

Version number: 1.21

Publication Date: 24/03/2015 Effective Date: 10/04/2015



VFRSION 12

# **Document Information**

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

# **Version History**

Version	Who	Date	Reason of modification	
1.0	MSC	29/08/2011	Initial Version DRAFT	
1.01	MSC	27/10/2011	Added CRL validity period, revision	
1.02	MSC	24/11/2011	Modified – Document OIDs for CAs	
1.03	MSC	09/02/2012	Modified – Added LCP for integration purposes.	
1.04	MSC	01/03/2012	Modified:      Added LCP for integration purposes for CSS      Table for OIDs      Modification of the CRL issuance algorithm (SHA256 to SHA1)	
1.05	MSC	19/03/2012	Modifications following review by Chris Quaresimin and Laurent Breuskin:  Removal of + Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime for non-SSL products  Display text for CSS integration product  Correct CRL and AIA for CSS integration product  SSL Object certificate profile	
1.06	MSC	26/03/2012	Modifications for CSS certificates, signature will be performed using SHA1WithRsa. Changes performed in CSS certificate profile for prod and integration, page 43 and 51.	
1.07	MSC	14/06/2012	Added: TimeStamping CA and TimeStamping certificate profile	
1.08	MSC	29/06/2012	Added: Private key usage Period in TSP	
1.09	LBR	01/08/2012	Added: Certificate Profiles under LuxTrust Global Qualified CA     SC LORA & LRS Certificate     Modified:     Table for OIDs & LuxTrust CA Hierarchy	
1.09.1	LBR	02/08/2012	Update of OID Page 22	
1.09.2	MSC	07/08/2012	Added: Certificate profile for Extended Validation Certificates :  • EVCP – ETSI TS 102 042  • EVCP+ - ETSI TS 102 042  Added: Certificate profile for Secure Online File Exchange (SOFiE)	
1.10	YNU	23/08/2012	Review for validation of CP	
1.10	CSPBoard	24/08/2012	Validation	
1.11	CSPBoard	20/09/2012	Typo update	
1.12	YNU	21/12/2012	Added CP SSL/TLS Certificate for Client Authentication	
	TKO		Added CP non SSCD NCP+ Certificates supporting Advanced	
			Electronic Signatures for Mass Signature Services	
			Various syntactical and format corrections	





VFRSION 1 21

1.13	CSP	23/04/2013	insertion of ILNAS logo including accreditation reference and technical			
	Board		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			
			- Туро			
			Add CP Seal Signature Services			
1.17	YNU	30/06/2014	Add certificate profile for eID			
			CP eID QCP+			
			CP eID NCP+			
			Update CP Seal Signature Services OID			
1.18	YNU	15/10/2014	Update AIA in SSL CA			
1.19	YNU	11/11/2014	Update AIA in CP under the SSL CA since SSL CA 2			
1.20	YNU	19/12/2014	Add Integration CP for eID			
			Update eID CP with pseudonym			
			Update Global Root CA CP with OID attribute			
			Update SSL CA profile since SSL CA 3			
			Update lifetime of SSL Server/Object/SSL Client auth to 24 months			
1.21	CSP	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			







# **Table of content**

DOCUME	NT INFORMATION	2
VERSION	I HISTORY	2
TABLE O	F CONTENT	4
INTELLE	CTUAL PROPERTY RIGHTS	6
REFEREI	NCES	7
1	INTRODUCTION	8
1.1	THE LUXTRUST PROJECT	8
1.2	GOAL OF THE LUXTRUST PKI	
1.3	LuxTrust PKI Hierarchy	
2	LUXTRUST CERTIFICATION AUTHORITIES	9
2.1	TWO-LEVEL CA HIERARCHY	9
3	CERTIFICATE AND CRL PROFILES	12
3.1	CERTIFICATE TYPES	12
3.2	LuxTrust Certification Authorities – Certificates profiles	29
3.2.1	LuxTrust Global Root CA	29
3.2.2	LuxTrust Global Qualified CA	30
3.2.3	LuxTrust Privacy+ CA	31
3.2.4	LuxTrust SSL CA	33
3.2.5	LuxTrust TEST CA	34
3.2.6	LuxTrust Internal CA	35
3.2.7	LuxTrust TSA (Timestamping) CA	36
3.2.8	LuxTrust e-Government CA	38
3.2.9	Certificate extensions	39
3.2.10	Algorithm object identifiers	39
3.2.11	Name forms	39
3.2.12	Name constraints	39
3.2.13	Certificate policy object identifier	39
3.2.14	Usage of Policy Constraints extension	39
3.2.15	Policy qualifiers syntax and semantics	39
3.3	LUXTRUST END-ENTITY – CERTIFICATES PROFILES	39
3.3.1	Certificate profiles	39
3.3.2	Version number(s)	40
3.3.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	40
3.3.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	43
3.3.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	46
3.3.6	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	
3.3.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	
3.3.8	LuxTrust NCP+ Certificates supporting Mass Signature Services	55
3.3.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	
3.3.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	
3.3.11	LuxTrust Signing Server Account LCP Certificates supporting Signature, Authentication & Encryption for	
	purposes	62



#### VFRSION 1 21

3.3.12	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	64
3.3.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	; <i>67</i>
3.3.14	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures	69
3.3.15	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures	72
3.3.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	<i>75</i>
3.3.17	LuxTrust eID SSCD LCP+ Certificates supporting Qualified Signatures	77
3.3.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	80
3.3.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	83
3.3.20	LuxTrust SSL/TLS Standard Server Certificates - LCP certificates supporting Signature,	Authentication &
	Encryption	85
3.3.21	SSL/TLS Extended Validation Server Certificates - EVCP certificates supporting Signature,	Authentication &
	Encryption	90
3.3.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature,	Authentication &
	Encryption	96
3.3.23	LuxTrust Object (or Code) Signing Certificates	103
3.3.24	LuxTrust SSL/TLS Certificate for Client Authentication	106
3.3.25	Timestamping Certificate Profile	109
3.3.26	Certificate extensions	111
3.3.27	Algorithm object identifiers	111
3.3.28	Name forms	111
3.3.29	Name constraints	111
3.3.30	Certificate policy object identifier	111
3.3.31	Usage of Policy Constraints extension	111
<i>3.3.32</i>	Policy qualifiers syntax and semantics	111
3.3.33	Processing semantics for the critical Certificate Policies	111
3.4	CRL PROFILE	111
3.4.1	Version number(s)	112
3.4.2	CRL entry extensions	112
3.5	OCSP PROFILE	112
3.5.1	Version number(s)	112
352	OCSP extensions	112





VFRSION 1 21

## **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.
- [2] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
- [3] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- [4] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- [5] ICAO (International Civil Aviation Organization) Machine Readable Travel Documents Technical Report PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, October 01, 2004
- [6] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- [7] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [8] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [9] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [10] Règlement Grand-Ducal du 1<sup>er</sup> juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [11] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [12] LuxTrust Time Stamping Policy. Document OID 1.3.171.1.3.1.0, latest version in force.
- [13] Guidelines for the Issuance And Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.
- [14] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force.
- [15] eID Certificate Life Cycle Procedure latest version in force
- [16] RNCID: National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16
- [17] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [18] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [19] 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





### 1 INTRODUCTION

#### 1.1 The LuxTrust project

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

Established in November 2005 through a partnership between the Luxembourg government and the major private financial actors in Luxembourg, LUXTRUST S.A. was created to become a provider of certification services as defined in the law of the Grand-Duchy of Luxembourg modified on 14/08/2000 [7] itself derived from the European Directive on electronic signatures (1999/93/EC; 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.

#### 1.2 Goal of the LuxTrust PKI

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

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

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

#### 1.3 LuxTrust PKI Hierarchy

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







VFRSION 1 21

## **2 LuxTrust Certification Authorities**

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

#### 2.1 Two-level CA hierarchy

The top level is the *LuxTrust Global Root CA*, the highest level of authority managed by LuxTrust. The LuxTrust PKI is formed using additional subordinates 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. Currently, the following CAs are foreseen:
  - LuxTrust Global Qualified CA
  - LuxTrust Privacy+ CA
  - LuxTrust SSL CA
  - LuxTrust TEST CA
  - LuxTrust Internal CA
  - o LuxTrust Time Stamping Authority
  - LuxTrust eGovernment 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.



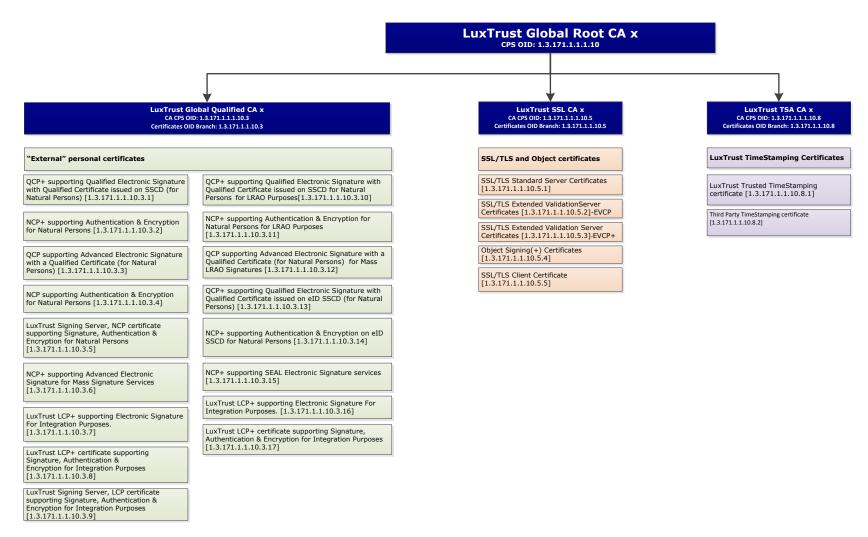


Figure 1 - LuxTrust running CA Hierarchy

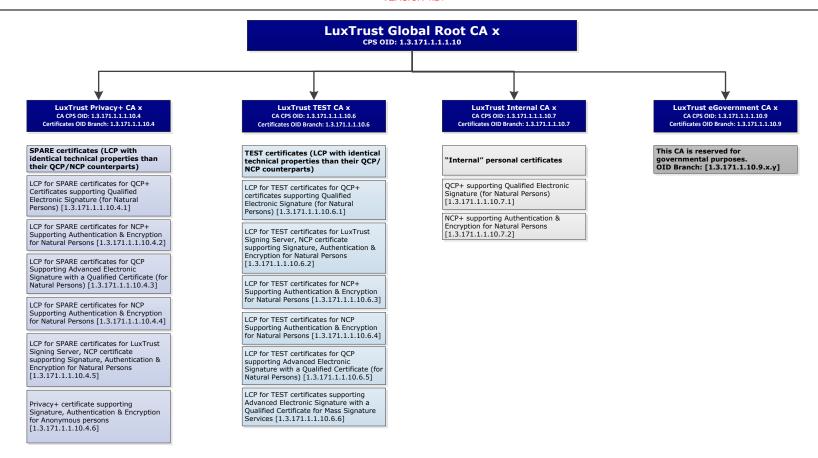


Figure 2 - LuxTrust foreseen CA Hierarchy

VFRSION 12

## **3 CERTIFICATE AND CRL PROFILES**

#### 3.1 Certificate types

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

CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
LuxTrust Qualified Cer	rtification Authority			
QCP+ supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.1	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature.  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.	SSCD QCP+ Certificates supporting Qualified Signatures
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.2	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.  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

<sup>&</sup>lt;sup>1</sup> Corresponding CP will be defined later when field is empty.



