

Version number: 1.24

Publication Date: 15/06/2017 Effective Date: 01/07/2017



VERSION 1 24

Document Information

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

Version History

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





VFRSION 1 24

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
1.22	YNU	03/11/2015	Update Common Names in non SSL certificates
			Remove NetscapeCertType extension from SSL and Object Signing
			Certificates
			Added: OCSP signing Certificate which contains an extension of type id-pkix-
			ocsp-nocheck, as defined by RFC2560
1.23	YNU	05/08/2016	Add Timestamping Profile under Global Qualified CA
4.01	DE:	40/00/00:=	Update Signing Server LCP Certificate profil
1.24	DEL	12/06/2017	Add:
			LuxTrust Qualified Timestamping Certificate profile with QC
			statements
			SPARE LuxTrust Signing Server LCP Certificate Profile Out 15 at 12 decreased a 2 and a set 15 and a set
			Qualified/Advanced eSeal certificate profiles
			elDAS qualified certificate profiles
			 Signing Server Signature and eSeal certificates and QWAC certificate and signing stick certificates









Table of content

DOCUME	INT INFORMATION	2
VERSION	N HISTORY	2
TABLE O	F CONTENT	4
INTELLE	CTUAL PROPERTY RIGHTS	6
REFERE	NCES	7
INTRODU	JCTION	9
1.1	THE LUXTRUST PROJECT	9
1.2	GOAL OF THE LUXTRUST PKI	9
1.3	LuxTrust PKI Hierarchy	9
2	LUXTRUST CERTIFICATION AUTHORITIES	10
2.1	Two-level CA hierarchy	10
3	CERTIFICATE AND CRL PROFILES	12
3.1	CERTIFICATE TYPES	12
3.2	LuxTrust Certification Authorities – Certificates profiles	26
3.3	LuxTrust Global Root CA	26
3.4	LuxTrust Global Qualified CA	27
3.4.1	LuxTrust SSL CA	28
3.4.2	LuxTrust TSA (Timestamping) CA	30
3.4.3	Certificate extensions	31
3.4.4	Algorithm object identifiers	31
3.4.5	Name forms	31
3.4.6	Name constraints	31
3.4.7	Certificate policy object identifier	31
3.4.8	Usage of Policy Constraints extension	
3.4.9	Policy qualifiers syntax and semantics	
3.5	LuxTrust End-entity – Certificates profiles	
3.5.1	Certificate profiles	
3.5.2	Version number(s)	
3.5.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	
3.5.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	
3.5.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	
3.5.6 3.5.7	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	
3.5.7 3.5.8	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption LuxTrust NCP+ Certificates supporting Mass Signature Services	
3.5.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	
3.5.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	
3.5.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for in	
5.5.77	purposes	
<i>3.5.12</i>	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	
3.5.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	
3.5.14	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures	
3.5.15	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures	66



3.5.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	68
3.5.17	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures	71
3.5.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	74
3.5.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	<i>76</i>
3.5.20	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature,	Authentication &
	Encryption	79
3.5.21	SSL/TLS Extended Validation Server Certificates - EVCP certificates supporting Signature,	Authentication &
	Encryption	83
3.5.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature,	Authentication &
	Encryption	90
<i>3.5.23</i>	LuxTrust Object (or Code) Signing Certificates	97
3.5.24	LuxTrust SSL/TLS Certificate for Client Authentication	99
<i>3.5.25</i>	SSL/TLS QCP-w Extended Validation Server Certificates	102
3.5.26	LuxTrust SPARE Signing Server LCP Certificate Profile	107
3.5.27	LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature	110
3.5.28	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	114
3.5.29	LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature	117
3.5.30	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	120
3.5.31	LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature	123
3.5.32	LuxTrust Smart Card QCP-n-qscd Certificate Profile	127
3.5.33	LuxTrust Smart Card NCP+ Certificate Profile	130
3.5.34	LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature	132
<i>3.5.35</i>	LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purp	poses135
<i>3.5.36</i>	QCP-n-qscd supporting Qualified Electronic Signature for elD smart cards	
<i>3.5.37</i>	NCP+ supporting Authentication & Encryption for eID smart cards	139
<i>3.5.38</i>	LuxTrust Signing Server QCP-n-qscd Certificate Profile	
3.5.39	LuxTrust Signing Server QCP-l-qscd Certificate Profile	144
3.5.40	LuxTrust Signing Stick QCP-n-qscd certificate profile	
3.5.41	LuxTrust Signing Stick NCP+ Certificate Profile	151
3.6	TIMESTAMPING CERTIFICATE PROFILE	154
3.6.1	Normalized Certificate Policy for LuxTrust Qualified Timestamping	
3.6.2	Qualified Timestamping Certificate Profile	157
3.6.3	TimeStamp Request and Response Format	
3.7	CERTIFICATE EXTENSIONS	161
3.8	ALGORITHM OBJECT IDENTIFIERS	
3.9	Name forms	161
3.10	Name constraints	162
3.11	CERTIFICATE POLICY OBJECT IDENTIFIER	
3.12	Usage of Policy Constraints extension	162
3.13	POLICY QUALIFIERS SYNTAX AND SEMANTICS	
3.14	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES	162
3.15	CRL PROFILE	
3.15.1	Version number(s)	
<i>3.15.2</i>	CRL entry extensions	
3.16	OCSP PROFILE	
3.16.1	Version number(s)	
3.16.2	OCSP extensions	163





