False			
	distributionPoint				S	
						23
	fullName					http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						
subjectAltNar	ne		False			
	Rfc822Name			0	D	N/A
subjectKeylde	entifier		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 unuse bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
certificatePoli	icies		False			
	Policyldentifier					1.3.171.1.1.10.3.20
	policyQualifierID				S	Id-qt-1 (CPS)
	Qualifier				S	https://repository.luxtrust.lu
	Policyldentifier			1	1	0.4.0.2042.1.3





#### 1.12.27 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 Certificates is limited to sole authorised usage of supporting the creation of qualified eseals supported by Qualified Certificate compliant with ETSI EN 319 411-2 [20] QCP-l-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.21>. The following table provides the description of the fields for LuxTrust Qualified Certificates for digital signatue purpose.

	LuxTrust Qualified eSEAL Certificate Profile										
Attribute	Field	IN <sup>30</sup>	CE <sup>31</sup>	O/M <sup>32</sup>	CO33	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		✓	False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>34</sup>					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	✓			D	Certificate generation process date/time + 24 Months					
Subject	<u> </u>	✓	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)					

 $<sup>^{30}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certify cate profile.

 $<sup>^{31}</sup>$  CE = Critical Extension.

 $<sup>^{32}</sup>$  O/M: O = Optional, M = Mandatory.

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

 $<sup>^{34}</sup>$  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.



	organisationIdentifier (2.5.4.97)	<b>✓</b>		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	<b>✓</b>		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	<b>✓</b>		0	D	Company/institution department or other information item
	serialNumber	<b>✓</b>		М	D	Serial Number as constructed by LRAO
subjectPubli	cKevinfo	<b>√</b>	False			
Casjooti asii	Algorithm	· ✓	. 4.50			Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	· ✓		М	<del>                                     </del>	public exponent: Fermat-4 (=010001).
Extensions	Subjecti ubilcitey	,		IVI		public experient. Fernat + (-010001).
A						
Authority						
Properties authorityKey	(Idontifior	<b>√</b>	Fo!ss			
aumontyney		<b>∨</b>	False			SHA 1 Hoch of the LuxTruct Clabel Qualified CA sublice
	keyldentifier	<b>'</b>				SHA-1 Hash of the LuxTrust Global Qualified CA public
outhouts dut-	A 00000	<b>√</b>	Fals -			key
authorityInfo		<b>∨</b>	False			14 -4 0
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
DI DI CI	accessLocation	✓	<b>.</b>			http://qca.ocsp.luxtrust.lu/35
cRLDistribut		<b>√</b>	False		_	
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeylo	dentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>	2.30		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).

<sup>35</sup> SINCE LTGQCA3





Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo	olicies	✓	False			
	Lux	xTrust	NCP+	Certifica	te Profi	le for authentication
						1.0.17 1.1.1.10.0.21
	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	rtificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	<b>✓</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	<b>✓</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

### 1.12.28 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>.





Passe   Profile   Profil	Attribute	Field	IN <sup>36</sup>	CE <sup>37</sup>	O/M <sup>38</sup>	CO <sub>39</sub>	Value
SerialNumber							
SerialNumber							
SerialNumber	Version	T	<b>V</b>	False			Marriage O Malua (60)
SignatureAlgorithm	0! - 101 1			F-1		S	version 3 value = "2"
SignatureAlgorithm	Seriainumbe	er	V	Faise		ED\/	Validated on dunlicates
Social Country Name	signaturo Alo	l sorithm	1	Falco		FDV	validated on duplicates.
Encryption   Encryption	SignatureAig		1	i aise		S	OID = "1 2 840 113549 1 1 11" - SHΔ256 with RSΔ
SignatureValue		/ igoriami					
Issuer	signatureVal	lue	✓	False			
CountryName						D	Issuing CA Signature.
CommonName	Issuer		✓	False		S	<u> </u>
Validity			✓				
NotBefore			✓			S	
NotBefore   V		organizationName	✓			S	LuxTrust S.A.
NotAfter	Validity			False			
CommonName							
countryName  M D Shall contain the full registered name of the subject (legal person).  the country in which the subject (legal person) is established (ISO3166)  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 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 uniformResourceIdentifier.  Shall contain the full registered name of the subject (legal uniformResourceIdentifier).		NotAfter				D	Certificate generation process date/time + 24 Months
countryName  M D erson). the country in which the subject (legal person) is established (IsO3166)  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 trae 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.	Subject		<b>✓</b>	False			
organisationIdentifier (2.5.4.97)  M D established (ISO3166)  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 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.  Shall contain the full registered name of the subject (legal		commonName	✓		М	D	person).
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 an attional 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.  Shall contain the full registered name of the subject (legal		countryName	✓		М	D	
TODANIZANONNAME TV T TWI TI TO T		_	<b>*</b>		M	D	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
		organizationName	<b>✓</b>		М	D	Shall contain the full registered name of the subject (legal person).

 $<sup>^{36}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certify cate profile.

 $<sup>^{37}</sup>$  CE = Critical Extension.

<sup>&</sup>lt;sup>38</sup> O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>39</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $<sup>^{40}</sup>$  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.





	organizationalUnitName	✓		0	D	Company/institution department or other information item
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
subjectPubli	icKevInfo	✓	False			
•	Algorithm	<b>√</b>				Public Key: Key length: 2048bit up to 4096bit (RSA);
		LuyT	rust Adv	anced e	SEAL C	Sertificate Profile
Extensions		Luxi	rust Au	anoca	OLAL C	octanoate i Tome
Authority						
Properties						
authorityKey	vldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/41
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>√</b>			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
1	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	<b>√</b>				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			

### 1.12.29 LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature

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

41	SINCE	LTGQCA3
----	-------	---------





Attribute	Field	IN <sup>42</sup>	CE <sup>43</sup>	O/M <sup>44</sup>	CO <sup>45</sup>	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.
signatureVal	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>46</sup>
	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)	<b>*</b>		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).

 $<sup>^{\</sup>rm 42}$  IN = Included: Attribute / field included within the certify cate profile.

 $<sup>^{43}</sup>$  CE = Critical Extension.

<sup>44</sup> O/M: O = Optional, M = Mandatory.

<sup>45</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $<sup>^{46}</sup>$  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.





	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);
		LuxT	rust Adv	anced e	SEAL C	Sertificate Profile
Extensions						
Authority Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/4/
cRLDistribut		✓	False		_	
	distributionPoint	<b>√</b>			S	
	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	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.23
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

### 1.12.30 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

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

<sup>&</sup>lt;sup>47</sup> SINCE LTGQCA3





Attribute	Field	IN <sup>48</sup>	CE <sup>49</sup>	O/M <sup>50</sup>	CO <sup>51</sup>	Value
Base						
Profile						
Version	Г	✓	False		S	Version 3 Value = "2"
SerialNumbe	\	<b>√</b>	False		5	version 3 value = 2
Serialivumbe	<b>31</b>	•	raise		FDV	Validated on duplicates.
signatureAlg	l	<b>/</b>	False		FDV	Validated on duplicates.
SignatureAig	Algorithm	-	1 4136		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	7.1g01111111					Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	y y
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>52</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			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	<b>✓</b>		М	D	Shall contain the full registered name of the subject (legal person).
		1	<u> </u>	l	l	

 $<sup>^{48}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certify cate profile.