Page 12 de 112





CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.3	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate.	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures
NCP supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.4	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.5	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a <b>non</b> SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption
NCP+ supporting Advanced Electronic Mass Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	1.3.171.1.1.1.10.2.3 .x(version) .y(sub-version)	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	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures







CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.8	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA  QCP+ supporting Qualified Electronic Signature with Qualified Certificate issued on SSCD for Natural Persons for LRAO Purposes issued by LuxTrust	1.3.171.1.1.10.3.10	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)  1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a <b>non</b> 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.  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 Signing Server Account LCP Certificates supporting Signature, Authentication & Encryption for integration purposes  LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes
Global Qualified CA  NCP+ supporting  Authentication &  Encryption for Natural  Persons for LRAO  Purposes  issued by LuxTrust  Global Qualified CA	1.3.171.1.1.10.3.11	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for LRAO Purposes.	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes







	CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
	QCP supporting	1.3.171.1.1.10.3.12	1.3.171.1.1.10.2.3	ETSI TS 101 456 QCP compliant	LuxTrust non
	Advanced Electronic		.x(version)	Qualified Certificate not issued on	SSCD Mass
	Signature with a		.y(sub-version)	SSCD Hardware token, with creation	LRAO QCP
	Qualified Certificate for		.y(oub voicion)	of the keys by the CSP, 2048-bit key	Certificates
	Mass LRAO Signature			size and three (3) years validity, and	supporting
	· ·			with a key usage limited to the support	Advanced
	issued by LuxTrust			of advanced electronic signature with	Electronic
	Global Qualified CA			a qualified certificate for Mass LRAO	Signatures
ı				Signatures.	LouiTroot alD
	QCP+ supporting	1.3.171.1.1.10.3.13	1.3.171.1.1.10.2.3	ETSI TS 101 456 QCP+ compliant	LuxTrust elD
	Qualified Electronic		.x(version)	Qualified Certificate on SSCD	SSCD QCP+
	Signature (for Natural		.y(sub-version)	Hardware token (e.g., Luxemburguish	Certificates
	Persons)		,	elD Smart Card), with creation of the	supporting
	issued by LuxTrust			keys by the CSP, 2048 bit key size	Qualified
	Global Qualified CA			and sixty-one (61) months validity, and	Signatures
				with a key usage limited to the support	
ı				of qualified electronic signature.	
	NCP+ supporting	1.3.171.1.1.10.3.14	1.3.171.1.1.10.2.3	ETSI TS 102 042 NCP+ compliant	LuxTrust eID
	Authentication &		.x(version)	Normalised Certificate on SSCD	SSCD NCP+
	Encryption for Natural		.y(sub-version)	Hardware token (e.g., Luxemburguish	Certificates
	Persons			eID Smart Card), with creation of the	supporting
	issued by LuxTrust			keys by the CSP, 2048-bit key size	Authentication
	Global Qualified CA			and sixty-one (61) months validity, and	& Encryption
				with a key usage limited to	
				authentication purpose (to the	
				exclusion of electronic signature) and	
				key & data encryption.	
	NCP+ Advanced	1.3.171.1.1.10.3.15	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant	LuxTrust
	Electronic Seal		.x(version)	Normalised Certificate on Secure User	NCP+
	Signature Services		.y(sub-version)	Device (HSM), with creation of the	Certificates
	issued by LuxTrust			keys by the CSP, 2048-bit key size	supporting
	Global Qualified CA			and three (3) years validity, and with a	SEAL
				key usage limited to the support of	Signature
				advanced electronic Seal Signature	Services
1				Services.	
	LCP for	1.3.171.1.1.10.3.16	1.3.171.1.1.1.10.2.3	ETSI TS 102 042 LCP compliant	LuxTrust eID
	INTEGRATION			certificate, on SSCD, Hardware token	SSCD LCP+
	certificates LCP		.x(version)	(e.g., Luxemburguish elD Smart Card),	Certificates
	compliant certificates		.y(sub-version)	with creation of the keys by the CSP,	supporting
	supporting integration			2048 bit key size and one (1) year	Qualified
	Electronic Signature			validity, and with a key usage limited	Signatures
'	_			to the support of electronic signature	
	issued by LuxTrust			for INTEGRATION purposes of QCP+	
	Global Qualified CA			signature certificates.	







CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	1.3.171.1.1.10.2.3 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburguish 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
LuxTrust Privacy+ Certifi	cation Authority			
LCP for SPARE certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Privacy+ CA	1.3.171.1.1.10.4.1	1.3.171.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for SPARE purposes of QCP+ signature certificates.	
LCP for SPARE certificates for NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Privacy+ CA	1.3.171.1.1.10.4.2	1.3.171.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for SPARE purposes of NCP+ authentication and encryption certificates.	
LCP for SPARE certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) issued by LuxTrust Privacy+ CA	1.3.171.1.1.10.4.3	1.3.171.1.1.10.2.4 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for SPARE purposes of QCP signature certificates.	





LCP for SPARE certificates for NCP supporting Authentication & Encryption for Natural Persons  LCP for SPARE certificates for NCP certificates for LuxTrust Signing Server, NCP certificate for Natural Persons  LSSued by LuxTrust Privacy+ CA  LCP for SPARE certificates for LuxTrust Signing Server, NCP certificates assert by LuxTrust Privacy+ CA  LCP for Natural Persons  LCP for SPARE certificates for LuxTrust Signing Server, NCP certificates Server, NCP certificates assert by LuxTrust Signing Server, NCP certificates Server, NCP certificate Server, NCP certificates S	CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust Privacy+ CA  1.3.171.1.1.10.4.6  Encryption for Anonymous persons issued by LuxTrust Privacy+ CA  2.x(version)  2.x(version)  2.x(version)  2.x(version)  2.x(version)  2.x(version)  2.x(version)  2.x(version)  2.x(version)  3.x(version)  3.x(version)  4.x(version)  2.x(version)  2.x(version)  3.x(version)  3.x(version)  4.x(version)  3.x(version)  4.x(version)  3.x(version)  4.x(version)  5.x(version)  6.x(version)  6.x(version)  6.x(version)  6.x(version)  6.x(version)  6.x(version)  6.x(version)  7.x(version)  8.x(version)  8.x(version)  9.x(version)  9.x(version)  1.3.171.1.1.1.10.4.6  1.3.171.1.1.1.10.2.4  1.3.171.1.1.1.10.2.4  1.3.171.1.1.1.10.2.4  1.3.171.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	certificates for NCP supporting Authentication & Encryption for Natural Persons issued by LuxTrust	1.3.171.1.1.10.4.4	.x(version)	certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for SPARE purposes of NCP authentication and encryption	
supporting Signature, Authentication & Encryption for Anonymous persons issued by LuxTrust Privacy+ CA   Lix(version)  Lix(versi	certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust	1.3.171.1.1.10.4.5	.x(version)	Certificate issued on a <b>non</b> SSCD centralised hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for SPARE purposes of NCP authentication, encryption and	
	supporting Signature, Authentication & Encryption for Anonymous persons issued by LuxTrust	1.3.171.1.1.10.4.6	.x(version)	Certificate issued on a <b>non</b> SSCD hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for authentication,	



CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
SSL/TLS(+) Standard Server Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	1.3.171.1.1.10.2.5 .x(version) .y(sub-version)	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	1.3.171.1.1.10.2.5 .x(version) .y(sub-version)	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	1.3.171.1.1.10.2.5 .x(version) .y(sub-version)	ETSI TS 102 042 <b>EVCP+</b> 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	1.3.171.1.1.10.2.5 .x(version) .y(sub-version)	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





CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
LuxTrust SSL/TLS Certificate for Client Authentication issued by LuxTrust SSL CA	1.3.171.1.1.10.5.5	1.3.171.1.1.10.2.5 .x(version) .y(sub-version)	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 TEST Certificati	ion Authority			
LCP for TEST certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Test CA	1.3.171.1.1.10.6.1	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for TEST purposes of QCP+ signature certificates.	
LCP for TEST certificates for NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Test CA	1.3.171.1.1.10.6.2	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for TEST purposes of NCP+ authentication and encryption certificates.	
LCP for TEST certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) issued by LuxTrust Test CA	1.3.171.1.1.10.6.3	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for TEST purposes of QCP signature certificates.	







CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
LCP for TEST certificates for NCP supporting Authentication & Encryption for Natural Persons issued by LuxTrust Test CA	1.3.171.1.1.10.6.4	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for TEST purposes of NCP authentication and encryption certificates.	
LCP for TEST certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust Test CA	1.3.171.1.1.10.6.5	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a <b>non</b> SSCD centralised hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity or validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for TEST purposes of NCP authentication, encryption and signature certificates.	
LCP for TEST certificates supporting Advanced Electronic Signature with a Qualified Certificate for Mass Signature Services issued by LuxTrust Test CA	1.3.171.1.1.10.6.6	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for Mass Signature Services.	
LuxTrust Internal Certific  QCP+ supporting  Qualified Electronic  Signature (for Natural  Persons)  issued by LuxTrust  Internal CA	1.3.171.1.1.10.7.1	1.3.171.1.1.10.2.6 .x(version) .y(sub-version)		





CP identification	CP OID	Document OID	Short Description	Ref. <sup>1</sup>
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Internal CA	1.3.171.1.1.10.7.2	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)		
	ping) Certification Authority			
LuxTrust Trusted TimeStamping certificate issued by LuxTrust TSA CA	1.3.171.1.1.10.8.1	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)	LuxTrust certificate compliant with ETSI TS 102 023. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority.  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
Third Party TimeStamping certificate issued by LuxTrust TSA CA	1.3.171.1.1.10.8.2	1.3.171.1.1.1.10.2.6 .x(version) .y(sub-version)		

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

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

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

In addition to the above described certifications services, the LuxTrust CSP activities include the LuxTrust Time Stamping Services (TSS). These services consist of the management of the infrastructure, and the provisioning of Time Stamp Tokens according to the LuxTrust Time Stamping Policy [12].

These services are provided by LuxTrust S.A. acting as LuxTrust Trusted Time Stamping Services Provider (TTSSP) to the Subscribers and are an integral part of the LuxTrust PKI. Hereafter the term CSP includes the activities and provision of trusted time stamping services as expressed in the European Directive on electronic signatures (cf. [1]). LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy [12].

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





VFRSION 1 21

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



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

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





Document category	Document		Sub-document - description	LuxTrust Product	Version	Sub- version	Complete OID	ETSI OID
		0	Master document	N/A	х	у	1.3.171.1.1.10.3.0.x.y	N/A
		1	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1.1.10.3.1	0.4.0.1456.1.1
		2	NCP+ supporting Authentication & Encryption for Natural Persons	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1.1.10.3.2	0.4.0.2042.1.2
		3	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick PRI/PRO Signature Certificate	-	-	1.3.171.1.1.10.3.3	0.4.0.1456.1.2
		4	NCP Authentication & Encryption	Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1.1.10.3.4	0.4.0.2042.1.1
	3	5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1.1.10.3.5	0.4.0.2042.1.1
	LuxTrust Global Qualified CA Certificates issued to Natural Persons	6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-	-	1.3.171.1.1.10.3.6	0.4.0.2042.1.1
		7	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration SmartCard Signature Certificate	-	-	1.3.171.1.1.10.3.7	0.4.0.2042.1.3
		8	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration SmartCard  Authentication  Certificate	-	-	1.3.171.1.1.10.3.8	0.4.0.2042.1.3
		9	LuxTrust LCP Certificates supporting Signature, Authentication & Encryption for integration purposes	Integration Signing Server Certificate	-	-	1.3.171.1.1.10.3.9	0.4.0.2042.1.3
		10	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons) for Natural Persons for LRAO Purposes	SmartCard LORA Signature Certificate	-	-	1.3.171.1.1.10.3.10	0.4.0.1456.1.1



Document category	Document		Sub-document - description	LuxTrust Product	Version	Sub- version	Complete OID	ETSI OID
		11	NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes	SmartCard LORA Authentication Certificate	-	-	1.3.171.1.1.10.3.11	0.4.0.2042.1.2
			QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) for Mass LRAO Signatures [1.3.171.1.1.10.3.12]	Mass LRAO Signature Certificate	-	-	1.3.171.1.1.10.3.12	0.4.0.1456.1.2
		13	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	eID SmartCard Signature Certificate	-	-	1.3.171.1.1.10.3.13	0.4.0.1456.1.1
		14	NCP+ supporting Authentication & Encryption for Natural Persons	eID SmartCard Authentication Certificate	-	-	1.3.171.1.1.10.3.14	0.4.0.2042.1.2
		15	NCP+ supporting Advanced Electronic Seal Signature Services	Seal Signature Services	-	-	1.3.171.1.1.10.3.15	0.4.0.1456.1.2
		16	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration eID SmartCard Signature Certificate	-	-	1.3.171.1.1.10.3.16	0.4.0.2042.1.3
		17	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration eID SmartCard Authentication Certificate	-	-	1.3.171.1.1.10.3.17	0.4.0.2042.1.3
		0	Master document		x	у	1.3.171.1.1.10.4.0.x.y	N/A
	4 LuxTrust Privacy+ CA 1		LCP for SPARE certificates for QCP+ Certificates supporting Qualified Electronic Signature (for Natural Persons)	SmartCard SPARE Signature certificate	-	-	1.3.171.1.1.10.4.1	0.4.0.2042.1.3
		2	LCP for SPARE certificates for NCP+ Supporting Authentication & Encryption for Natural Persons	SmartCard SPARE Authentication Certificate	-	-	1.3.171.1.1.10.4.2	0.4.0.2042.1.3