VFRSION 1 24

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] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- [6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 1 i juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [10] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [11] LuxTrust Time Stamping Policy, latest version in force.
- [12] Guidelines for the Issuance and Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.
- [13] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force
- [14] eID Certificate Life Cycle Procedure latest version in force
- [15] RNCID: National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16
- [16] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [17] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [18] Loi du 19 juin 2013 Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques
- [19] EN 319 411 1 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [20] EN 319 411 2 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- [21] According to EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)



VFRSION 1 24

- [22] According to EN 319 422 V1.1.1, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (2016-03)
- [23] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)
- [24] According to EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)
- [25] According to EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)
- [26] According to EN 319 412-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (2016-02)
- [27] According to EN 319 412-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)
- [28] According to EN 319 412-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)
- [29] According to EN 319 412-4 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (2016-02)
- [30] According to EN 319 412-5 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements (2016-02)
- [31] eIDAS regulation: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG



VERSION 1.24



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 center for Luxembourg. LuxTrust as TTP especially focuses on providing support for any existing business needs in terms of security and also promotes new "e-business" and "e-government" opportunities, making the best possible use of existing legal and commercial assets which are unique to Luxembourg.

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

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

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

1.2 Goal of the LuxTrust PKI

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

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

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

1.3 LuxTrust PKI Hierarchy

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

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

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







VFRSION 1 24

2 <u>LuxTrust Certification Authorities</u>

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:
 - LuxTrust Global Qualified CA
 - LuxTrust SSL CA
 - LuxTrust Time Stamping Authority
- Additional CAs or CA hierarchies might be signed in the future under the LuxTrust Global Root CA

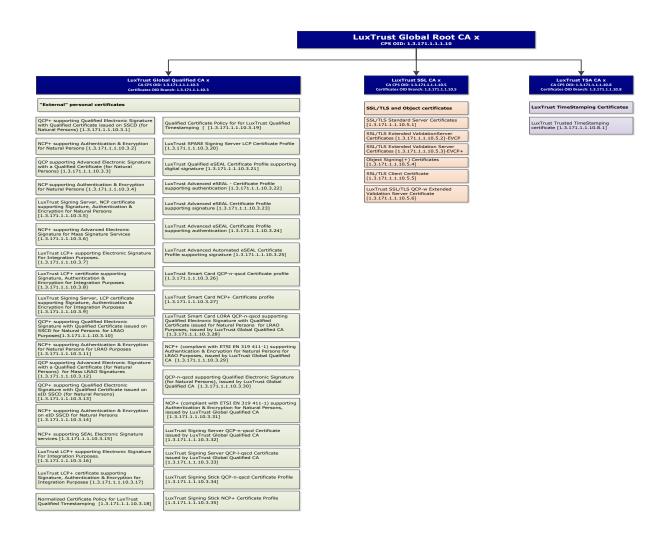
Subordinate CAs are operating within a grant of authority for issuing certificates under the LuxTrust CPS and the applicable CP. This grant has been provided by the "LuxTrust Global Root CA" (hereafter "LTGRCA") under the responsibility and authority of LuxTrust S.A. acting as CSP.