 $<sup>^{49}</sup>$  CE = Critical Extension.

<sup>50</sup> O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>51</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $<sup>^{52}</sup>$  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.





	organizationalUnitName	✓		0	D	Company/institution department or other information item
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>53</sup>
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	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	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.24
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
ļ	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

### 1.12.31 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.

<sup>&</sup>lt;sup>53</sup> SINCE LTGQCA3



Base   Profile	LuxTrust Advanced Automated eSEAL Certificate Profile											
Profile   Version	lue	Value	CO <sup>5</sup>	O/M <sup>56</sup>	CE <sup>55</sup>	IN <sup>54</sup>	Field	Attribute				
Version												
SerialNumber								Profile				
SerialNumber					False	✓		Version				
SignatureAlgorithm		Version 3 Value = "2"	S									
SignatureAlgorithm					False	✓	er	SerialNumbe				
SignatureValue		Validated on duplicates.	FDV									
SignatureValue					False	✓	gorithm	signatureAlg				
SignatureValue	1.11" - SHA256 with RSA	OID = "1.2.840.113549.1.1.11" - SHA256	S				Algorithm					
Issuer		Encryption.										
CountryName					False	✓	lue	signatureVal				
CountryName   CommonName   CountryName   CountryNam		Issuing CA Signature.										
CommonName					False			Issuer				
Validity						✓						
NotBefore   V	A x <sup>58</sup>	LuxTrust Global Qualified CA x <sup>58</sup>	S			<b>√</b>						
NotBefore   V		LuxTrust S.A.	S			✓	organizationName					
NotBefore   V					False	✓		Validity				
CommonName	s date/time.	Certificate generation process date/time.	D			✓	NotBefore					
commonName  countryName  M  D  Shall contain the full registere person).  the country in which the established (ISO3166)  Shall contain information usir the presented order: 3 character legal person iden 2 character ISO 3166 countr hyphen-minus "-" and identifier (according to countr reference). The three initial characters she defined values: 1) "VAT" for identification bas tax identification number. 2) "NTR" for identification bas national trade register. Or Two local definition within the sper registration authority, identify considered appropriate for national trade appropriate for national trade appropriate for national trade register.	s date/time + 24 Months	Certificate generation process date/time + 24	D			✓	NotAfter					
countryName  M D person).  the country in which the established (ISO3166)  Shall contain information usir the presented order: 3 character legal person iden 2 character ISO 3166 countr hyphen-minus "-" and identifier (according to countr reference). The three initial characters sh defined values: 1) "VAT" for identification bas tax identification number. 2) "NTR" for identification bas national trade register. Or Two local definition within the sper registration authority, identify considered appropriate for national trade register. The considered appropriate for national trade register. Or Inconsidered appropriate for national trade register. Or Inconsidered appropriate for national trade register. Or Inconsidered appropriate for national trade register.		<u>.</u>			False	✓		Subject				
established (ISO3166)  Shall contain information usir the presented order: 3 character legal person iden 2 character ISO 3166 countr hyphen-minus "-" and identifier (according to countr reference). The three initial characters sh defined values: 1) "VAT" for identification bas tax identification number. 2) "NTR" for identification bas national trade register. Or Tw local definition within the speregistration authority, identify considered appropriate for national trade register.	, , ,		D	М		✓	commonName					
the presented order: 3 character legal person iden 2 character ISO 3166 countr hyphen-minus "-" and identifier (according to countr reference). The three initial characters sh defined values: 1) "VAT" for identification bas tax identification number. 2) "NTR" for identification bas national trade register. Or Tw local definition within the sper registration authority, identify considered appropriate for na followed by the character ":" (colon).	subject (legal person) is	the country in which the subject (legal established (ISO3166)	D	М		✓	countryName					
(two characters followed by "nameRegistrationAuthorities SemanticsInformation (IETF) present and shall contain at lo	ntity type reference; ry code; ry and identity type hall have one of the following sed on a national value added sed on an identifier from a ro characters according to cified country and name ring a national scheme that is ational and European level, ty type reference is provided :"), the element of RFC 3739 [1]) shall be east a	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 defined values:  1) "VAT" for identification based on a national tax identification number.  2) "NTR" for identification based on an identificational trade register. Or Two characters accorded definition within the specified country and registration authority, identifying a national solutions of the properties of	D	М		<b>✓</b>						
		identity type reference following the ":" characteristic unique within the context of the specified uniformResourceIdentifier.			certify	vithin the	profile.	cate p				

<sup>55</sup> CE = Critical Extension.

<sup>56</sup> O/M: O = Optional, M = Mandatory.
57 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

<sup>&</sup>lt;sup>58</sup> 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.





					1	T
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/59
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	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	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePo		✓	False			
	Policyldentifier	<b>√</b>				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
	<b>.</b>					e

# 1.12.32 LuxTrust Smart Card QCP-n-qscd Certificate Profile

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

	LuxTrust Smart Card QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>60</sup>	CE <sup>61</sup>	O/M <sup>62</sup>	CO 63	Value					
Base Profile											

<sup>&</sup>lt;sup>59</sup> SINCE LTGQCA3

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

<sup>61</sup> CE = Critical Extension.

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

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



A44milata	Field	60	61	62	60	Value
Attribute	Field	IN <sub>60</sub>	CE <sup>61</sup>	O/M <sup>62</sup>	CO 63	Value
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False		FDV	Validated on duplicates
signature/	 Algorithm	<b>✓</b>	False		FDV	Validated on duplicates.
orgrideal or	Algorithm		1 4.00		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RS
signature\	/alue	<b>√</b>	False			Encryption.
signature	raiue	,	i aise		D	Issuing CA Signature.
ssuer		✓	False		S	5 5
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>64</sup>
/alidity	organizationName	✓ ✓	False		S	LuxTrust S.A.
allulty	NotBefore	<b>✓</b>	raise		D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months
Subject		✓	False			· ·
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	<b>PRO and PRIVATE products</b> : Concatenation of givename(s) and surname(s) as on ID card separated by "Space" character.
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) as on card
	surname	<b>✓</b>		М	D	PRO and PRIVATE products: Surname(s) as on 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
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	le 🗸		M	D	"Professional Person" (default) or "Profession
						Administrator"
						(Other titles possible for special purpose certificates)
						PRO products only:
						Name of company/institution as in articles
	organizationName	<b>√</b>		M	D	association or equivalent documents, including the legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country HQ (as in articles of association)
	organizationalUnit Name 1	<b>~</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT numb available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à: " & (Date birth + 18 years).
	organizationalUnit Name 2	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item
	blickovinte	<b>✓</b>	False			
subjectPu	blickeyinto					
subjectPu	Algorithm subjectPublicKey	√ ✓		М		Public Key: Key length: 2048bit (RSA); public exponer Fermat-4 (=010001).