Document category	Document		Sub-document - description	LuxTrust Product	Version	Sub- version	Complete OID	ETSI OID
		3	LCP for SPARE certificates for QCP Supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick SPARE Signature Certificate	-	-	1.3.171.1.1.10.4.3	0.4.0.2042.1.3
		4	LCP for SPARE certificates for NCP Supporting Authentication & Encryption for Natural Persons	Signing Stick SPARE Authentication Certificate	-	-	1.3.171.1.1.10.4.4	0.4.0.2042.1.3
		5	LCP for SPARE certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons	Signing Server SPARE certificate	-	-	1.3.171.1.1.10.4.5	0.4.0.2042.1.3
		6	Privacy+ certificate supporting Signature, Authentication & Encryption for Anonymous persons	Signing Server Privacy+ Certificate	-	-	1.3.171.1.1.10.4.6	
		0	Master document	N/A	x	у	1.3.171.1.1.10.5.0.x.y	N/A
10		1	SSL/TLS Standard Server Certificates	SSL/TLS Standard Server Certificates	-	-	1.3.171.1.1.10.5.1	0.4.0.2042.1.3
CP's LuxTrust Global Chain		2	SSL/TLS(+) Extended Validation Server Certificates - EVCP	SSL/TLS Extended Validation Server Certificates	-	-	1.3.171.1.1.10.5.2	0.4.0.2042.1.4
	<b>5</b> LuxTrust SSL CA	3	SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	-	-	1.3.171.1.1.10.5.3	0.4.0.2042.1.5
		4	Object Signing(+ ) Certificates	Object Signing(+ ) Certificates	-	-	1.3.171.1.1.10.5.4	0.4.0.2042.1.3
		5	SSL/TLS Client Certificate	SSL/TLS Client Certificate			1.3.171.1.1.10.5.5	0.4.0.2042.1.3
		0	Master document	N/A	x	у	1.3.171.1.1.10.6.0	N/A
	6	1	LCP for TEST certificates for QCP+ certificates		-	-	1.3.171.1.1.10.6.1	0.4.0.2042.1.3



Document category	Document		Sub-document - description	LuxTrust Product	Version	Sub- version	Complete OID	ETSI OID
	LuxTrust TEST CA		supporting Qualified Electronic Signature (for					
			Natural Persons)					
			LCP for TEST certificates for LuxTrust Signing					
		2	Server, NCP certificate supporting Signature,		-	-	1.3.171.1.1.10.6.2	0.4.0.2042.1.3
			Authentication & Encryption for Natural Persons					
		3	LCP for TEST certificates for NCP+ Supporting		_	_	1.3.171.1.1.10.6.3	0.4.0.2042.1.3
			Authentication & Encryption for Natural Persons					01110120121110
		4	LCP for TEST certificates for NCP Supporting		_	_	1.3.171.1.1.10.6.4	0.4.0.2042.1.3
			Authentication & Encryption for Natural Persons					01110120121110
			LCP for TEST certificates for QCP supporting					
			Advanced Electronic Signature with a Qualified		-	-	1.3.171.1.1.10.6.5	0.4.0.2042.1.3
			Certificate (for Natural Persons)					
			LCP for TEST certificates supporting Advanced					
		6	Electronic Signature with a Qualified Certificate		-	-	1.3.171.1.1.10.6.6	0.4.0.2042.1.3
			for Mass Signature Services					
		0	Master document	N/A	x	у	1.3.171.1.1.10.7.0	N/A
		1	QCP+ supporting Qualified Electronic Signature (for Natural Persons)	RA SmartCard Signature certificate	-	-	1.3.171.1.1.10.7.1	0.4.0.1456.1.2
	LuxTrust Internal CA	2	NCP+ supporting Authentication & Encryption for Natural Persons	RA SmartCard Authentication certificate	-	-	1.3.171.1.1.10.7.2	0.4.0.2042.1.2
		0	Master document	N/A			1.3.171.1.1.10.8.0	N/A
		1	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate			1.3.171.1.1.10.8.1	
	8 LuxTrust Global	LuxTrust Global Timestamping CA 2		Third Party				
	Timestamping CA		Third Party TimeStamping certificate	TimeStamping certificate			1.3.171.1.1.10.8.2	
		0	Master document	N/A			1.3.171.1.1.10.9.0	N/A
	8 LuxTrust eGovernment CA	Reser ved for future use						



Document category	Document	Sub-document - description	LuxTrust Product	Version	Sub- version	Complete OID	ETSI OID



#### 3.2 LuxTrust Certification Authorities - Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

#### 3.2.1 LuxTrust Global Root CA

	Lux	Trust Gl	obal Roo	ot 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 CA Signature	
Validity					
NotBefore		Х		Key Generation Process Date/Time	
NotAfter		х		Key Generation Process Date/Time + 10;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>2</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>2</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies <sup>3</sup>	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.10	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed

 $<sup>^{2}</sup>$  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.

 $<sup>^3</sup>$  Since LuxTrust Global Root 2



Page 29 de 112





VFRSION 1 21

	Lux	Trust Glo	obal Roo	t CA	
Base Profile	OID	Included	Critical	Value	
KeyUsage	{id-ce 15}	×	TRUE <sup>7</sup>		
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
Keyldentifier		X		SHA-1 Hash	
subjectKeyldentifier	{id-ce 14}	X	FALSE		
Keyldentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE <sup>7</sup>		
CA		×		TRUE	Fixed
pathLenConstraint		Х		None	Fixed

#### 3.2.2 LuxTrust Global Qualified CA

LuxTrust Global Qualified 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>2</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>4</sup>	Fixed		

 $<sup>^4</sup>$  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.



Page 30 de 112





	LuxTrust Global Qualified CA							
Base Profile	OID	Included	Critical	Value				
organizationName		Х		LuxTrust S.A.	Fixed			
CertificatePolicies	{id-ce 32}	Х	FALSE					
policyldentifier		Х		1.3.171.1.1.1.10.3	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>7</sup>					
keyCertSign				Set	Fixed			
crlSign				Set	Fixed			
authorityKeyldentifier	{id-ce 35}	Х	FALSE					
Keyldentifier		Х		SHA-1 Hash of Authority public key				
authorityInfoAccess <sup>5</sup>	{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/LTGRCAx <sup>22</sup> .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/LTGRCAx <sup>6</sup> .crl	Fixed			
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/A				
CA		Х		TRUE	Fixed			
pathLenConstraint		Х		0 (Zero)	Fixed			

#### 3.2.3 LuxTrust Privacy+ CA

LuxTrust Privacy+ 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		

<sup>&</sup>lt;sup>5</sup> Since LuxTrust Global Qualified CA 3

<sup>&</sup>lt;sup>7</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".



Page 31 de 112

 $<sup>^{6}</sup>$  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



VEDSION 1 21

LuxTrust Privacy+ CA						
Base Profile	OID	Included	Critical	Value		
SignatureValue		Х		Issuing LTGRCA Signature		
Validity						
NotBefore		Х		Key Generation Process Date/Time		
NotAfter		Х		Key Generation Process Date/Time +up to 6 years	Fixed	
SubjectPublicKeyInfo		Х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).		
Issuer						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>2</sup>	Fixed	
organizationName		Х		LuxTrust S.A.	Fixed	
Subject						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }			LuxTrust Privacy+ CA x <sup>8</sup>	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		Х		https://repository.luxtrust.lu	Fixed	
KeyUsage	{id-ce 15}	Х	TRUE <sup>7</sup>			
keyCertSign				Set	Fixed	
crlSign				Set	Fixed	
authorityKeyldentifier	{id-ce 35}	Х	FALSE			
Keyldentifier		Х		SHA-1 Hash of Authority public key		
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/LTGRCAx <sup>6</sup> .crl	Fixed	
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/a		
CA		Х		TRUE	Fixed	
pathLenConstraint		Х		0 (Zero)	Fixed	

 $<sup>^{8}</sup>$  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.



Page 32 de 112

#### 3.2.4 LuxTrust SSL CA

LuxTrust SSL CA							
Base Profile	OID	Included	Critical	Value			
Version		Х		V3			
SerialNumber		Х		As provided by CA or by LuxTrust S.A.			
SignatureAlgorithm							
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed		
SignatureValue		Х		Issuing LTGRCA Signature			
Validity							
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>2</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }			LuxTrust SSL CA x9	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
CertificatePolicies	{id-ce 32}	Х	FALSE				
policyldentifier (1)		X		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>7</sup>				
keyCertSign				Set	Fixed		
crlSign				Set	Fixed		
authorityKeyldentifier	{id-ce 35}	Х	FALSE				

 $<sup>^{9}</sup>$  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.



Page 33 de 112





	LuxTrust SSL CA							
Base Profile	OID	Included	Critical	Value				
Keyldentifier		Х		SHA-1 Hash of Authority public key				
authorityInfoAccess <sup>10</sup>	{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/LTGRCAx22.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/LTGRCAx <sup>2</sup> .crl	Fixed			
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/a				
CA		Х		TRUE	Fixed			
pathLenConstraint		Х		0 (Zero)	Fixed			

#### 3.2.5 LuxTrust TEST CA

LuxTrust TEST 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 6 years	Fixed		
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).			
Issuer							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>2</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	Х		LU	Fixed		

 $<sup>^{10}</sup>$  Since LuxTrust SSL CA 4



Page 34 de 112





VFRSION 1 21

	LuxTrust TEST CA						
Base Profile	OID	Included	Critical	Value			
CommonName	{ id-at-3 }			LuxTrust TEST CA x <sup>11</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
CertificatePolicies	{id-ce 32}	Х	FALSE				
policyldentifier		Х		1.3.171.1.1.10.6	Fixed		
policyQualifiers				N/a			
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed		
Qualifier		Х		https://repository.luxtrust.lu	Fixed		
KeyUsage	{id-ce 15}	Х	TRUE <sup>7</sup>				
keyCertSign				Set	Fixed		
crlSign				Set	Fixed		
authorityKeyldentifier	{id-ce 35}	Х	FALSE				
Keyldentifier		Х		SHA-1 Hash of Authority public key			
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>6</sup> .crl	Fixed		
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/A			
CA		Х		TRUE	Fixed		
pathLenConstraint		Х		0 (Zero)	Fixed		

#### 3.2.6 LuxTrust Internal CA

	LuxTrust Internal 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 6 years	Fixed				
SubjectPublicKeyInfo		Х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).					
Issuer									

 $<sup>^{11}</sup>$  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.



Page 35 de 112





	LuxTrust Internal CA							
Base Profile	OID	Included	Critical	Value				
CountryName	{ id-at-6 }	Х		LU	Fixed			
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>2</sup>	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
Subject								
CountryName	{ id-at-6 }	Х		LU	Fixed			
CommonName	{ id-at-3 }			LuxTrust Internal CA x <sup>12</sup>	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
CertificatePolicies	{id-ce 32}	Х	FALSE					
policyldentifier		Х		1.3.171.1.1.1.10.7	Fixed			
policyQualifiers				N/a				
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed			
Qualifier		Х		https://repository.luxtrust.lu	Fixed			
KeyUsage	{id-ce 15}	Х	TRUE <sup>7</sup>					
keyCertSign				Set	Fixed			
crlSign				Set	Fixed			
digitalSignature				Set	Fixed			
nonRepudiation				Set	Fixed			
authorityKeyldentifier	{id-ce 35}	Х	FALSE					
Keyldentifier		Х		SHA-1 Hash of Authority public key				
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>6</sup> .crl	Fixed			
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/a				
CA		Х		TRUE	Fixed			
pathLenConstraint		Х		0 (Zero)	Fixed			

#### 3.2.7 LuxTrust TSA (Timestamping) CA

LuxTrust Global Timestamping CA							
Base Profile	OID	Included	Critical	Value			
Version		Х		V3			
SerialNumber		Х		As provided by CA or by LuxTrust S.A.			
SignatureAlgorithm							

 $<sup>^{12}</sup>$  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.



Page 36 de 112





	LuxTrus	t Global T	imestan	iping CA	
Base Profile	OID	Included	Critical	Value	
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>2</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>13</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.1.10.8	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier		Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	Х	TRUE <sup>7</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyldentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess14	{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/LTGRCAx <sup>2</sup> .crt	Fixed
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Subject public key	

 $<sup>^{13}</sup>$  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>14</sup> Since LuxTrust Global Timestamping CA 2







VFRSION 1 21

	LuxTrust Global Timestamping CA									
Base Profile	OID	Included	Critical	Value						
cRLDistributionPoints	{id-ce 31}	Х	FALSE							
distributionPoint										
FullName		Х		http://crl.luxtrust.lu/LTGRCA <sup>6</sup> .crl	Fixed					
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/a						
CA		Х		TRUE	Fixed					
pathLenConstraint		Х		0 (Zero)	Fixed					

## 3.2.8 LuxTrust e-Government CA

	Lux	rust eGo	vernmer	nt 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 6 years	Fixed
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>2</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust eGovernment CA x <sup>15</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyldentifier		X		1.3.171.1.1.10.9	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier		Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	Х	TRUE'		
keyCertSign				Set	Fixed

 $<sup>^{15}</sup>$  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.