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

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



Figure 1- LuxTrust running CA Hierarchy



VFRSION 1 24

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 LuxTrust Global Root CA:

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





CP identification	CP OID	CPS OID	Short Description	Ref.
NCP supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.4	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.5	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption
NCP+ supporting Advanced Electronic Mass Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Mass Signature Services.	LuxTrust NCP+ Certificates supporting Mass Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.7	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures





CP identification	CP OID	CPS OID	Short Description	Ref.
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.8	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA QCP+ supporting Qualified Electronic Signature with Qualified Certificate	1.3.171.1.1.10.3.9	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048- bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for INTEGRATION PURPOSES. ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes LuxTrust Smartcard LORA Certificates
issued on SSCD for Natural Persons for LRAO Purposes issued by LuxTrust Global Qualified CA NCP+ supporting	4 2 474 4 4 40 2 44		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. ETSI TS 102 042 NCP+ compliant	supporting Signature for LRAO purposes
Authentication & Encryption for Natural Persons for LRAO Purposes issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.11	1.3.171.1.1.1.10.3	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.	Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes



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



CP identification	CP OID	CPS OID	Short Description	Ref.
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of authentication (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption
Normalized Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.18	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Normalized Certificate Policy for Qualified Timestamping
Qualified Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.19	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Qualified Certificate Policy for Qualified Timestamping
LuxTrust SPARE Signing Server LCP Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.20	1.3.171.1.1.1.10.3	LuxTrust SPARE Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy.	SPARE Signing Server LCP Certificate Profile
LuxTrust Qualified eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.21	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy.	Qualified eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSeal - Certificate Profile supporting authentication issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.22	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication





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





CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Smart Card LORA QCP-n-qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.28	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy, with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smart Card LORA QCP-n- qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes,
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.29	1.3.171.1.1.1.10.3	LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons for LRAO Purposes,
QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.30	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons),
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.31	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons,





CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Signing Server QCP-n-qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.32	1.3.171.1.1.1.10.3	Signing Server certificate for qualified signature	LuxTrust Signing Server QCP-n-qscd Certificate profile
LuxTrust Signing Server QCP-I-qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.33	1.3.171.1.1.1.10.3	Signing Server certificate for qualified eSeal	LuxTrust Signing Server QCP-I-qscd Certificate profile
LuxTrust Signing Stick QCP-n-qscd Certificate Profile	1.3.171.1.1.10.3.34	1.3.171.1.1.1.10.3	Signing Stick QCP-n-qscd Certificate Profile	Signing Stick QCP-n-qscd Certificate Profile
LuxTrust Signing Stick NCP+ Certificate Profile	1.3.171.1.1.10.3.35	1.3.171.1.1.1.10.3	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile
LuxTrust SSL Certification	on Authority			
SSL/TLS Standard Server Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	1.3.171.1.1.1.10.5	ETSI TS 102 042 LCP compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption
SSL/TLS(+) Extended Validation Server Certificates - EVCP issued by LuxTrust SSL CA	1.3.171.1.1.10.5.2	1.3.171.1.1.1.10.5	ETSI TS 102 042 EVCP compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentication & Encryption





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





VFRSION 1 24

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

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

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

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

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

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

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





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

Domain	Document category	Document		Sub-document – description	LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
1 LuxTrust PKI	LuxTrust Certificat	ion Practice Statements							
	1 CPS LuxTrust	1 CPS Summary GTE/Verizon Chain	0			x	у	1.3.171.1 .1.1.0.x.y	N/A
		2 Not Used		Not Used		-	-	not used	N/A
		10 CPS LuxTrust Global		LuxTrust Global Root CA		-	-	1.3.171.1 .1.1.10	N/A
		Root Chain	3	LuxTrust Global Qualified CA		-	-	1.3.171.1 .1.1.10.3	N/A
			5	LuxTrust SSL CA		-	-	1.3.171.1. 1.1.10.5	N/A
			8	LuxTrust Global Timestamping CA		-	-	1.3.171.1. 1.1.10.8	N/A
1 LuxTrust PKI	LuxTrust Certificat	te Policies							
	10 CP's LuxTrust	3 LuxTrust Global	1	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1. 1.10.3.1	0.4.0.1456.1.1
	Global Chain	Qualified CA Certificates	2	NCP+ supporting Authentication & Encryption for Natural Persons	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1. 1.10.3.2	0.4.0.2042.1.2
			3	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick PRI/PRO Signature Certificate	-	-	1.3.171.1. 1.10.3.3	0.4.0.1456.1.2
			4	NCP Authentication & Encryption	Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1. 1.10.3.4	0.4.0.2042.1.1
			5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1 .1.10.3.5	0.4.0.2042.1.1