\_

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



LuxTrust Smart Card QCP-n-qscd Certificate Profile									
Attribute	Field	IN <sup>60</sup>	CE <sup>61</sup>	O/M <sup>62</sup>	CO 63	Value			
					63				
Authorit									
y Properti									
es									
authorityK	eyldentifier	<b>✓</b>	False						
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key			
authoritylr	nfoAccess	<b>✓</b>	False			public key			
,	AccessMethod	✓				Id-ad-2			
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt			
	AccessMethod	✓				ld-ad-1			
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>65</sup>			
cRLDistrib	outionPoint	✓	False						
	distributionPoint	<b>√</b>			S	17			
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl			
Subject Properti									
es eubicat Alt	Nome	<b>√</b>	Folse						
subjectAlt	Name Rfc822Name	<b>∨</b>	False	0	D	Certificate Holder's email address			
subjectKe		· /	False	0	D	Certificate Florder's email address			
<b>,</b>	keyldentifier	<b>✓</b>	1 4.00		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						ouring bito).			
Properti									
es			_						
keyUsage	digitalSignature	<b>✓</b>	True		S	False			
	nonRepudiation	<b>✓</b>			S	True			
	keyEncipherment	<b>√</b>			S	False			
	dataEncipherment	✓			S	False			
certificate		✓	False						
	Policyldentifier	<b>√</b>				1.3.171.1.10.3.26			
	policyQualifierI D	✓			S	Id-qt-1 (CPS)			
	qualifier	<b>✓</b>			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	Policyldentifier	<b>✓</b>							
						0.4.0.194112.1.2			
QualifiedC	ertificateStat	<b>√</b>	False						
	QcCompliance	<b>√</b>	. 4.00	М	S	True			
	(0.4.0.1862.1.1)		<u> </u>						
	QcSSCD			М	S	True			
	(0.4.0.1862.1.4)								
	QcPDS	✓		М	S	https://www.luxtrust.lu/upload/data/repository/PD			
	(0.4.0.1862.1.5)					S.pdf			
	QcType	<b>√</b>		М	S	id-etsi-qct-esign			
	(0.4.0.1862.1.6)					5.5. 40t 66tgii			
	(/	1	1	I	1				

### 1.12.33 LuxTrust Smart Card NCP+ Certificate Profile

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

LuxTrust Smart	Card NCP+	Certificate	Prof	ile
----------------	-----------	-------------	------	-----

<sup>&</sup>lt;sup>65</sup> SINCE LTGQCA3





Attribute	Field	IN 66	CE <sub>67</sub>	O/M <sup>68</sup>	CO <sub>ea</sub>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False		==>:/	N 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
oi an oturo /	l a a vitla m	<b>√</b>	False		FDV	Validated on duplicates.
signature/	Algorithm	· ·	raise		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
oiemature)	,	<b>✓</b>	False		3	RSA Encryption.
signature	alue	•	raise		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	issuing OA Signature.
100001	countryName	<b>√</b>	1 aloo		S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>70</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	or gamzation tanto	<b>√</b>	False		J	Edit 1 dot 6.7 ti
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	<b>PRO and PRIVATE products</b> : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>✓</b>		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	<b>✓</b>		М	D	PRIVATE products:  Fixed value: "Private Person"  PRO products:  "Professional Person" (default) or  "Professional Administrator"  (Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>√</b>		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).

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

 $<sup>^{67}</sup>$  CE = Critical Extension.

<sup>68</sup> O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>69</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

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



	LuxTrust Smart Card NCP+ Certificate Profile											
Attribute	Field	IN 66	CE <sup>67</sup>	O/M <sup>68</sup>	CO <sub>ea</sub>	Value						
	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	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key						
authoritylr		✓	False									
	AccessMethod	✓				Id-ad-2						
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt						
	AccessMethod	✓				Id-ad-1						
	accessLocation	<b>✓</b>				http://qca.ocsp.luxtrust.lu/ <sup>71</sup>						
cRLDistrib	outionPoint	✓	False									
	distributionPoint	✓			S							
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl						
Subject Properti es												
subjectAlt		✓	False									
	Rfc822Name	✓		0	D	Certificate Holder's email address						
subjectKe		✓	False									
	keyldentifier	<b>√</b>			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	<b>√</b>			S	True						
	nonRepudiation	<b>✓</b>			S	False						
	keyEncipherment	✓ ✓			S S	True						
certificate	dataEncipherment	<b>∨</b>	False		3	False						
Scrincate	Policyldentifier	· /	i aise			1.3.171.1.1.10.3.27						
	policyQualifierID	·			S	Id-qt-1 (CPS)						
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu						
	policyQualifierID	✓			S	Id-gt-2 (User Notice)						
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2						

# 1.12.34 LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature

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 1.3.171.1.10.3.28>.

LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			

<sup>&</sup>lt;sup>71</sup> SINCE LTGQCA3



	LuxTrust Sr	nart C	ard LOF	RA NCP	+ - Sign	ature Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base	1.000					
Profile						
Version	T	✓	False		S	Version 3 Value = "2"
SerialNumb	er	<b>√</b>	False		3	Version 3 value - 2
					FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
signatureVa	lua	<b>√</b>	False			Encryption.
Signatureva		·	1 alsc		D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
N 12 12	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NotBefore	<b>√</b>	False		D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time.  Certificate generation process date/time + 36 Months
Subject	1100 1101	✓	False			Continuate generation process date time 1 20 months
-	serialNumber	✓		М	D	Serial Number as constructed by LRAO
					<del>-</del>	, i
	commonName	✓		M	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	<b>√</b>		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	<b>√</b>		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		<b>√</b>	False			
	Algorithm subjectPublicKey	<b>✓</b>		М		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extension	aunjecu-uniickey	,		IVI		охронона т синас <del>т</del> (=010001).
S						
Authority						
Properties authorityKe	yldentifier	<b>√</b>	False			
authorityNe	keyldentifier	<b>✓</b>	raise			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	oAccess	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		<b>√</b>	False			
	distributionPoint fullName	<b>✓</b>			S	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject	Tumtame					nup.//cri.iuxtrust.iu/LTGQCAX .cri
Properties						
subjectAltN	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyl	dentifier	✓	False			



	LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
	keyldentifier	<b>√</b>			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	olicies	✓	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	<b>✓</b>				0.4.0.2042.1.2					

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

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

	LuxTrust Smart Card LORA NCP+ - authentication Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumb	er	✓	False								
					FDV	Validated on duplicates.					
signatureAl		✓	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 <sup>17</sup>					
	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	<b>✓</b>		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					



( 6	Field  localityName  organizationalUnitNam	IN <sup>13</sup> ✓	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
( 6						
( 6		✓				
( 6				М	D	Country of RA
(	organizationalUnitNam					
(	OLUANIZALIONALUNILINALII					
(	e 1	✓		М	D	RA code Constructed by LuxTrust
•						
	organizationalUnitNam	✓		М	D	RAO code Constructed by LuxTrust
	e 2					To to ood oondradied by EaxTract
subjectPublic		✓	False			
_ <i></i>	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Extension						
S						
Authority Properties						
authorityKeylo	dentifier	<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA
	•					public key
authorityInfoA	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
1	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistributio	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						
Properties						
subjectAltNan		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylde		✓	False			
ļ	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						and a string and j.
Properties						
keyUsage		<b>√</b>	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	<b>√</b>			S	False
certificatePoli		<b>√</b>	False			
<u> </u>	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.29
L	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
 	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	Policyldentifier	V				0.4.0.2042.1.2
						0.4.0.2042.1.2

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

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.30>.



	LuxTrus	st eID :	Smart C	ard Q0	CP-n-qs	cd Certificate Profile
Attribute	Field	IN <sup>72</sup>	CE <sup>73</sup>	O/M 74	CO <sup>75</sup>	Value
Base						
Profile Version		<b>✓</b>	False			
VEISIOIT	1	*	i aise		S	Version 3 Value = "2"
SerialNumb	er	✓	False			voidin o value 2
					FDV	Validated on duplicates.
signatureAlo	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer	T	<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU 76
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>76</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	I	<b>√</b>	False			
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
Subject		✓	False			1 GEODGITTIN GGILINGAG
,	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	<b>✓</b>		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	<b>✓</b>		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		<b>√</b>	False			Bull K. K. I. d. ooks in the second of the s
	Algorithm	✓ ✓		N #		Public Key: Key length: 2048bit up to 4096bit (RSA);
Extension	subjectPublicKey	v		M		public exponent: Fermat-4 (=010001).
Authority Properties						
authorityKey	vldentifier	<b>✓</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfo	Access	<b>√</b>	False			F 3.2
	AccessMethod	<b>✓</b>				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		<b>√</b>	False			парл доалосорлиха изили
CITEDISTIBU	distributionPoint	· /	1 4130		S	
	fullName	·				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
	Tain tains	<u> </u>				http://cn.luxtrust.lu/LTGQGAX .Cff

 $<sup>^{72}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certificate profile.

 $<sup>^{73}</sup>$  CE = Critical Extension.

<sup>74</sup> O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>75</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $<sup>^{76}</sup>$  X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



	LuxTrust eID Smart Card QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>72</sup>	CE <sup>73</sup>	O/M 74	CO <sup>75</sup>	Value					
Subject Properties											
subjectAltNa	ame	✓	False								
	Rfc822Name	✓		0	D	Subject email address					
subjectKeyl	dentifier	✓	False								
	keyldentifier	<b>√</b>			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 bitstring bits).					
Policy Properties						· ·					
keyUsage		✓	True								
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificatePo	olicies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.30					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2					
QualifiedCe	rtificateStat	✓	False								
	QcCompliance (0.4.0.1862.1.1)	~		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	<b>✓</b>		М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf					
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign					

# 1.12.37 NCP+ supporting Authentication & Encryption for eID smart cards

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

	LuxTrust elD Smart card NCP+ Certificate Profile									
Attribute	Field	IN''	CE <sup>78</sup>	O/M 79	CO <sub>80</sub>	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				

 $<sup>^{77}\,\</sup>mbox{IN}$  = Included: Attribute / field included within the certificate profile.

<sup>&</sup>lt;sup>78</sup> CE = Critical Extension.

<sup>&</sup>lt;sup>79</sup> O/M: O = Optional, M = Mandatory.

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



	LuxTru	st eID	Smart o	card N	CP+ Ce	rtificate Profile
Attribute	Field	IN''	CE <sup>78</sup>	O/M 79	CO <sub>80</sub>	Value
	commonName	<b>√</b>			S	L T 101 10 W 101 81
		<b>→</b>				LuxTrust Global Qualified CA x <sup>81</sup>
Validity	organizationName	<b>√</b>	False		S	LuxTrust S.A.
validity	NotBefore	<b>✓</b>	i aise		D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + maximum
	Notation	·				120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	<b>✓</b>		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	<b>✓</b>		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					Subject's email address
		<b>√</b>		0	D	
	Title	✓		М	D	"Private Person"
	organizationalUnitNam e 1	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubl		✓	False			
	Algorithm	<b>√</b>				Public Key: Key length: 2048bit up to 4096bit (RSA);
Extension	subjectPublicKey	•		M		public exponent: Fermat-4 (=010001).
S						
Authority Properties						
authorityKe		✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInf		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		✓	False			
	distributionPoint	✓			S	17
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						
Properties	ama	./	Fels:			
subjectAltN	ame Rfc822Name	<b>✓</b>	False	0	_	Subject email address
subjectKeyl		<b>√</b>	False	0	D	Subject email address
Jubjectneyi	keyldentifier	<b>▼</b>	i aise		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
Policy						bit-string bits).
Properties		<b>√</b>	Trus			
keyUsage	dinitalCiameture	<b>✓</b>	True			Truce
	digitalSignature nonRepudiation	<b>✓</b>	<b> </b>		S	True False
	keyEncipherment	<b>∨</b>	1	1	S	True
	dataEncipherment	<b>√</b>	1		S	False
certificatePo		<b>√</b>	False			1 dioc
Joi micater (	Policyldentifier	·	1 0130			1.3.171.1.1.10.3.31
	. Shojiaonanoi		1	1	1	

-

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



	LuxTrust elD Smart card NCP+ Certificate Profile										
Attribute	Field	IN"	CE <sup>78</sup>	O/M 79	CO <sub>80</sub>	Value					
	policyQualifierID	✓			S	Id-gt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2					