Page 38 de 112





VFRSION 1 21

	Lux	Trust eGo	vernmer	nt CA	
Base Profile	OID	Included	Critical	Value	
crlSign				Set	Fixed
digitalSignature				Set	Fixed
nonRepudiation				Set	Fixed
authorityKeyldentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
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>6</sup> .crl	Fixed
BasicConstraints	{id-ce 19}	Х	TRUE <sup>7</sup>	N/a	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

### 3.2.9 Certificate extensions

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

### 3.2.10 Algorithm object identifiers

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

### 3.2.11 Name forms

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

## 3.2.12 Name constraints

Name constraints are supported as per RFC 5280.

### 3.2.13 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

### 3.2.14 Usage of Policy Constraints extension

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

### 3.2.15 Policy qualifiers syntax and semantics

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

## 3.3 LuxTrust End-entity - Certificates profiles

## 3.3.1 Certificate profiles

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







For the purpose of integration with current devices such as the smartcard, the signing stick and signing server, the following five types of LuxTrust Certificates will be issued under the 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>16</sup> Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy OID 1.3.171.1.10.3.1. and
  - One LuxTrust NCP+<sup>17</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.
- 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>16</sup> Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.1.10.3.3, and
  - One LuxTrust NCP<sup>17</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.4.
- 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>17</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.

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

- LuxTrust SSL/TLS Standard Server Certificates: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.1.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.2.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP+: SSL compliant ETSI TS 102 042 [4] Certificate
  generated on Secure User Device, under the Certificate OID Policy 1.3.171.1.1.10.5.3.
- LuxTrust Object Signing (+) Certificates: Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.4.
- LuxTrust SSL/TLS Client Certificates: Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.11.05.5.

#### 3.3.2 Version number(s)

X.509 v3 is supported and used.

### 3.3.3 LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures

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

<sup>&</sup>lt;sup>17</sup> As defined in ETSI TS 102 042 (cf. [4]).



 $<sup>^{16}</sup>$  As defined by ETSI TS 101 456 (cf. [3]).





VFRSION 1 21

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.

	Lux	Trust SS	CD Q	CP+ Ce	rtifica	ite Profile
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"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	<b>√</b>	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVal	ue	<b>√</b>	False			
					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	
	countryName	<b>✓</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity		<b>√</b>	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36
						Months
Subject		<b>√</b>	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)

 $<sup>^{18}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certificate profile.

 $<sup>^{22}</sup>$  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.



 $<sup>^{19}</sup>$  CE = Critical Extension.

<sup>20</sup> O/M: O = Optional, M = Mandatory.

 $<sup>^{21}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.





	Lux	rust SS	CD QC	P+ Ce	rtifica	te Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:  Fixed value: "Private Person"
	title	<b>√</b>		М	D	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., 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	<b>√</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPublic	KeyInfo	✓	False			
	Algorithm	<b>✓</b>				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	<b>√</b>		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyl	dentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo/	Access	<b>√</b>	False			
	AccessMethod	<b>√</b>				ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				
cRLDistribution		<b>√</b>	False			
	distributionPoint	✓ ✓			S	22
	fullName	<b>v</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl







Attribute	Field	IN18	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Subject						
Properties						
subjectAltNa	ıme	<b>✓</b>	False			
•	Rfc822Name	<b>✓</b>		0	D	Certificate Holder's email address
subjectKeylo	lentifier	<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						
keyUsage	•	<b>✓</b>	True			
	digitalSignature	<b>✓</b>			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	<b>✓</b>			S	False
certificatePo	licies	<b>✓</b>	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>√</b>				LuxTrust Qualified Certificate on SSC compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP.  Sole Authorised Usage: Support of Qualified Electronic Signature.
	Policyldentifier	<b>✓</b>				0.4.0.1456.1.1
QualifiedCer	tificateStat					
	QcCompliance	<b>✓</b>		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliand with [5]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliand with [5]
	QcSSCD	✓		М	D	Set

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

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

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]).





# **LuxTrust Global Root CA Certificate Specifications**

VFRSION 1 21

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.

	Lux	Trust S	SSCD N	ICP+ Ce	ertifica	te Profile
Attribute	Field	<b>IN</b> 18	<b>CE</b> <sup>19</sup>	<b>O/M</b> <sup>20</sup>	CO <sup>21</sup>	Value
Base Profile						
Version		<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumber	r	<b>✓</b>	False			
					FDV	Validated on duplicates.
signatureAlgo	orithm	<b>✓</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValu	ie	<b>√</b>	False			
					D	Issuing CA Signature.
issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	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	✓		М	D	Serial Number as constructed by LRAO
						PRO and PRIVATE products: Concatenation
	commonName	✓		М	D	of given name(s) and surname(s) as on ID
						card separated by a "Space" character
						PRO and PRIVATE products: Given name(s)
	givenName	<b>√</b>		М	D	as on ID card
						PRO and PRIVATE products: Surname(s) as
	surname	✓		М	D	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







	LuxT	rust S	SCD N	ICP+ Ce	rtifica	te Profile
Attribute	Field	<b>IN</b> 18	<b>CE</b> <sup>19</sup>	<b>O/M</b> <sup>20</sup>	<b>CO</b> <sup>21</sup>	Value
	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>		M	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		M	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<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	<b>√</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPublich	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeylo	dentifier	<b>√</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfoA	ccess	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributio	nPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						







VFRSION 12:

	Lux	Trust S	SSCD I	NCP+ Ce	rtifica	te Profile
Attribute	Field	<b>IN</b> 18	<b>CE</b> <sup>19</sup>	<b>O/M</b> <sup>20</sup>	CO <sup>21</sup>	Value
subjectAltNar	me	<b>√</b>	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylde	entifier	✓	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		<b>√</b>	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	<b>✓</b>			S	True
	dataEncipherment	✓			S	True
certificatePoli	icies	<b>√</b>	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.2
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	noticeNumbers					
	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

## 3.3.5 LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures

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

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

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

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

## **LuxTrust non SSCD QCP Certificate Profile**





# **LuxTrust Global Root CA Certificate Specifications**

Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	ər	<b>✓</b>	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	lue	✓	False			
					D	Issuing CA Signature.
Issuer	,	<b>✓</b>	False		S	
	countryName	<b>√</b>			s	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>✓</b>			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	,	<b>✓</b>	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
	sumame	<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	✓		М	D	PRIVATE products:  Fixed value: "Private Person"  PRO products:  "Professional Person" (default) or "Professional Administrator"  (Other titles possible for special purpose certificates)







	LuxTı	rust n	on SS	CD QCP	Certif	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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
subj	jectPublicKeyInfo	✓	False			
	Algorithm	<b>~</b>				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Pro	pperties					
authorityKey	Identifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Qualified</b> 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	<b>✓</b>				http://ocsp.luxtrust.lu
cRLDistributi	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Prop	perties					
subjectAltNa	me	✓	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address







	LuxT	rust n	on SS	CD QCP	Certif	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</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 Prope	erties					
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	<b>✓</b>			S	True
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	✓			S	False
certificatePo	olicies	✓	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.3
	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)
	noticeNumbers					
	DisplayText	<b>✓</b>				LuxTrust Qualified Certificate <b>not</b> on SSCD compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Advanced Electronic
						Signature supported by a Qualified cert
	PolicyIdentifier	✓				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 [5]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓				NOT SET

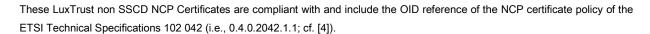
# 3.3.6 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

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









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.

	LuxTr	ust non S	SSCD N	NCP Cer	tificat	e Profile
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"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVa	llue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>22</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	<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
	sumame	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	<b>✓</b>		М	D	Nationality of holder (ISO3166)
	emailAddress	<b>✓</b>		0	D	Subject's email address







	LuxTrust	non S	SSCD N	ICP Cer	tificat	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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	✓		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	cKeyInfo	<b>√</b>	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey	Identifier keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	<b>√</b>				ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓ ✓				ld-ad-1
<b></b>	accessLocation	<b>✓</b>				http://ocsp.luxtrust.lu
cRLDistribut	T .	· ·	False			
	distributionPoint fullName	· ·			S	http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
	iuiiivaitie					http://ch.iuxtrust.iu/LTGQCAX .Cfl







	LuxTrust	non S	SSCD N	ICP Cer	tificat	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Subject						
Properties						
subjectAltNa	ime	<b>✓</b>	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	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						
keyUsage		<b>√</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation				S	False
	. =	<b>√</b>				_
	keyEncipherment				S	True
	data Francisch anna ant	<b>-</b>				Tmus
	dataEncipherment				S	True
certificatePo	licias	✓	False			
ocitinoator o	Policyldentifier	<b>√</b>	1 dioc			1.3.171.1.1.10.3.4
	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)
	noticeNumbers					
	DisplayText	<b>✓</b>				LuxTrust Certificate not on SSCD
						compliant with ETSI TS 102 042 NCP
						certificate policy. Key Generation by CSP.
						Sole Authorised Usage: Data or Entity
						Authentication and Data Encryption.
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.1

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

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

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





# **LuxTrust Global Root CA Certificate Specifications**

VFRSION 1 21

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

	LuxTrust	Signing	Serve	r NCP (	Certific	cate 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			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption.
						OID = "1.2.840.113549.1.1.11" - if
						SHA256 with RSA Encryption.
signatureVa	alue	<b>✓</b>	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>√</b>			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	L	<b>✓</b>	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	<b>✓</b>		0	D	Subject's email address





	LuxTrust Si	gning	Serve	r NCP (	Certific	cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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	✓		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	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey	ldentifier keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	<b>V</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	✓ ✓				http://ocsp.luxtrust.lu
cRLDistribut	T	<b>V</b>	False			
	distributionPoint	· ·			S	http://crl.luxtrust.lu/LTGQCA <sup>22</sup> .crl
	fullName					nup://cn.iuxtrust.iu/LTGQCA .cri





**L**LUXTUUST

VERSION 1.2

	LuxTrust	Signing	Serve	r NCP (	Certific	cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Subject						
Properties						
subjectAltNa	ime	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyId	dentifier	✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit
						field with a 0100 value, followed by the
						least significant 60 bits of the SHA-1 hash
						of the value or subjectPublicKey bit string
						(tag, not including the length and number
						of unused bit-string bits).
Policy						
Properties						
keyUsage		<b>*</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation				S	True
		<b>✓</b>			_	
	keyEncipherment				S	True
		<b>✓</b>				-
	dataEncipherment				S	True
certificatePol	liaiaa	<b>✓</b>	False			
Certificater of	Policyldentifier	<b>✓</b>	1 disc			1.3.171.1.1.10.3.5
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					1- 4 (
	DisplayText	✓				LuxTrust Certificate not on SSCD
	= .5p.my . 57					compliant with ETSI TS 102 042 NCP
						certificate policy. Key Generation by CSP.
						Sole Authorised Usage: Signature, Data or
						Entity Authentication and Data Encryption.
			1	ı	1	,

## 3.3.8 LuxTrust NCP+ Certificates supporting Mass Signature Services

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

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

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

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







LuxTrust non	SSCD NCP+ Public (	Certi	ficate	Profil	e for	Mass Signature Services
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		<b>√</b>	False			
					FDV	Validated on duplicates.
signatureAlgorithm	<u> </u>	<b>✓</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" -
						SHA256 with RSA Encryption
signatureValue		✓	False			
-					D	Issuing CA Signature.
Issuer		<b>✓</b>	False		S	
	countryName	<b>✓</b>			S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	ga	<b>✓</b>	False			
validity	NotBefore	<b>✓</b>	1 dioc		D	Certificate generation process
	Notboloro					date/time.
	NotAfter	<b>√</b>			D	
	Noone				D	Certificate generation process date/time + <b>36</b> Months
subject		<b>✓</b>	False			date/time + 30 Worths
Subject			i aise			
						Names as in articles of association,
	commonName	✓		М	D	including the legal form (as specified in
						the memorandum and articles of
						association or an equivalent document)
						Country in which the organization's
	a a company de la company	<b>✓</b>			_	registered office is established (as
	countryName	*		M	D	specified in the memorandum and
						articles of association). (ISO3166)
	stateOrProvinceName	<b>√</b>		0	D	
	StateOfFioviliceName	ļ ,		0	D	
	emailAddress	✓		0	D	Subject's email address if available
						Names as in articles of association,
					_	including the legal form (as specified in
	organizationName	✓		М	D	the memorandum and articles of
						association or an equivalent document)
						Location in which the organization's
	la a life Allama	<b>✓</b>			_	registered office is established (as
	localityName	•		M	D	specified in the memorandum and
						articles of association or an equivalent
						document)
	organizational InitName 4	<b>✓</b>		0	D	As provided by Subscriber
	organizationalUnitName 1	*		U	U	As provided by Subscriber
	organizationalUnitName 2	✓		0	D	As provided by Subscriber