6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-		1.3.171.1. 1.10.3.6	0.4.0.2042.1.1
7	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration SmartCard Signature Certificate	-	-	1.3.171.1. 1.10.3.7	0.4.0.2042.1.3
8	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration SmartCard Authentication Certificate	-		1.3.171.1.1.10.3.8	0.4.0.2042.1.3
9	LuxTrust LCP Certificates supporting Signature, Authentication & Encryption for integration purposes	Integration Signing Server Certificate	-		1.3.171.1 .1.10.3.9	0.4.0.2042.1.3
10	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons) for Natural Persons for LRAO Purposes	SmartCard LORA Signature Certificate	-	-	1.3.171.1. 1.10.3.10	0.4.0.1456.1.1
11	NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes	SmartCard LORA Authentication Certificate	-	-	1.3.171.1. 1.10.3.11	0.4.0.2042.1.2
12	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) for Mass LRAO Signatures	Mass LRAO Signature Certificate	-	-	1.3.171.1. 1.10.3.12	0.4.0.1456.1.2
13	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	eID SmartCard Signature Certificate	-	-	1.3.171.1. 1.10.3.13	0.4.0.1456.1.1
14	NCP+ supporting Authentication & Encryption for Natural Persons	eID SmartCard Authentication Certificate	-	-	1.3.171.1. 1.10.3.14	0.4.0.2042.1.2
15	NCP+ supporting Advanced Electronic Seal Signature Services	Seal Signature Services	-	-	1.3.171.1 .1.10.3.15	0.4.0.1456.1.2
16	LuxTrust LCP+ supporting Electronic Signature For Integration purposes.	Integration eID SmartCard Signature Certificate	-	-	1.3.171.1. 1.10.3.16	0.4.0.2042.1.3
17	LuxTrust LCP+ certificate supporting Signature, Authentication & Encryption for Integration purposes	Integration eID SmartCard Authentication Certificate	-	-	1.3.171.1. 1.10.3.17	0.4.0.2042.1.3
18	Normalized Certificate Policy for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1. 1.10.3.18	0.4.0.2042.1.2
19	Qualified Certificate Policy for for LuxTrust Qualified Timestamping	LuxTrust Qualified Timestamping	-	-	1.3.171.1. 1.10.3.19	0.4.0.194112.1.1
20	LuxTrust SPARE Signing Server LCP Certificate	LuxTrust SPARE Signing Server LCP Certificate	-	-	1.3.171.1 .1.10.3.20	0.4.0.2042.1.3



21	LuxTrust Qualified eSEAL Certificate supporting digital signature	LuxTrust Qualified eSeal	-	-	1.3.171.1. 1.10.3.21	0.4.0.194112.1.3
22	LuxTrust Advanced eSeal NCP+ Certificate for authentication	LuxTrust Qualified eSeal	-	-	1.3.171.1. 1.10.3.22	0.4.0.2042.1.2
23	LuxTrust Advanced eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.23	0.4.0.2042.1.2
24	LuxTrust Advanced eSEAL Certificate supporting authentication	LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.24	0.4.0.2042.1.2
25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. 1.10.3.25	0.4.0.2042.1.2
	La Tarat Orand Orand OOD a roand Orant Starte Burgle	SmartCard PRI/PRO			4 2 474 4 4 40 0 00	0.4.0.40440.4.0
26	LuxTrust Smart Card QCP-n-qscd Certificate Profile	Signature Certificate	-	-	1.3.171.1 .1.10.3.26	0.4.0.194112.1.2
27	Lux Trust Count Count NOD Contiferts Deefle	SmartCard PRI/PRO			1 2 474 4 4 40 2 27	0.4.0.2042.4.2
27	LuxTrust Smart Card NCP+ Certificate Profile	Authentication Certificate	-	-	1.3.171.1 .1.10.3.27	0.4.0.2042.1.2
28	LuxTrust Smart Card LORA NCP+ - Signature Certificate for	SmartCard LORA			1.3.171.1 .1.10.3.28	0.4.0.2042.1.2
20	LRAO Purposes	Signature Certificate		-	1.5.171.1.1.10.5.20	0.1.0.2012.1.2
00	LuxTrust Smart Card LORA NCP+ - authentication Certificate for	SmartCard LORA			4 2 474 4 4 40 0 00	0.4.0.0040.4.0
29	LRAO Purposes	Authentication Certificate	-	-	1.3.171.1.1.10.3.29	0.4.0.2042.1.2
	L T	eID SmartCard			40.474.4.40.000	0.4.0.40440.4.0
30	LuxTrust eID Smart Card QCP-n-qscd Certificate	Signature Certificate	-	-	1.3.171.1 .1.10.3.30	0.4.0.194112.1.2
0.4	La Tarata ID Guarda and NGD, Godffanta	eID SmartCard			4 2 474 4 4 40 0 04	0.4.0.0040.4.0
31	LuxTrust eID Smart card NCP+ Certificate	Authentication Certificate	1	-	1.3.171.1. 1.10.3.31	0.4.0.2042.1.2
32	LuxTrust Signing Server QCP-n-qscd Certificate	Signing Server certificate for qualified signature	-	-	1.3.171.1. 1.10.3.32	0.4.0.194112.1.2
33	LuxTrust Signing Server QCP-I-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1.1.10.3.33	0.4.0.194112.1.3
34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171. 1.1.10.3.34	0.4.0.194112.1.2
35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171. 1.1.10.3.35	0.4.0.2042.1.2