### 1.12.38 LuxTrust Signing Server QCP-n-qscd Certificate Profile

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

	LuxTru	st Signir	ng Serv	er QCP	-n-qscd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>1</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		<b>✓</b>	False			
10.0.0			1 4100		S	Version 3 Value = "2"
SerialNumb	per	✓	False			
					FDV	Validated on duplicates.
signatureA		✓	False		_	
	algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
laaau			Falsa		D	Issuing CA Signature.
Issuer	countryName	<b>✓</b>	False		S	LU
	commonName	<b>→</b>	<del>                                     </del>	+	S	LuxTrust Global Qualified CA x 17
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity	Organizationi valie	<b>√</b>	False		0	Edit Hust G.A.
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 30 Months
subject	T	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	<b>~</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as of ID card without indication "épouse", "ép." or similal and the subsequent name(s)
	countryName	<b>✓</b>		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) of "Professional Administrator" (Other titles possible for special purposic 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-qscd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>1</sup> <sub>5</sub>	CO <sup>16</sup>	Value
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitNa me 1	<b>*</b>		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	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPub		<b>√</b>	False			
	algorithm subjectPublicKey	<b>✓</b>	-	M		Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extension s	Subjecti unitericy	Ţ		IVI		равно ехронона. Геннат ч (=010001).
Authority Properties						
authorityKe	yldentifier keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf		✓	False			
	AccessMethod	✓ ✓				Id-ad-2
	accessLocation	<b>∨</b>				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod accessLocation	<b>✓</b>				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu	rtionPoint	<b>✓</b>	False			http://qca.ocsp.idxtrust.id/
	distributionPoint	<b>✓</b>	. 4.00		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
Subject Properties						
subjectAltN	ame Rfc822Name	<b>✓</b>	False	0	D	Certificate Holder's email address
subjectKeyl		· /	False		D	Certificate Florder's erriali address
	keyldentifier	<b>√</b>			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).
Properties			Terra			
keyUsage	digitalSignature	<b>✓</b>	True		S	True
	nonRepudiation				S	True
	keyEncipherment	<b>✓</b>			S	True
	dataEnciphorment	<b>✓</b>	-		S	False
certificateP	dataEncipherment olicies	<b>✓</b>	False		<u>ა</u>	I disc
	Policyldentifier	<b>✓</b>	. 2.00			1.3.171.1.1.10.3.32
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2
	rtificateStat	<b>✓</b>	False	-		U.T.U. 13411Z. 1.Z



	LuxTrust Signing Server QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>1</sup>	CO <sup>16</sup>	Value					
	QcCompliance (0.4.0.1862.1.1)	✓		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		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)	<b>V</b>		M	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)					

### 1.12.39 LuxTrust Signing Server QCP-I-qscd Certificate Profile

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

	LuxTrust Signing Server QCP-I-qscd Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	per	✓	False							
					FDV	Validated on duplicates.				
signatureA		✓	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 <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	<b>✓</b>			D	Certificate generation process date/time.				
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 12, 24, Months				
subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		М	D	Shall contain the full registered name of the subject (legal person).				
	countryName	<b>✓</b>		М	D	the country in which the subject (legal person) is established (ISO3166)				



	LuxTrus	st Sigr	ning Ser	ver QCF	P-I-qscd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Attribute	organisationIdentifier (2.5.4.97)	IN <sup>13</sup> ✓	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	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 1	<b>√</b>		0	D	Company/institution department or other information item
	organizationalUnitNa me 2	✓		0	D	Company/institution department or other information item
subjectPub		<b>√</b>	False			Dublic Keep Keep Landby on the 1999 Lts (DOS)
	algorithm subjectPublicKey	<u>√</u>	-	M		Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extensio ns	Subject ublickey	•		IVI		pasilo experiente i dimat <del>ra</del> (=010001).
Authority Propertie s						
authorityKe		<b>√</b>	False			CHA 4 Hook of the LowTweet Olevel Occupation
and to the	keyldentifier	<b>√</b>	F-1			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf		<u>√</u>	False			Id-ad-2
	AccessMethod accessLocation		-			http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	· ·				http://ca.luxtrust.lu/LTGQCAx .crt Id-ad-1
	accessLocation	<u>√</u>				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		<u>,</u>	False			imp.//qca.ocsp.iuxtrust.iu/
CITEDISTIBL	distributionPoint	<u>√</u>	1 0130		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
			<u> </u>	<u> </u>		http://off.idxtrubt.id/ETGQGA .CII



	LuxTri	ust Sigi	ning Ser	ver QCF	P-I-qscd	l Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Subject Propertie s						
subjectKey		✓	False			
	keyldentifier	<b>√</b>			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	<b>✓</b>			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateF		✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.33
	policyQualifierID	✓			S	Id-gt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	<b>√</b>				0.4.0.194112.1.3
Qualific	edCertificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>~</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	<b>V</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

### 1.12.40 LuxTrust Signing Stick QCP-n-qscd certificate profile

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

	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>82</sup>	CE <sub>83</sub>	O/M <sup>84</sup>	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					

 $<sup>^{82}</sup>$  IN = Included: Attribute / field included within the certificate profile.

<sup>83</sup> CE = Critical Extension.

<sup>&</sup>lt;sup>84</sup> O/M: O = Optional, M = Mandatory.

 $<sup>^{85}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	Lux	Trust S	Signing	Stick Q	CP-n-c	qscd Certificate Profile
Attribute	Field	IN <sup>82</sup>	CE <sup>83</sup>	O/M <sup>84</sup>	CO 85	Value
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>86</sup>
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity	organizationivanie	·	False		- 3	Luxitusi S.A.
	NotBefore	<b>✓</b>	. 4.00		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	<b>~</b>		М	D	<b>PRO and PRIVATE products</b> : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>~</b>		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	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>~</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnit Name 2	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPul	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	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified CA public
authoritylr	l nfo Access	<b>√</b>	False			key
audiorityli	AccessMethod	<b>V</b> ✓	i aise			Id-ad-2
	accessLocation	<b>✓</b>		1		http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	accessedation					
	AccessMethod	✓				Id-ad-1

-

 $<sup>^{86}</sup>$  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.



	Lux			Stick Q	CP-n-c	qscd Certificate Profile
Attribute	Field	IN <sup>82</sup>	CE <sup>83</sup>	O/M <sup>84</sup>	CO 85	Value
cRLDistrib	cRLDistributionPoint		False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properti es						
subjectAlt		✓	False			
	Rfc822Name	<b>✓</b>		0	D	Certificate Holder's email address
subjectKe		✓	False			
	keyldentifier	<b>✓</b>			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	<b>√</b>			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	<b>✓</b>			S S	False
certificate	dataEncipherment	<b>∨</b>	Folso		5	False
Certificate	Policyldentifier	<b>✓</b>	False			1.3.171.1.1.10.3.34
	policyQualifierI D	· ✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>✓</b>				0.4.0.194112.1.2
QualifiedC	ertificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)			М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	<b>✓</b>		М	S	id-etsi-qct-esign

### 1.12.41 LuxTrust Signing Stick NCP+ Certificate Profile

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

	LuxTrust Signing Stick NCP+ Certificate Profile										
Attribute Field IN CE <sup>89</sup> O/M <sup>90</sup> CO <sup>91</sup> Value											
Base Profile											
Version		<b>✓</b>	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								

<sup>&</sup>lt;sup>87</sup> SINCE LTGQCA3

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

<sup>89</sup> CE = Critical Extension.