VFRSION 1 21

Attribute	Field	IN18	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
subjectPublicKeyInfo	1 1014	<b>■</b> ✓	False	O/III		Value
<b>,</b>	algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	<b>✓</b>		М		public exponent: Fermat-4 (=010001).
Extensions	oubjood ubilottoy			141		pasie experient remar ( 0 recer).
Authority Properties						
authorityKeyIdentifier		<b>✓</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Glob</b> a
	noyiuoniino.					Qualified CA public key
authorityInfoAccess		<b>✓</b>	False			addinion of passion roy
	AccessMethod	<b>✓</b>				ld-ad-2
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>✓</b>				Id-ad-1
	accessLocation	<b>✓</b>				http://ocsp.luxtrust.lu
cRLDistributionPoint	dooosecodaton	<b>✓</b>	False			TRE-MOOSPHAKITUSCHU
OTEDIORIDATION ONE	distributionPoint	<b>✓</b>	1 0100		S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties	Tullivarie					TREP.//GIT.IUX.IUS.T.IU/ET GQO/X
subjectAltName		<b>✓</b>	False			
3ubject aname	Rfc822Name	<b>✓</b>	1 disc	0	D	Certificate Holder's email address
subjectKeyldentifier	MODZZMAINE	<b>✓</b>	False			Octimeate Floride 3 ciriaii address
Subjectiveyidentinei	keyldentifier	<b>✓</b>	i aise		Fixed	The Key Identifier comprises a four-b
	Regidentifie				i ixeu	field with a 0100 value, followed by th
						least significant 60 bits of the SHA-
						hash of the value or subjectPublicKe
						bit string (tag, not including the length
						and number of unused bit-string bits).
Policy Properties						and number of unused bit-string bits).
keyUsage		<b>✓</b>	True			
ney Osage	digitalSignature	<b>✓</b>	True		S	False
	digitaloighature				3	i dise
	nonRepudiation				S	True
	nomæpadiation				3	Tide
	keyEncipherment	<b>✓</b>			S	False
	Reyundiplientient				3	i dise
	dataEncipherment	<b>✓</b>			S	False
	- GALGETTOPHOTHOUR					
certificatePolicies		<b>✓</b>	False			
3.0.00	Policyldentifier	<b>✓</b>				1.3.171.1.10.3.6
	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)
	noticeNumbers				3	ia que (OSCI NOLICE)





VFRSION 1 21

LuxTrust non	LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services								
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value			
	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.			
						GTC, CP and CPS on			
						http://repository.luxtrust.lu.			
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2			

## 3.3.9 LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures

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

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

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

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

	LuxTrus	t SSCD	LCP+ I	ntegra	tion C	ertificate Profile
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"
SerialNumbe	er	<b>√</b>	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	<b>√</b>	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVal	ue	<b>√</b>	False			
					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	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		✓	False			







	LuxTrus	t SSCD	LCP+ I	ntegra	tion Co	ertificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>~</b>		М	D	LGQCA XX SC PRI V3 (XX a number selected internally by LuxTrust)
	givenName	✓		М	D	LGQCA XX (XX a number selected internally by LuxTrust)
	surname	<b>√</b>		М	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	<b>√</b>		0	D	N/A
	title	✓		М	D	Private Person
subjectPublic	:KeyInfo	<b>√</b>	False			
	Algorithm	<b>✓</b>				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	<b>√</b>		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyl	dentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified
authorityInfo/	Access	<b>√</b>	False			CA public key
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>✓</b>				http://ocsp.luxtrust.lu
cRLDistributi	1	<b>√</b>	False			- op - o - o - o - o - o - o
	distributionPoint	<b>√</b>			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeyld		<b>✓</b>	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significan 60 bits of the SHA-1 hash of the value o subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits)
Policy						,
Properties						
keyUsage		<b>√</b>	True			
-	digitalSignature	<b>✓</b>			S	False
	nonRepudiation	<b>✓</b>			S	True
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	<b>✓</b>	1		S	False





FLUXTUUST

VERSION 1.21

	LuxTrus	t SSCD L	.CP+ I	ntegra	tion Co	ertificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
certificatePoli	icies	✓	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.7
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on SSCD compliant with ETSI TS 102 042 LCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage:</b> Support of Integration Electronic Signature.
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.3
QualifiedCert	ificateStat					
	QcCompliance	<b>✓</b>		0	S	Not Set
	QcLimitValue	✓		0	D	Not Set
	QcRetentionPeriod	✓		0	D	Not Set
	QcSSCD	✓		М	D	Set

# 3.3.10 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 S	SSCD L	.CP+ I	ntegra	tion Ce	ertificate Profile
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	Validated on duplicates.
signatureAlgo	rithm	<b>✓</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValue	е	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	







A46-11 4	LuxTrust	15.140	0540	0.5 400	0004	W.I
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	countryName	<b>V</b> ✓			S	LU
	commonName				S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>√</b>			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 + 3
						Months
subject		<b>√</b>	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						LGQCA XX SC PRI V3 (XX a number selecte
	commonName	✓		М	D	internally by LuxTrust)
						mornary by Laxiraby
	givenName	<b>✓</b>		М	D	LGQCA XX (XX a number selected internal
	givernitainis					by LuxTrust)
	surname	✓		М	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	N/A
	title	✓		М	D	Private Person
subjectPublic	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); publi
	subjectPublicKey	<b>√</b>		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKeyl	dentifier	<b>✓</b>	False			
	keyldentifier	<b>~</b>				SHA-1 Hash of the LuxTrust Global Qualifie
						CA public key
authorityInfo/	Access	<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
cRLDistribution	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNar	me	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeyIde	entifier	✓	False			
- ·	keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field wit
						a 0100 value, followed by the least significar
						60 bits of the SHA-1 hash of the value of
					1	subjectPublicKey bit string (tag, not includin







VFRSION 12

	LuxTrust	SSCD I	_CP+ I	ntegra	tion Ce	ertificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
						the length and number of unused bit-string
						bits).
Policy						
Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	<b>✓</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePoli	cies	<b>√</b>	False			
'	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.8
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on
						SSCD compliant with ETSI TS 102 042 LCP+
						certificate policy. Key Generation by CSP. Sole
						Authorised Usage: Authentication and
						Encryption for Integration Purposes.
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.3

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

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

These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the 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. These Certificates include the corresponding LuxTrust Signing Server Account OID, i.e., <OID 1.3.171.1.1.10.3.9>.

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

	LuxTrust Sig	gning	Serve	er LCP C	ertific	ate 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			
					S	Version 3 Value = "2"







	LuxTrus	t Signing	Serve	r LCP (	Certific	cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" - it SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>22</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	~		М	D	LGQCA XX CSS (XX a number selected internally by LuxTrust)
	givenName	~		М	D	LGQCA XX (XX a number selected internally by LuxTrust)
	surname	<b>✓</b>		М	D	CSS
	countryName	<b>✓</b>		М	D	LU
	emailAddress	✓		0	D	N/A
	title	<b>*</b>		М	D	Private Person
subjectPubli	1	<b>√</b>	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA)
	subjectPublicKey	<b>✓</b>		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Globa Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistribut	tionPoint	✓	False			







						cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	distributionPoint	<b>*</b>			S	22
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeyl	dentifier	✓	False			
	keyldentifier	<b>*</b>			Fixed	The Key Identifier comprises a four-bettel field with a 0100 value, followed by the least significant 60 bits of the SHA-1 has 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	blicies	✓	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.10.3.9
	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)
	noticeNumbers					-
	DisplayText	V				INTEGRATION Certificate not on SSC compliant with ETSI TS 102 042 LC cert.policy. Key Generation by CSP. So Authorised Usage: Signature, Data Entity Auth. and Data Enc. for integration
	Policyldentifier	<b>✓</b>				purposes 0.4.0.2042.1.3

## 3.3.12 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]).





# **LuxTrust Global Root CA Certificate Specifications**

VFRSION 1 21

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.

	LuxTru	st SSCD	LORA	QCP+	Certif	icate Profile
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"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
		<b>√</b>				RSA Encryption.
signatureVal	ue	•	False		_	
1		<b>√</b>			D	Issuing CA Signature.
Issuer		<b>→</b>	False		S	
	countryName	√ ·			S	LU Luc Truck Olabel Ovelland CA v 22
	commonName	<i>'</i>			S	LuxTrust Global Qualified CA x <sup>22</sup>
Validit.	organizationName	✓	Falsa		S	LuxTrust S.A.
Validity	NotBefore	<b>√</b>	False		D	Cartificate gaparation process data/time
	NotAfter	<b>√</b>			D	Certificate generation process date/time.  Certificate generation process date/time + 36
	NODAILE					Months
Subject		✓	False			Working
Cubject	serialNumber	<b>√</b>	. 4.00	M	D	Social Number as constructed by LPAO
	Serialivumber	•		IVI	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(s) as on ID card without indication
	surname	✓		М	D	"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	<b>√</b>		М	D	Country of RA
	- County Harris			141		Soundy of tot
	organizationalUnitName	✓		М	D	RA code Constructed by LuxTrust
	1					







	LuxTru	st SSCD	LORA	QCP+	Certif	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	organizationalUnitName					
	2	✓		М	D	RAO code Constructed by LuxTrust
subjectPublic	cKeyInfo	✓	False			
Subjecti ubili	Algorithm	<b>√</b>	1 alsc			Public Key: Key length: 2048bit (RSA); publi
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions	oubjooti ubilortoy			141		onpononia i dimati i ( di todo i).
Authority						
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualifie
						CA public key
authorityInfo	Access	<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributi	ionPoint	<b>√</b>	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNa	ime	<b>√</b>	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	dentifier	✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field
						with a 0100 value, followed by the leas
						significant 60 bits of the SHA-1 hash of the
						value or subjectPublicKey bit string (tag, no
						including the length and number of unused
						bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			
	digitalSignature	<b>√</b>			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePo	licies	✓	False		_	
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.3.10
	policyQualifierID	<b>~</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers	-				







VFRSION 12:

	LuxTru	st SSCD	LORA	QCP+	Certif	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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	tificateStat					
	QcCompliance	✓		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [5]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓		М	D	Set

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

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

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

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

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

	LuxTri	ust SSC	D LOR	A NCP+	Certif	icate Profile
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	Validated on duplicates.
signatureAlgo	rithm	<b>√</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValu	е	<b>✓</b>	False			
					D	Issuing CA Signature.
issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.