5 LuxTrust SSL CA	1	SSL/TLS Standard Server Certificates	SSL/TLS Standard Server Certificates	-		1.3.171.1 .1.10.5.1	0.4.0.2042.1.3
Certificates	2	SSL/TLS(+) Extended Validation Server Certificates – EVCP	SSL/TLS Extended Validation Server Certificates	-		1.3.171.1. 1.10.5.2	0.4.0.2042.1.4
	3	SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	-	-	1.3.171.1. 1.10.5.3	0.4.0.2042.1.5
	4	Object Signing(+) Certificates	Object Signing(+) Certificates	-	-	1.3.171.1. 1.10.5.4	0.4.0.2042.1.3
	5	SSL/TLS Client Certificate	SSL/TLS Client Certificate	-	-	1.3.171.1. 1.10.5.5	0.4.0.2042.1.3
	6	SSL/TLS QCP-w Extended Validation Server Certificates	SSL/TLS Qualified website authentication certificate	-	-	1.3.171.1. 1.10.5.6	0.4.0.194112.1.4
8 LuxTrust Global Timestamping CA Certificates	1	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate	-	-	1.3.171.1 .1.10.8.1	0.4.0.2042.1.3



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:

3.3 LuxTrust Global Root CA

	Lux	Trust Glo	obal Roo	t 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 ¹	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Root x ¹	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies ²	{id-ce 32}	Х	FALSE		
policyldentifier		х		1.3.171.1.1.10	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed

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

² Since LuxTrust Global Root 2







VFRSION 1 24

	Lux	Trust Glo	bal Roo	t CA	
Base Profile	OID	Included	Critical	Value	
Qualifier	CPSuri	×		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE ⁶		
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
Keyldentifier		Х		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
Keyldentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	Х	TRUE ⁶		
CA		Х		TRUE	Fixed
pathLenConstraint		×		None	Fixed

3.4 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 ¹	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
Subject								
CountryName	{ id-at-6 }	х		LU	Fixed			







VERSION 1.24

	LuxTr	ust Glob	al Qualif	ied CA	
Base Profile	OID	Included	Critical	Value	
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA x ³	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier		Х		1.3.171.1.1.10.3	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	Х	TRUE ⁶		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess4	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx17.crt	Fixed
subjectKeyIdentifier	{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 ⁵ .crl	Fixed
BasicConstraints	{id-ce 19}	Х	TRUE ⁶	N/A	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

3.4.1 LuxTrust SSL CA

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

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

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



 $^{^4}$ Since LuxTrust Global Qualified CA 3

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





		LuxTru	st SSL (CA	
Base Profile	OID	Included	Critical	Value	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed
SignatureValue		Х		Issuing LTGRCA Signature	
Validity					
NotBefore		Х		Key Generation Process Date/Time	
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). 20 years certificate requires a 4096 key length.	
Issuer					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x ¹	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust SSL CA x ⁷	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier (1)		Х		1.3.171.1.1.10.5	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 ⁶		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyldentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess ⁸	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				