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

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



	L	.uxTı	rust Sig	rtificate Profile		
Attribute	Field	IN 88	CE <sub>89</sub>	O/M <sup>90</sup>	CO <sup>91</sup>	Value
					FDV	Validated on duplicates.
signature	Algorithm	<b>√</b>	False		TDV	validated on duplicates.
<u> </u>	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature\	/alue	✓	False			
1			F-1		D	Issuing CA Signature.
Issuer	a a untruttama	<b>✓</b>	False		S	
	countryName commonName	<b>∨</b>			S	LU
					_	LuxTrust Global Qualified CA x <sup>92</sup>
M-11-116	organizationName	<b>√</b>	F-1		S	LuxTrust S.A.
Validity	NatDafana	<b>√</b>	False		_	Contificate managetica anacce data/time
	NotBefore NotAfter	<b>✓</b>			D D	Certificate generation process date/time.  Certificate generation process date/time + 3  Months
Subject		<b>√</b>	False			WORLDS
Jubject	serialNumber	· ·	1 0136	М	D	Serial Number as constructed by LRAO
	Serialitatilisei	<u> </u>	-	IVI		<u> </u>
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID care separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) a on ID card
	surname	✓		М	D	PRO and PRIVATE products: Surname(s) as o ID card without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	<b>√</b>		0	D	Subject's email address
						•
	title	<b>✓</b>		М	D	PRIVATE products:  Fixed value: "Private Person"  PRO products:  "Professional Person" (default) of "Professional Administrator"  (Other titles possible for special purposicertificates)
						PRO products only:
	organizationName	<b>✓</b>		М	D	Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	<b>✓</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VA number available, other unique nations company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à:" (Date of birth + 18 years).
	organizationalUnit Name 2	<b>V</b>		0	D	PRO products only: Company/institution department or other information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
Extensio	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).

\_

 $<sup>^{92}</sup>$  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.



	L	.uxTı	rust Sig	LuxTrust Signing Stick NCP+ Certificate Profile										
Attribute	Field	IN 88	CE <sub>89</sub>	O/M <sup>90</sup>	CO <sup>91</sup>	Value								
Authorit														
y Properti														
es authorityK	l Ceyldentifier	<b>√</b>	False											
<u>uuuiioiiiyii</u>	keyldentifier	<b>✓</b>	1 4100			SHA-1 Hash of the LuxTrust Global Qualified CA public key								
authoritylr	nfoAccess	<b>√</b>	False			public Key								
	AccessMethod	<b>√</b>				Id-ad-2								
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt								
	AccessMethod	<b>√</b>				Id-ad-1								
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>93</sup>								
cRLDistrib	outionPoint	<b>√</b>	False			Titip.// qua.uuupinaxiruutiia/								
0.122.01.12	distributionPoint	<b>✓</b>	. 4.00		S									
	fullName	✓			_	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl								
Subject Properti es														
subjectAlt	Name	✓	False											
	Rfc822Name	✓		0	D	Certificate Holder's email address								
subjectKe		✓	False											
	keyldentifier	<b>\</b>			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	1: 1: 10:	<b>√</b>	True			_								
	digitalSignature	<b>✓</b>			S	True								
	nonRepudiation	<b>✓</b>			S S	False								
	keyEncipherment dataEncipherment	<b>✓</b>	-		S	True False								
certificate		<b>V</b>	False		3	I dise								
Jei tilleate	Policyldentifier	· ·	i aise			1.3.171.1.1.10.3.35								
	policyQualifierID	·			S	Id-qt-1 (CPS)								
	qualifier	√	<u> </u>		S	https://repository.luxtrust.lu								
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)								
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2								

## 1.12.42 LuxTrust Signing Server Advanced Automated eSeal Certificate Profile

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

	Advanced eSeal - LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base											
Profile											
Version		<b>√</b>	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	<b>√</b>	False								
					FDV	Validated on duplicates.					
signatureAlg	jorithm	✓	False								

<sup>&</sup>lt;sup>93</sup> SINCE LTGQCA3

LuxTrust proprietary and confidential

# **LuxTrust Global Root CA Certificate Specifications**





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



	Adv	vance	d eSea	I - LCP	Certif	icate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organisationIdentifie r (2.5.4.97)	<b>→</b>		M	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).  When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		M	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitNam e 1	<b>√</b>		0	D	Company/institution department or other information item



	Adv	/ance	d eSea	ıl - LCP	Certif	ficate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationalUnitNam					
	e 2	✓		0	D	Company/institution department or other
						information item
subjectPubl	icKeyInfo	✓	False			
	algorithm	<b>✓</b>				Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	<b>\</b>		М		public exponent: Fermat-4 (=010001).
Extension						
s						
Authority						
Properties						
authorityKey	yldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInfo		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
Subject						
Properties						
subjectKeyl	dentifier	<b>√</b>	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		<b>√</b>	_			
keyUsage	I	<b>→</b>	True		_	  -
	digitalSignature	•			S	True
	nanDanii Pari	<b>√</b>				File
	nonRepudiation	· ✓	1		S	False
	keyEncipherment	· ·			S	False
	dataEncipherment	<i>✓</i>	Felsi		S	False
certificatePo		<i>·</i>	False			
	Policyldentifier					1.3.171.1.1.10.3.36
						1.5.171.1.1.10.5.50
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	1				_	- to select the selection of the selecti
				1	]	1





	Advanced eSeal - LCP Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
	Policyldentifier	✓							
						0.4.0.2042.1.3			

### 1.12.43 LuxTrust Corporate LCP Certificate Profile

LuxTrust Lightweight Certificate Policy Certificate compliant with ETSI EN 319 411-1 LCP certificate policy, with creation of the keys by the LuxTrust, 4096 -bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.4.1>.