	Luxirus	st 55C	D LUK	ANCPT	cerui	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
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	<b>√</b>		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by "Space" character
	givenName	✓		М	D	Given name(s) as on ID card
	surname	<b>√</b>		M	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	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName	<b>✓</b>		М	D	RAO code Constructed by LuxTrust
subjectPublicl	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); publ
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeylo	dentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualifie</b> CA public key
authorityInfoA	Access	✓	False			
-	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
cRLDistributio		✓	False			
	distributionPoint	<b>✓</b>			_	
	aistributionPoint				S	







	LuxTrus	st SSC	D LOR	A NCP+	NCP+ Certificate Profile		
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value	
Subject							
Properties		<b>✓</b>					
subjectAltNan	subjectAltName		False				
	Rfc822Name	✓		0	D	Certificate Holder's email address	
subjectKeylde	entifier	<b>√</b>	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							
keyUsage		<b>√</b>	True				
	digitalSignature	✓			S	True	
	nonRepudiation				S	False	
	keyEncipherment	<b>✓</b>			S	True	
	dataEncipherment	✓			S	True	
certificatePolic	cies	✓	False				
	Policyldentifier	✓				1.3.171.1.1.10.3.11	
	policyQualifierID	✓			S	Id-qt-1 (CPS)	
	qualifier	✓			S	https://repository.luxtrust.lu	
	policyQualifierID	✓			S	Id-qt-2 (User Notice)	
	noticeNumbers						
	DisplayText	<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	<b>√</b>				0.4.0.2042.1.2	

# 3.3.14 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]).





# **LuxTrust Global Root CA Certificate Specifications**

VFRSION 1 21

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>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"	
SerialNumbe	er	<b>✓</b>	False				
					FDV	Validated on duplicates.	
signatureAlg	signatureAlgorithm		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>Global Qualified</b> CA x <sup>22</sup>	
	organizationName	✓			S	LuxTrust S.A.	
Validity	Validity		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	
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character	
	givenName	<b>✓</b>		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	<b>√</b>		0	D	Subject's email address	
	Title	✓		М	D	"LuxTrust RA officer – LRS"	







	LuxTrust non SSC	CD QC	P Mas	s LRAO	Signa	tures Certificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	organizationName	<b>✓</b>		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA
	localityName	<b>√</b>		М	D	Country of RA (as in articles of association)
	organizationalUnitName	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName	<b>√</b>		0	D	RAO code Constructed by LuxTrust
sub	jectPublicKeyInfo	✓	False			
	Algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Pro	pperties					
authorityKey	Identifier	✓	False			
	keyldentifier	<b>~</b>				SHA-1 Hash of the <b>LuxTrust Global Qualified</b> CA public key
authorityInfo	authorityInfoAccess		False			
	AccessMethod	<b>✓</b>				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Prop	erties					
subjectAltNa	me	✓	False			
	Rfc822Name	<b>✓</b>		0	D	Certificate Holder's email address
subjectKeyld	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	keyUsage		True			







VFRSION 12:

	LuxTrust non SS	CD QC	P Mas	s LRAO	Signa	tures Certificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.12
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate <b>not</b> SSCD compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP.
						Sole Authorised Usage: Support of Advanced Electronic Signature for Mass LRAO purposes
	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 [5]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [5]
	QcSSCD	✓				NOT SET

### 3.3.15 LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures

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

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

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

According to the Luxembourg legislation, the eID card must always contain certificates. When ordering an eID card, the citizen has the choice to request or not the activation of his certificates. In case he has chosen not to activate his certificates, LuxTrust is







VFRSION 1 21

not allowed to detain the personal citizen data according to the personal data protection and management of the national register law. Therefore, when a citizen does not want to activate and use his certificates:

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

The certificate re-key is not allowed.

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

	LuxTrust eID SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>23</sup>	CE <sup>24</sup>	O/M <sup>25</sup>	CO <sup>26</sup>	Value				
Base										
Profile										
Version	<b>.</b>	<b>✓</b>	False							
					S	Version 3 Value = "2"				
SerialNumb	er	<b>✓</b>	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	<b>√</b>	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	<b>✓</b>			S	LU				
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x <sup>27</sup>				
	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 +				
						maximum 120 Months;				
						Certificate generation process date/time + 1				
						day for PSEUDONYM Certificate				
Subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s)				
	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				

 $<sup>^{23}\,\</sup>mbox{IN}$  = Included: Attribute / field included within the certificate profile.

 $<sup>^{27}</sup>$  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.



 $<sup>^{24}</sup>$  CE = Critical Extension.

 $<sup>^{25}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{26}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.





LuxTrust eID SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>23</sup>	CE <sup>24</sup>	O/M <sup>25</sup>	CO <sup>26</sup>	Value			
	countryName	✓		М	D	LU			
	emailAddress	✓		0	D	Subject's email address			
	title	✓		М	D	"Private Person"			
	organizationalUnitName 1	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " (Date of birth + 18 years).			
subjectPublic	:KeyInfo	<b>√</b>	False						
	Algorithm	<b>√</b>				Public Key: Key length: 2048bit up to 4096l			
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).			
Extensions									
Authority Properties									
authorityKeyl	Identifier	✓	False						
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualifi</b> CA x public key			
authorityInfo/	Access	<b>✓</b>	False						
	AccessMethod	<b>√</b>				Id-ad-2			
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt			
	AccessMethod	<b>√</b>				Id-ad-1			
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu			
cRLDistributi	onPoint	<b>√</b>	False						
	distributionPoint	<b>√</b>			S				
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl			
Subject Properties									
subjectAltNa	me	✓	False						
	Rfc822Name	<b>√</b>		0	D	Subject email address			
subjectKeyld	entifier	<b>√</b>	False						
	keyldentifier	·			Fixed	The Key Identifier comprises a four-bit firm with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, including the length and number of unused lestring bits).			
Policy Properties									
keyUsage		<b>√</b>	True						
	digitalSignature	<b>√</b>			S	False			
	nonRepudiation	<b>√</b>			S	True			
	keyEncipherment	<b>√</b>			S	False			
	dataEncipherment	<b>√</b>			S	False			
certificatePol	icies	<b>√</b>	False						
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.13			
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			





L'UXTL'UET

VFRSION 12:

	LuxTrust eID SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>23</sup>	CE <sup>24</sup>	O/M <sup>25</sup>	CO <sup>26</sup>	Value				
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText PolicyIdentifier	✓ ✓				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.  0.4.0.1456.1.1				
QualifiedCer	tificateStat									
	QcCompliance	<b>✓</b>		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [5]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [5]				
	QcSSCD	<b>~</b>		М	D	Set				

#### 3.3.16 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	Attribute Field IN <sup>18</sup> CE <sup>19</sup> O/M <sup>20</sup> CO <sup>21</sup> Value								
Base Profile									
Version	Version   ✓ False								
S Vei						Version 3 Value = "2"			







A (( !!						e Profile
Attribute	Field	<b>IN</b> ¹8 ✓	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
SerialNumber	· T	•	False			
		/			FDV	Validated on duplicates.
signatureAlgo	rithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 wit
						RSA Encryption.
signatureValu	e	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust <b>Global Qualified</b> CA x <sup>22</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time
						maximum 120 Months;
						Certificate generation process date/time +
						day for PSEUDONYM Certificate
subject	L	✓	False			,
•	oorialNumbor	<b>√</b>		М		Social Number of constructed by LPAO
	serialNumber	•		IVI	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) and
	Commonwante	,		IVI	D	surname(s)
						Given name(c) as on ID card or as provide
	givenName	✓		М	D	Given name(s) as on ID card or as provide
						by the RNCID
						Surname(s) as on ID card without indication
	surname	✓		М	D	"épouse", "ép." or similar and the subseque
						name(s) or as provided by the RNCID
	to Ni					
	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).
subjectPublicl	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096b
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKeylo	dentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualifie
						CA x public key
authority/lnfc^	ccess	✓	Folso			Or CA Public Rey
authorityInfoA		<b>√</b>	False			ld ad 2
	AccessMethod	· ✓				Id-ad-2
	accessLocation	,				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt







VFRSION 12:

	LuxT	rust S	SCD N	CP+ Cei	tificat	e Profile
Attribute	Field	<b>IN</b> 18	<b>CE</b> <sup>19</sup>	<b>O/M</b> <sup>20</sup>	<b>CO</b> <sup>21</sup>	Value
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
cRLDistribution	onPoint	<b>√</b>	False			
	distributionPoint	<b>✓</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNar	ne	<b>√</b>	False			
	Rfc822Name	<b>V</b>		0	D	Subject email address
subjectKeyIde		<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	1	<b>√</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation				S	False
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>✓</b>			S	True
certificatePoli	cies	<b>√</b>	False			
	PolicyIdentifier	<b>√</b>				1.3.171.1.1.10.3.14
	policyQualifierID	<b>V</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	noticeNumbers	<b>✓</b>				
	DisplayText	·				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity
	Policyldontifica	<b>✓</b>				Authentication and Data Encryption.
-	Policyldentifier					0.4.0.2042.1.2

# 3.3.17 LuxTrust eID SSCD LCP+ Certificates supporting Qualified 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]).







VFRSION 1 21

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust eID SSC	D LCP I	ntegra	tion Si	gnatı	ıre Certificate Profile
Attribute	Field	IN <sup>28</sup>	CE <sup>29</sup>	<b>O/M</b> <sup>30</sup>	<b>CO</b> <sup>31</sup>	Value
Base						
Profile						
Version		<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumbe	er	<b>√</b>	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	<b>√</b>	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	
	countryName	✓			S	LU
	commonName	<b>√</b>			S	LuxTrust <b>Global Qualified</b> CA x <sup>32</sup>
	organizationName	✓			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
						Months;
						Certificate generation process date/time + 1
						day for PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO

 $<sup>^{28}</sup>$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>32\</sup> X$  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.



 $<sup>^{29}</sup>$  CE = Critical Extension.

 $<sup>^{30}</sup>$  O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>31</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.





	LuxTrust eID SSC	D LCP I		tion Si	gnatı	ıre Certificate Profile
Attribute	Field	$IN^{28}$	CE <sup>29</sup>	<b>O/M</b> <sup>30</sup>	<b>CO</b> <sup>31</sup>	Value
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s)
	givenName	<b>√</b>		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x as 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	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli	cKeyInfo	<b>√</b>	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit
	subjectPublicKey	<b>✓</b>		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	rldentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInfo	Access	<b>√</b>	False			
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>✓</b>				Id-ad-1
	accessLocation	<b>✓</b>				http://ocsp.luxtrust.lu
cRLDistribut	ionPoint	<b>✓</b>	False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						
subjectAltNa	T	<b>√</b>	False			
	Rfc822Name	<b>\</b>		0	D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo	dentifier	✓	False			
<u> </u>	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	<b>√</b>			S	False
		l		l		





LUXTUUST

VFRSION 12:

	LuxTrust eID SSCD LCP Integration Signature Certificate Profile									
Attribute	Field	IN <sup>28</sup>	<b>CE</b> <sup>29</sup>	<b>O/M</b> <sup>30</sup>	<b>co</b> <sup>31</sup>	Value				
	nonRepudiation	<b>✓</b>			S	True				
	keyEncipherment	<b>√</b>			S	False				
	dataEncipherment	<b>√</b>			S	False				
certificatePo	olicies	<b>√</b>	False							
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.16				
	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)				
	noticeNumbers									
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on				
						eID SSCD compliant with ETSI TS 102 042				
						LCP certificate policy. Key Generation by CSP.				
						Sole Authorised Usage: Electronic signature				
						for Integration Purposes.				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCe	rtificateStat									
	QcCompliance	<b>✓</b>		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance				
						with [5]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance				
						with [5]				
	QcSSCD	<b>√</b>		М	D	Set				

# 3.3.18 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.







VFRSION 1 21

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

	LuxTrust eID	SSCD	LCP I	ntgratio	n AE C	Certificate Profile
Attribute	Field	$IN^{18}$	<b>CE</b> <sup>19</sup>	O/M <sup>20</sup>	<b>CO</b> <sup>21</sup>	Value
Base Profile						
Version		<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumber	•	✓	False			
					FDV	Validated on duplicates.
signatureAlgo	orithm	<b>√</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValu	ie .	✓	False			
					D	Issuing CA Signature.
issuer	1	<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>22</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	T	<b>✓</b>	False			
	NotBefore	<b>∨</b> ✓			D	Certificate generation process date/time.
	NotAfter	•			D	Certificate generation process date/time + 12
						Months;
						Certificate generation process date/time + 1
		<b>✓</b>	F-1			day for PSEUDONYM Certificate
subject			False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and
				141		surname(s)
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x provided by the RNCID
	countryName	✓		М	D	LU
						specimen-x Subject's email address as
	emailAddress	<b>√</b>		0	D	provided by the RNCID
	title	<b>√</b>		М	D	"Private Person"
	organizationalUnitName 1	<b>√</b>		0	D	If the holder is underage: "Mineur jusqu'à : " &
	organizational Official H				U	(Date of birth + 18 years).
subjectPublic	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit
	subjectPublicKey	<b>√</b>		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKeylo	dentifier	✓	False			







VFRSION 12:

	LuxTrust eI	D SSCD		ntgratio	n AE C	ertificate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	<b>O/M</b> <sup>20</sup>	<b>co</b> <sup>21</sup>	Value
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified
						CA x public key
authorityInfoAccess		<b>√</b>	False			
	AccessMethod	<b>√</b>				ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
cRLDistribution	onPoint	<b>√</b>	False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNar	ne	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	specimen-x Subject's email address a
						provided by the RNCID
subjectKeylde	entifier	<b>√</b>	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit fiel
						with a 0100 value, followed by the least
						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		<b>√</b>	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	<b>✓</b>			S	True
	dataEncipherment	✓			S	True
certificatePoli	icies	<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	<b>√</b>			S	Id-qt-2 (User Notice)
	noticeNumbers					,
	DisplayText	<b>✓</b>				LuxTrust INTEGRATION CERTIFICATE o
	P					eID SSCD compliant with ETSI TS 102 04
						LCP certificate policy. Key Generation b
						CSP. Sole Authorised Usage: Authentication
						and Encryption for Integration Purposes