	LuxTrust Corporate LCP Certificate Profile – Corporate CA								
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value			
Base Profile									
Version	•	<b>√</b>	False						
					S	Version 3 Value = "2"			
SerialNumber	•	<b>√</b>	False						
					FDV	Sequential CSN			
signatureAlgo	rithm	<b>√</b>	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with RSA Encryption.			
signatureValu	e	<b>√</b>	False						
					D	Issuing CA Signature.			
Issuer	•	<b>√</b>	False		S				
	countryName	<b>√</b>			S	LU			
	commonName	<b>√</b>			S	LuxTrust Corporate CA x			
	organizationName	<b>√</b>			S	LuxTrust S.A.			
Validity	•	<b>√</b>	False						
	NotBefore	<b>√</b>			D	Certificate generation process date/time.			
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months			
Subject	•	<b>√</b>	False						
	serialNumber	<b>✓</b>		М	D	Serial Number as constructed by LRAO			



	LuxTru	st Corpor	ate LCP (	Certificate I	Profile – C	orporate CA
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s) separated by a "Space" character.
	givenName	<b>√</b>		М	D	Given name(s) as on ID document
	Surname	<b>√</b>		М	D	Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	<b>√</b>		М	D	Nationality of holder (ISO3166)
	Title	<b>√</b>		М	D	Private Person
subjectPublicK	eyInfo	<b>√</b>	False			
	Algorithm	<b>√</b>				Public Key: Key length: 2048 bit up to 4096 (RSA); public exponent: Fermat-4
	subjectPublicKey	<b>√</b>		М		(=010001).
Extensions						
Authority Properties						
authorityKeylde	entifier	<b>√</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Corporate</b> CA public key
authorityInfoAc	cess	<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTCCAx2.crt
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	<b>~</b>				http://cca.ocsp.luxtrust.lu/23
cRLDistribution	Point	<b>√</b>	False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTCCAx <sup>22</sup> .crl
Subject Properties						



	LuxTr	ust Corpor	ate LCP (	Certificate F	Profile – Co	orporate CA
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
subjectAltName	е	<b>V</b>	False			
	Rfc822Name	<b>~</b>		0	D	N/A
subjectKeylder	ntifier	<b>~</b>	False			
	keyldentifier	<b>✓</b>			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	<b>√</b>			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePolici	ies	<b>~</b>	False			
	Policyldentifier	<b>~</b>				1.3.171.1.1.10.4.1
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	Policyldentifier	<b>~</b>				0.4.0.2042.1.3

# 1.13 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.



	LuxTru	ıst Tim	estampi	ng Cert	ificate F	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile		<b>√</b>	False			
Version		<b>V</b>	False		S	Version 3 Value = "2"
SerialNumbe	l er	<b>√</b>	False		3	Version 3 value – 2
			. 4.00		FDV	Validated on duplicates.
signatureAlg		✓	False			·
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
signatureVal	110	<b>√</b>	False			with RSA Encryption.
Signatureval			i aise		D	Issuing CA Signature.
issuer	I	✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Timestamping CA x <sup>17</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False			Contificate generation process data/time
	NotBefore	<b>✓</b>			D D	Certificate generation process date/time.  Certificate generation process date/time +
						60 Months
subject		✓	False			
	commonName	✓		М	D	tts.luxtrust.lu
	IocalityName	✓		М	D	Capellen
	organizationName	✓		М	D	LuxTrust S.A.
	organizationalUnitName 1	✓		М	D	PKI Entity
	countryName	✓		0	D	LU
subjectPubli	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust
						Timestamping CA public key
authorityInfo	AccessMethod	<b>√</b>	False			Id-ad-2
	accessLocation	· /				http://ca.luxtrust.lu/LTGTSACAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGTSACAx17.crl
Subject						
Properties subjectAltNa	ame	<b>✓</b>	False			
- Judjeot Aitiva	Rfc822Name	<b>→</b>	1 4130	0	D	info@luxtrust.lu
subjectKeylo	lentifier	✓	False			
	keyldentifier	<b>√</b>			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	digitalCian at	<b>√</b>	True			True
	digitalSignature nonRepudiation	<b>→</b>	1		S	True False
	keyEncipherment	<b>▼</b>			S	False
	dataEncipherment	· /			S	False
Extended Ke	y Usage	✓	False			
	TimeStamping	✓			S	Set
	(1.3.6.1.5.5.7.3.8)					



	LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Private Key I	Usage Period	✓	False							
	Usage period (2.5.29.16)	<b>✓</b>		М	D	Certificate generation process date/time + 12 Months				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.8.1				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>√</b>				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				

#### 1.13.1 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.

			cate Poil	Cy for Lu	IXTrust	Qualified Timestamping
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	r	✓	False			
					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
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
-	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		✓	False			
	organisationIdentifier (2.5.4.97)	✓		М	D	VATLU-20976985
	commonName	✓		М	D	LuxTrust Qualified Timestamping
	organizationName	✓		М	D	LuxTrust S.A.
	countryName	✓		М	D	LU
subjectPubli	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA
authorityInfo	Access	✓	False			
-	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt



	Normalized (			cy for Lu		Qualified Timestamping
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	<u>info@luxtrust.lu</u>
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>✓</b>			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		<b>✓</b>	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
Extended Ke		✓	True			
	TimeStamping (1.3.6.1.5.5.7.3.8)	✓			S	Set
Private Key I	Usage Period	✓	False			
	Usage period (2.5.29.16)	✓		М	D	Certificate generation process date/time + 12 Months
certificatePo	licies	✓	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.18
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

### 1.13.2 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.

	Qı	alified Certi	ficate P	olicy for	for LuxT	rust Qualified Timestamping
Attribute	Field	IN1 3	CE1 4	O/M1 5	CO1 6	Value
Base Profile						
Version		<b>*</b>	Fals e			
					S	Version 3 Value = "2"
SerialNuml	ber	<b>√</b>	Fals e			
					FDV	Validated on duplicates.
signatureA	lgorithm	<b>√</b>	Fals e			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	Fals			
-			е			
					D	Issuing CA Signature.