#### 3.3.19 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 (	Certi	ficate	Profil	e for	Mass Signature Services
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	Validated on duplicates.
signatureAlgorithm		<b>√</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" -
						SHA256 with RSA Encryption
signatureValue		<b>√</b>	False			
					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust <b>Global Qualified</b> CA x <sup>22</sup>
	organizationName	<b>√</b>			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		<b>√</b>	False			
	commonName	<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)
	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







LuxTrust non	SSCD NCP+ Public (	Certi	ficate	Profil	e for	Mass Signature Services
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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		✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	<b>✓</b>		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyIdentifier		<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/LTGQCAx <sup>22</sup> .crt
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		<b>✓</b>	False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						
subjectAltName		<b>✓</b>	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKeyldentifier		<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		<b>✓</b>	True			
	digitalSignature	<b>√</b>			S	True
	nonRepudiation				S	True





**L**LUXTUUST

VFRSION 12:

LuxTrust non	SSCD NCP+ Public	Certi	ficate	Profil	e for	Mass Signature Services
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>✓</b>			S	False
certificatePolicies		✓	False			
	Policyldentifier	<b>√</b>				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)
	noticeNumbers					
	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 seal signature services. GTC. CP and CPS on
	Policyldentifier	<b>✓</b>				http://repository.luxtrust.lu.  0.4.0.2042.1.2

# 3.3.20 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 SSCD, 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>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"					
SerialNumbe	ər	<b>√</b>	False								
					FDV	Validated on duplicates.					
signatureAlg	orithm	✓	False								







	LuxTrust					e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA25
						with RSA Encryption.
signatureVa	ilue	<b>√</b>	False			
					D	Issuing CA Signature.
issuer		<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust <b>SSL</b> CA x <sup>22</sup>
	organizationName	✓ ✓			S	LuxTrust S.A.
Validity			False			
	NotBefore	<b>V</b>			D	Certificate generation process date/time.
	NotAfter	Ý			D	Certificate generation process date/time 12;24;36 Months
subject		✓	False			
	countryName	<b>*</b>		М	D	Country in which the company's constitution's registered office is established (as specified in the memorandum an articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	<b>✓</b>		М	D	Location in which the company registered office is established (a specified in the memorandum and article of association or an equivalent document
	organizationName	<b>V</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	<b>√</b>		0	D	As provided by Subscriber
	organizationalUnitName2	<b>✓</b>		0	D	As provided by Subscriber
	commonName	~		М	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or IP address or uniquename of server.
	serialNumber	<b>√</b>		0	D	Serial Number as provided by subscriber
	emailAddress	~		0	D	Subject's email address
subjectPubl	icKeyInfo	<b>✓</b>	False			
,	algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	<b>✓</b>		М		public exponent: Fermat-4 (=010001).
Extensions	,					
Authority						
Properties						
authorityKey	yldentifier	✓	False			







	LuxTrust	SSL S	erver L	.CP Cer	tificat	te Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust SSL CA
						public key
authorityInfo	Access	<b>√</b>	False			
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>√</b>				http://ssl.ocsp.luxtrust.lu <sup>33</sup>
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx <sup>22</sup> .crt
cRLDistribut	tionPoint	✓	False			
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	<b>✓</b>		0	D	Certificate Holder's email address
	Subject Althorne dNSName			0		FQDN (Fully Qualified Domain Name) of
	SubjectAltName-dNSName					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
	SubjectAllivarile-unSivarile					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
	Oubject-itivame-divorvame					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
		<b>✓</b>				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
		<b>✓</b>				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
		<b>✓</b>				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.

<sup>33</sup> Since SSL CA 2







	LuxTrust	SSL Se	erver l	.CP Cer	tificat	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</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-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	✓		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.







	LuxTrust SSL Server LCP Certificate Profile										
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value					
	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 o unique name of server.					
	SubjectAltName-URL			0		FQDN (Fully Qualified Domain Name) o					
		<b>✓</b>				application/server – Exact and full second URL for a Web Server or IP address of unique name of server.					
subjectKeyl	dentifier	<b>✓</b>	False								
	keyldentifier	<b>V</b>			Fixed	The Key Identifier comprises a four-bifield 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	<b>√</b>			S	True					
	nonRepudiation	<b>~</b>			S	False					
	keyEncipherment	<b>~</b>			S	True					
	dataEncipherment	<b>√</b>			S	True					
certificatePo	plicies	<b>√</b>	False								
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.5.1					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu					
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	<b>*</b>				LuxTrust Standard SSL/TLS Server Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on http://repository.luxtrust.lu. Signed by a SSL CA.					
	Policyldentifier	<b>√</b>				0.4.0.2042.1.3					
Extended K	ey Usage	<b>√</b>	False								
	serverAuth	✓			S	True					
	clientAuth	✓			S	True					
	emailProtection	✓			S	True					
Netscape Proprietary											
Netscape C	ertificate Type	<b>√</b>	False								
	SSL Client	✓			S	Set					





LuxTrust Global Root CA Certificate Specifications

VERSION 1 21

LuxTrust SSL Server LCP Certificate Profile									
Attribute	Field IN <sup>18</sup> CE <sup>19</sup> O/M <sup>20</sup> CO <sup>21</sup> Value								
	SSL Server	✓			S	Set			
	S/MIME	✓			S	Set			

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

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

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

#### Prohibited Certificate uses:

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

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

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







Verification of Applicant's Legal Existence and Identity:

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

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

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

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

	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <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	Validated on duplicates.				
signatureAlgo	rithm	<b>✓</b>	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" -				
						SHA256 with RSA Encryption.				
signatureValu	е	<b>√</b>	False							
					D	Issuing CA Signature.				
issuer		<b>√</b>	False		S					
	countryName	✓			S	LU				
	commonName	<b>√</b>			S	LuxTrust <b>SSL</b> CA x <sup>22</sup>				
	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		✓	False							







	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value				
	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)				
	jurisdictionOfIncorporationCount ryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	<b>√</b>		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)				
	jurisdisctionOfIncorporationState OrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	<b>√</b>		0	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,				
	localityName (2.5.4.7)	✓		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)				
	jurisdictionOfIncorporationLocalit yName (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>		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.				







	SSL/TLS Exten	ded V	alidati	on Ser	ver C	ertificates
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	businessCategory (OID: 2.5.4.15)	<b>√</b>		M	D	Depending on the Subject qualifications, this field contains one of the following String:  Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	<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)	<b>√</b>		0	D	Postal code of the subject place of business.
	streedAddress (OID: 2.5.4.9)	<b>√</b>		0	D	Number and Street of the physical location of the subject
subjectPublic	KeyInfo	<b>√</b>	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	<b>√</b>		M		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKeyl	dentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfoA	Access	<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://ssl.ocsp.luxtrust.lu 33
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx <sup>22</sup> .crt





	SSL/TLS Exte	nded V	alidati	on Ser	ver C	ertificates
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
cRLDistribution	pnPoint	<b>✓</b>	False			
	distributionPoint	<b>✓</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNar	ne	<b>√</b>	False			
	SubjectAltName-dNSName			М		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		✓				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		✓				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		✓				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		<b>~</b>				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
	0.11 (4/01 :::2::			_		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.





	SSL/TLS Exten	ded V	alidati	on Ser	ver C	ertificates
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		✓				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		✓				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server - Exact DNS for a
						Web Server or IP address or unique
		<b>✓</b>				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
		<b>✓</b>				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
		<b>✓</b>				name of server, owned or controlled by
						the subject and to be associated with the
						Subject's server. Wildcard name not
		<b>√</b>				allowed for EV SSL Certificates.
subjectKeyIde		<b>V</b> ✓	False		F2	The Key Idea/Sey areas 2
	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						number of unused bit-stilly bits).
Properties						
keyUsage		<b>√</b>	True			
,	digitalSignature	<b>√</b>			S	True
	J				_	-
		<u> </u>	L	<u> </u>		





**L**LUXTUUST

VFRSION 12:

	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value				
	nonRepudiation	<b>√</b>			S	False				
	keyEncipherment	✓			S	True				
		<b>✓</b>								
	dataEncipherment	<b>,</b>			S	True				
		<b>✓</b>								
certificatePoli	1	· ·	False							
	Policyldentifier					1.3.171.1.1.10.5.2				
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)				
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>✓</b>				ETSI TS 102 042 EVCP compliant				
						certificate signed by a SSL CA. Key				
						generation by the Subscriber.				
						Certificates intended to be used for				
						authenticating servers accessible				
						through the Internet.				
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.4				
Extended Key	/ Usage	<b>√</b>	False							
	serverAuth	✓			S	True				
	clientAuth	✓			S	True				
	emailProtection	✓			S	False				

# 3.3.22 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 Secure User Device, with creation of the keys by the Subscriber, with 2048-bit key size and one (1) or two (2) years validity from issuing start date.

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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







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

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

#### Prohibited Certificate uses:

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.

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

# SSL/TLS Extended Validation Server Certificates on Secure User Device





# **LuxTrust Global Root CA Certificate Specifications**

Base Profile       Version     ✓ False       SerialNumber     ✓ False		
Version Faise		
SerialNumber False		
SerialNumber False	S Version	on 3 Value = "2"
- F	DV Valida	ated on duplicates.
signatureAlgorithm		·
algorithm	S OID	= "1.2.840.113549.1.1.11" -
	SHA2	256 with RSA Encryption.
signatureValue ✓ False		· · · · · · · · · · · · · · · · · · ·
	D Issuin	ng CA Signature.
issuer   √ False	S	
countryName	S LU	
commonName		rust <b>SSL</b> CA x <sup>22</sup>
organizationName		rust S.A.
Validity ✓ False	Luxii	
NotBefore 1 dise	D Certifi	icate generation process
Notbelore	date/t	
NotAfter	D Certifi	
subject False	uate/t	time + 12;24 Months
1		
countryName		try in which the company's or
(OID: 2.5.4.6)		ution's registered office is
		olished (as specified in the
		orandum and articles of
	assoc	ciation). (ISO3166)
jurisdictionOfIncorporationCountryNa M	D Conta	ains the country information
me	specif	fied using the applicable ISO
(OID: 1.3.6.1.4.1.311.60.2.1.3)	count	try code for the jurisdiction of
	Incorp	poration for the Incorporating
	Agend	cy or Jurisdiction of
	Regis	stration for a Registration
	Agend	cy that operates at the country
	level,	at state/pr.
stateOrProvinceName M	D State	or Province in which the
	compa	
(OID: 2.5.4.8)		olished (as specified in the
		orandum and articles of
		ciation or an equivalent
	docun	
jurisdisctionOfIncorporationStateOrPro O		ains the jurisdiction for the
vinceName		cable Incorporating Agency or
(OID: 1.3.6.1.4.1.311.60.2.1.2)	_	stration Agency at the state or
	·	nce level MUST include both
		try and state or province
	inform	nation,





# **LuxTrust Global Root CA Certificate Specifications**

SS	L/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	localityName (2.5.4.7)	<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)
	jurisdictionOfIncorporationLocalityNam e (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





SSI	L/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	serialNumber			М	D	See EV Guidelines [13] :
	(OID: 2.5.4.5)	✓				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	<b>✓</b>		0	D	is a Government Entity.  Postal code of the subject place of business.
	(OID: 2.5.4.17) streedAddress	<b>✓</b>		0	D	Number and Street of the physical
	(OID: 2.5.4.9)					location of the subject
subjectPublic	KeyInfo	<b>√</b>	False			
	algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyl	dentifier	<b>V</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfoA	Access	<b>V</b>	False			
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://ssl.ocsp.luxtrust.lu 33
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTSSLCAx <sup>22</sup> .crt
cRLDistribution	T	✓ ✓	False		_	
	distributionPoint	<b>✓</b>			S	
	fullName	•				http://crl.luxtrust.lu/LTSSLCAx <sup>22</sup> .crl







	L/TLS Extended Validation					
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Subject						
Properties						
subjectAltNa			False			50011 (5.11 0.115 1.5
	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 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>V</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	✓		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.





SSI	L/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</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
	SubjectAltName-dNSName	<b>√</b>		0		EVCP+ Certificates.  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.
subjectKeyld	SubjectAltName-dNSName	✓ <b>✓</b>	False	Ο		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.







VFRSION 12

SSL	_/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</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	,	<b>√</b>	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	<b>√</b>			S	True
		<b>✓</b>				
certificatePoli	T	<b>✓</b>	False			
	Policyldentifier	<b>∨</b>				1.3.171.1.1.10.5.3
	policyQualifierID				S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				ETSI TS 102 042 EVCP+ compliant
						certificate signed by a SSL CA. Key
						generation by the Subscriber on
						Secure Device. Intended to be used
						for authenticating servers accessible
		<b>/</b>				through the Internet.
	Policyldentifier					0.4.0.2042.1.5
Extended Key	/ Usage	<b>✓</b>	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False

# 3.3.23 LuxTrust Object (or Code) Signing Certificates

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

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

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., <1.3.171.1.1.10.5.4>.







VFRSION 1 21

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

	Lu	xTrust L	.CP Code	Signing	Certificate	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Base Profil	ө					
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	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>SSL</b> CA x <sup>22</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; 24; 36 months
subject		✓	False			
	countryName	<b>~</b>		М	D	Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	✓		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	<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







	Lu	xTrust L	.CP Code	Signing	Certificat	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	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 of an equivalent document)
	serialNumber	✓		0	D	NA or Serial Number as provided by subscriber
	emailAddress	✓		0	D	Subject's email address if available
subjectPub	olicKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority P	roperties					
authorityKe	eyldentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInf	foAccess	✓	False			
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 33
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx <sup>22</sup> .crt
CRLDistrib	utionPoint	✓	False			
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx <sup>22</sup> .crl
Subject Pro	operties					
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Subject's email address
subjectKey	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 Prop	perties					





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

VFRSION 1 21

	Lu	xTrust L	CP Code	Signing (	Certificat	e Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>✓</b>			S	False
certificateF	Policies	✓	False			
	Policyldentifier	<b>✓</b>			S	1.3.171.1.1.10.5.4
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	<b>✓</b>			S	http://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			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 I	Key Usage	✓	False			
	Object Signing	✓			S	Set
Netscape F	Proprietary					
NetscapeC	ertificateType	✓	False			
	Object Signing	✓			S	Set

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

LuxTrust SSL/TLS Client Certificates are ETSI TS 102 042 LCP Certificates not certified as generated on SSCD, 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., <1.3.171.1.1.1.0.5.5>.

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

	LuxTrust SSL Client LCP Certificate Profile								
Attribute	Attribute Field IN <sup>18</sup> CE <sup>19</sup> O/M <sup>20</sup> CO <sup>21</sup> Value								







LuxTrust SSL Client 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		<b>✓</b>	False			
					S	Version 3 Value = "2"
SerialNumbe	er T	✓	False			
		<b> </b>			FDV	Validated on duplicates.
signatureAlg		•	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	lue	<b>✓</b>	False			with NOA Encryption.
oigi latai e v ai			1 0100		D	Issuing CA Signature.
issuer		<b>✓</b>	False		S	issuing of Colgridation
	countryName	<b>✓</b>			S	LU
	commonName	<b>✓</b>			S	LuxTrust <b>SSL</b> CA
	organizationName	<b>✓</b>			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; 36 Months
subject		<b>✓</b>	False			
	countryName			М	D	Country in which the company's or
		<b>✓</b>				institution's registered office is established
						(as specified in the memorandum and
						articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName			М	D	Location in which the company's
		<b>✓</b>				registered office is established (as
						specified in the memorandum and articles
						of association or an equivalent document)
	organizationName			М	D	Names as in articles of association,
						including the legal form (as specified in the
		<b>✓</b>				memorandum and articles of association
						or an equivalent document)
	organizationalUnitName 1			0	D	As provided by Subscriber
	0.94	✓				, to provided by edisconies.
	organization all Inith I are a C	<b>✓</b>				As provided by Cubscalles
	organizationalUnitName 2			0	D	As provided by Subscriber
	commonName	<b>✓</b>		M	D	As provided by Subscriber
	serialNumber	✓		0	D	Serial Number as provided by subscriber
	emailAddress	✓		0	D	Subject's email address
subjectPublic	l cKeyInfo	<b>✓</b>	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);







LuxTrust SSL Client LCP Certificate Profile						
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust SSL C
						public key
authorityInfo	Access	<b>√</b>	False			
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 33
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx <sup>22</sup> .crt
cRLDistribut	tionPoint	✓	False			
	distributionPoint	<b>✓</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx <sup>22</sup> .crl
Subject						
Properties						
subjectAltNa	ame	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
11 414 1	1 45	· ·				
subjectKeyIdentifier			False			
	keyldentifier				Fixed	The Key Identifier comprises a four-b
						field with a 0100 value, followed by th
						least significant 60 bits of the SHA-1 has
						of the value or subjectPublicKey bit strin
						(tag, not including the length and number
						of unused bit-string bits).
Policy						
Properties		<b>✓</b>	_			
keyUsage	1		True		_	
	digitalSignature				S	True
		<b>✓</b>				 
	nonRepudiation				S	False
		<b>✓</b>				_
	keyEncipherment				S	True
		<b>✓</b>				_
	dataEncipherment				S	True
andiffert D		<b>✓</b>	Fals:			
certificatePo		· ·	False			4 0 474 4 4 4 0 5 5
	PolicyIdentifier	· ·		1	_	1.3.171.1.1.10.5.5
	policyQualifierID				S	Id-qt-1 (CPS)
	qualifier	<b>V</b>			S	https://repository.luxtrust.lu
	policyQualifierID	· ·			S	Id-qt-2 (User Notice)
	noticeNumbers					







VFRSION 1 21

LuxTrust SSL Client LCP Certificate Profile						
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	DisplayText	<b>✓</b>				LuxTrust Standard SSL/TLS Client
						Authentication Certificate. Not supported
						by SSCD, Key Generation by Subscriber.
						GTC, CP and CPS on
						http://repository.luxtrust.lu.
						Signed by a SSL CA.
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.3
Extended Ke	Extended Key Usage		False			
	serverAuth	✓			S	False
	clientAuth	✓			S	True
	emailProtection	✓			S	True

# 3.3.25 Timestamping Certificate Profile

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

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 [6]. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

	LuxTrust Timestamping 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			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	signatureAlgorithm		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>Global Timestamping</b> CA x <sup>22</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	Validity		False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						60 Months
subject	subject		False			







field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string		LuxTrust Timestamping Certificate Profile					
	Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
OrganizationName		commonName	<b>√</b>		М	D	tts.luxtrust.lu
OrganizationalUnitName 1		localityName	✓		М	D	Capellen
CountryName		organizationName	<b>✓</b>		М	D	LuxTrust S.A.
subject/Public KeyIrfo		organizationalUnitName 1	<b>√</b>		М	D	PKI Entity
Algorithm		countryName	<b>√</b>		0	D	LU
Authority	subjectPublic	⊥ cKevInfo	<b>√</b>	False			
Subject   Sub		-	<b>✓</b>				Public Kev: Kev length: 2048 bit (RSA):
Extensions   Authority   Properties			<b>✓</b>		М		
Authority Properties authoritykeyld-entifier   Keyldentifier	Extensions	Subject ability			141		pablic experience remact r ( e recer).
Properties							
Reyldentifier   False   SHA-1 Hash of the LuxTrust   Timestamping CA public key							
authorityInfolacess  AccessMethod AccessMet	authorityKey	ldentifier	✓	False			
AccessMethod accessLocation  AccessMethod accessLocation  CRLDistributionPoint  AccessMethod accessLocation  CRLDistributionPoint  AccessMethod Antiplication Antiplication AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod AccessMethod Antiplication Antiplication AccessMethod AccessMethod Antiplication Antiplication AccessMethod AccessMethod Antiplication Antiplication Antiplication AccessMethod AccessMethod Antiplication Antiplication Antiplication AccessMethod AccessMethod Antiplication Antiplication Antiplication AccessMethod AccessMethod AccessMethod Antiplication Antiplication AccessMethod AccessMethod AccessMethod AccessMethod		keyldentifier	<b>\</b>				
AccessMethod	authorityInfo	Access	✓	False			
AccessMethod   AccessMethod   AccessMethod   AccessLocation   AccessMethod   AccessLocation   AccessLocati		AccessMethod	✓				Id-ad-2
Accessive mode		accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGTSACAx <sup>22</sup> .crt
cRLDistributionPoint  distributionPoint  fullName  V		AccessMethod	<b>√</b>				Id-ad-1
distributionPoint   Faise		accessLocation	<b>√</b>				http://ocsp.luxtrust.lu
Subject   Properties   Subject   S	cRLDistributionPoint		✓	False			
Subject Properties SubjectAltName		distributionPoint	<b>√</b>			S	
Properties         subjectAltName       ✓       False       Image: Control of the properties         Rfc822Name       ✓       False       Image: Control of the properties       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         ReyUsage       ✓       True         digitalSignature nonRepudiation       ✓       S       True         keyEncipherment       ✓       S       False         Extended Key Usage       ✓       False         TimeStamping (1.3.6.1.5.5.7.3.8)       ✓       False		fullName	✓				http://crl.luxtrust.lu/LTGTSACAx <sup>22</sup> .crl
Rfc822Name	_						
subjectKeyIdentifier    KeyIdentifier   False   Fixed   The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).    Policy   Properties	subjectAltNa	me	✓	False			
Reyldentifier   Fixed   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	<del>_</del>	Rfc822Name	✓		0	D	info@luxtrust.lu
Reyidentifier    Fixed   The Rey 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	subjectKeyld	lentifier	✓	False			
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		keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit
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							
Continuing the length and number of unused bit-string bits).    Policy   Properties   Properti							least significant 60 bits of the SHA-1 hash
Policy Properties  keyUsage  digitalSignature nonRepudiation keyEncipherment dataEncipherment  TimeStamping (1.3.6.1.5.5.7.3.8)  of unused bit-string bits).  True  S False  False  S False  S False  S False  S S False  S S Set							of the value or subjectPublicKey bit string
Policy Properties  keyUsage  digitalSignature nonRepudiation keyEncipherment dataEncipherment  TimeStamping (1.3.6.1.5.5.7.3.8)  True  S True S True S False False False S False S False S False S False S False							(tag, not including the length and number
keyUsage         ✓         True         ✓           digitalSignature         ✓         S         True           nonRepudiation         ✓         S         False           keyEncipherment         ✓         S         False           dataEncipherment         ✓         S         False           Extended Key Usage         ✓         False           TimeStamping (1.3.6.1.5.5.7.3.8)         ✓         S         Set							of unused bit-string bits).
keyUsage         True         True           digitalSignature         S         True           nonRepudiation         S         False           keyEncipherment         S         False           dataEncipherment         S         False           Extended Key Usage         False           TimeStamping (1.3.6.1.5.5.7.3.8)         S         Set	Policy						
digitalSignature							
Control of the cont	keyUsage			True			
NonRepudiation   S   False						S	True
ReyEncipherment   S Faise     dataEncipherment   V S Faise     Extended Key Usage   Faise     TimeStamping   S Set     (1.3.6.1.5.5.7.3.8)   S Set		nonRepudiation				S	False
Extended Key Usage  TimeStamping (1.3.6.1.5.5.7.3.8)  False  S False		keyEncipherment				S	False
TimeStamping   S   Set		dataEncipherment				S	False
(1.3.6.1.5.5.7.3.8)	Extended Ke	ey Usage		False			
			<b>√</b>			S	Set
	Private Kev I		✓	False			







VFRSION 1 21

	LuxTrust Timestamping Certificate Profile					
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	Usage period (2.5.29.16)	<b>✓</b>		М	D	Certificate generation process date/time +
						12 Months
certificatePol	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.8.1
	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)
	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	<b>✓</b>				0.4.0.2042.1.3

#### 3.3.26 Certificate extensions

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

#### 3.3.27 Algorithm object identifiers

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

# 3.3.28 Name forms

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

### 3.3.29 Name constraints

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

# 3.3.30 Certificate policy object identifier

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

# 3.3.31 Usage of Policy Constraints extension

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

#### 3.3.32 Policy qualifiers syntax and semantics

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

#### 3.3.33 Processing semantics for the critical Certificate Policies

Not applicable.

# 3.4 CRL profile

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

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







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

LuxTrust CRL Profile							
Field	Comments						
Version	v2						
Signature	Sha1RSA						
Issuer	<subjectca></subjectca>						
thisUpdate	<creation time=""></creation>						
nextUpdate	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""></creation></pre>						
	<creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" p="" subordinate<="" time=""></creation>						
	Qualified and 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	<pre><insert code="" list="" of="" reason="" revocation="" used=""></insert></pre>						
crlExtensions							
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>						
authorityKeyldentifier	Non-critical <ca assigned="" number="" unique=""></ca>						

# 3.4.1 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.

#### 3.4.2 CRL entry extensions

See section 3.4.

# 3.5 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported. The LuxTrust CAs support signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA.

# 3.5.1 Version number(s)

See section 3.5.

# 3.5.2 OCSP extensions

See section 3.5.