	Qualifie	d Certi	ficate P	olicy for	for Lux	Trust Qualified Timestamping
Attribute	Field	IN1	CE1	O/M1	CO1	Value
		3	4	5	6	
issuer		✓	Fals		S	
	countryName	<b>✓</b>	е		S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	Fals			
	T		е			
	NotBefore NotAfter	<b>✓</b>			D D	Certificate generation process date/time.
subject	NotAiter	<b>∨</b>	Fals		U	Certificate generation process date/time + 60 Months
Subject		*	e			
	organisationIdentifi					
	er	<b>✓</b>		М	D	VATLU-20976985
	(0.5.4.07)			141		
	(2.5.4.97)					
	commonName	✓		М	D	LuxTrust Qualified Timestamping
	organizationName	<b>✓</b>		М	D	LuxTrust S.A.
	countryName	✓		М	D	LU
subjectPub	licKeyInfo	✓	Fals			
		<b>✓</b>	е			Public Keyn Key length virg to 0070 Lt (DOA)
	algorithm subjectPublicKey	<b>✓</b>	-	M	1	Public Key: Key length: up to 3072 bit (RSA) public exponent: Fermat-4 (=010001).
Extension	SubjectrubilCNey	,		IVI		ραωπο σχροποτικ. τ σπιαι-4 (=010001).
S						
Authority						
Propertie						
S	11 400					
authorityKe	eyidentifier	✓	Fals e			
	keyldentifier	<b>✓</b>	E			
						SHA-1 hash of the LuxTrust Global Qualified CA
authorityIn	foAccess	✓	Fals			
	T		е			
	AccessMethod accessLocation	<b>√</b>				Id-ad-2
	AccessMethod	<b>∨</b>				http://ca.luxtrust.lu/LTGQCAx.crt Id-ad-1
	accessLocation	<b>∀</b>				http://qca.ocsp.luxtrust.lu/
						mp// qoarooopma/maoma/
cRLDistrib	utionPoint	✓	Fals			
			е		_	
	distributionPoint fullName	<b>√</b>			S	http://ord.lev.tm.ot.le//.TCOCA.cod
	Tulliname	<b>,</b>				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						
Propertie						
s						
subjectAltN	lame	✓	Fals			
	Rfc822Name	<b>✓</b>	е	0	D	info@luxtrust.lu
subjectKey		<b>V</b>	Fals		<u> </u>	IIIIO SIUALI USLIU
,,			e			
	keyldentifier	<b>✓</b>			Fixe	The Key Identifier comprises a four-bit field with a 0100
					d	value, followed by the least significant 60 bits of the SHA-
						1 hash of the value or subjectPublicKey bit string (tag, not
Policy						including the length and number of unused bit-string bits).
Propertie						
S						
keyUsage		✓	True			
	digitalSignature	<b>√</b>			S	True
	nonRepudiation	<b>✓</b>	ļ	1	S	False
	keyEncipherment	✓ ✓	<u> </u>	1	S	False
Extended K	dataEncipherment	<b>✓</b>	True		S	False
Exteriueu M	TimeStamping	<b>∨</b>	riue		S	Set
	(1.3.6.1.5.5.7.3.8)				~	
		<b>√</b>	Fals			
Private Key	Usage Period	•	i ais			



	Qualifie	ed Certi	ficate P	olicy for	for Lux1	rust Qualified Timestamping
Attribute	Field	IN1 3	CE1 4	O/M1 5	CO1 6	Value
	Usage period (2.5.29.16)	<b>√</b>		M	D	Certificate generation process date/time + 12 Months
certificateP	olicies	<b>V</b>	Fals e			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.19
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	Policyldentifier	✓				0.4.0.194112.1.1
certificateP	olicies	✓				
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/GTC_F_v2 _4.pdf

#### 1.13.3 TimeStamp Request and Response Format

#### 1.13.3.1 TimeStamp Request Format

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

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

<sup>\*</sup>no extension is required to be supported

#### 1.13.3.2 TimeStamp Response Format

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

LuxTrust Time Stamp Response						
Field	Value / comment					
Generation Time	The time at which the time-stamp token has been created by the TSA. It is expressed as UTC time (Coordinated Universal Time).					
Document Hash	Hash of the document on which the TimeStamp response has been computed					
Hash OID	(SHA-256/SHA-512)					



LuxTrust Time Stamp Response					
Field	Value / comment				
	Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.				
Serial Number	Serial Number of the current TSU certificate (unique, up to 160 bits)				
Policy OID	1.3.171.1.10.3.18.1 / Qualified timestamp token 1.3.171.1.10.8.1.1 / Non-qualified timestamp token				
	The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returnedtoken will include a policy identifier that is not defined by LuxTrust.				
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.				
Accuracy	1 second				
TSA Certificate Information	Current TSU Certificate				
Request Extensions	Value *				
None	None				

<sup>\*</sup>no extension is required to be generated, no extension shall be critical

#### 1.14 Certificate extensions

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

### 1.15 Algorithm object identifiers

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

#### 1.16 Name forms

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

### 1.17 Name constraints

Name constraints are supported as per RFC 5280.

### 1.18 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

### 1.19 Usage of Policy Constraints extension

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

VERSION 1.27



#### 1.20 Policy qualifiers syntax and semantics

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

### 1.21 Processing semantics for the critical Certificate Policies

Not applicable.

#### 1.22 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	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" qualified="" subordinate="" time=""></creation></creation></pre>							
	<creation (8="" +="" 30="" 8,5="" and="" for="" hours="" minutes)="" p="" subordinate<="" time=""></creation>							
	SSL CAs>							
	<pre><creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></pre>							
revokedCertificates								
userCertificate	<pre><certificate number="" serial=""></certificate></pre>							
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>							

### 1.22.1 Version number(s)

See section 3.4.

The CA will support X.509 version 2 CRLs, retrievable by online at <a href="http://crl.luxtrust.lu">http://crl.luxtrust.lu</a>.

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

### 1.22.2 CRL entry extensions

See section 3.4.

### 1.23 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.

#### 1.23.1 Version number(s)

See section 3.5.

# **LuxTrust Global Root CA Certificate Specifications**





#### 1.23.2 OCSP extensions

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

LuxTrust OCSP Certificate Profile						
Attribute	Field	IN18	CE19	O/M20	CO21	Value
Base Profile						
Version			False			
					S	Version 3 Value = "2"
SerialNumbe	er		False			
					FDV	Validated on duplicates.
signatureAlg			False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	lue T		False			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
			E-I		D	Issuing LTGRCA Signature
issuer	Lacuntu Alama		False		S	LU
	countryName commonName				S	LuxTrust Global Root x
	organizationName				S	LuxTrust S.A.
Validity	organizationivalile		False		3	LUATTUSI S.A.
validity	NotBefore		i aise		D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time +
	Notate				١٦	maximum 12 Months
subject	L		False			THEALTH I'L WORKE
22.2,300	countryName		1 4100	M	D	LU
	organizationName			M	D	LuxTrust S.A.
	organizationalUnitName 1			0	D	Pki entity
	commonName			M	D	LuxTrust S.A. OCSP Server 2
subjectPubli			False			Zaxii aat ah ii aasi aa ii aa
	algorithm					Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey			М		public exponent: Fermat-4 (=010001).
Extensions	,					
Authority						
Properties						
authorityKey	/Identifier		False			
	keyldentifier					SHA-1 Hash of the LuxTrust LTGR x CA public key
id-ocsp-noch	heck		False			
					S	NULL
Subject Properties						
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			T			
keyUsage	digitalCianature		True			Truce
	digitalSignature				S	True
	nonRepudiation				S	False
	keyEncipherment				S	False
	dataEncipherment				S	False
certificatePolicies			False			
- <del></del>	Policyldentifier					1.3.171.1.1.1.1.0.1.0
	policyQualifierID				S	Id-qt-1 (CPS)
	qualifier				S	https://repository.luxtrust.lu
	policyQualifierID				S	Id-qt-2 (User Notice)
	noticeNumbers					

# **LuxTrust Global Root CA Certificate Specifications**





LuxTrust OCSP Certificate Profile							
Attribute	Field	IN18	CE19	O/M20	CO21	Value	
	DisplayText					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 Key Usage			False				
-	OCSPSigning				S	True	