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

⁸ Since LuxTrust SSL CA 4







VFRSION 1 24

	LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value					
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed				
AccessMethod	{Id-ad-2}		False						
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx17.crt	Fixed				
subjectKeyldentifier	{id-ce 14}	X	FALSE						
Keyldentifier		Х		SHA-1 Hash of Subject public key					
cRLDistributionPoints	{id-ce 31}	Х	FALSE						
distributionPoint									
FullName		Х		http://crl.luxtrust.lu/LTGRCAx 1.crl	Fixed				
BasicConstraints	{id-ce 19}	Х	TRUE ⁶	N/a					
CA		Х		TRUE	Fixed				
pathLenConstraint		Х		0 (Zero)	Fixed				

3.4.2 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									
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed				
SignatureValue		Х		Issuing LTGRCA Signature					
Validity									
NotBefore		Х		Key Generation Process Date/Time					
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed				
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). 20 years certificate requires a 4096 key length.					
Issuer									
CountryName	{ id-at-6 }	Х		LU	Fixed				
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x ¹	Fixed				
organizationName		Х		LuxTrust S.A.	Fixed				
Subject									
CountryName	{ id-at-6 }	Х		LU	Fixed				
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA x ⁹	Fixed				
organizationName		Х		LuxTrust S.A.	Fixed				
CertificatePolicies	{id-ce 32}	Х	FALSE						

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



Page 30 de 165





VERSION 1 22

LuxTrust Global Timestamping CA									
Base Profile	OID	Included	Critical	Value					
policyldentifier		Х		1.3.171.1.1.10.8	Fixed				
policyQualifiers				N/a					
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed				
Qualifier		Х		https://repository.luxtrust.lu	Fixed				
KeyUsage	{id-ce 15}	Х	TRUE ⁶						
keyCertSign				Set	Fixed				
crlSign				Set	Fixed				
authorityKeyldentifier	{id-ce 35}	Х	FALSE						
Keyldentifier		Х		SHA-1 Hash of Authority public key					
authorityInfoAccess10	{id-pe 1}		False						
AccessMethod	{Id-ad-1}								
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed				
AccessMethod	{Id-ad-2}		False						
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx1.crt	Fixed				
subjectKeyldentifier	{id-ce 14}	Х	FALSE						
Keyldentifier		Х		SHA-1 Hash of Subject public key					
cRLDistributionPoints	{id-ce 31}	Х	FALSE						
distributionPoint									
FullName		Х		http://crl.luxtrust.lu/LTGRCA ⁵ .crl	Fixed				
Basic Constraints	{id-ce 19}	Х	TRUE ⁶	N/a					
CA		Х		TRUE	Fixed				
pathLenConstraint		Х		0 (Zero)	Fixed				

3.4.3 Certificate extensions

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

3.4.4 Algorithm object identifiers

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

3.4.5 Name forms

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

3.4.6 Name constraints

Name constraints are supported as per RFC 5280.

3.4.7 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

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







3.4.8 Usage of Policy Constraints extension

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

3.4.9 Policy qualifiers syntax and semantics

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

3.5 LuxTrust End-entity - Certificates profiles

3.5.1 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+¹¹ Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy OID 1.3.171.1.1.10.3.1, and
 - One LuxTrust NCP+¹² certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.10.3.2.

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

- LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.26.
- LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1]
 (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key
 pairs, according to two certificate policies
 - One LuxTrust QCP¹¹ Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.10.3.3, and
 - One LuxTrust NCP¹² certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID *1.3.171.1.1.10.3.4*.
- 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 NCP¹² certificate for Natural Persons for the combined purposes of electronic signature, data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.5.
- LuxTrust eSeal Smart card-based certificates: The eSeal smart card exists in two versions: advanced and qualified.

The qualified eSeal product is based on two certificate policies:

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

The advanced eSeal product is based on two certificate policies:

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



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





VFRSION 1 24

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

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

- LuxTrust SSL/TLS Standard Server Certificates: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.10.5.1.
- 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.

3.5.2 Version number(s)

X.509 v3 is supported and used.

3.5.3 LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures

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

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

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

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

LuxTrust SSCD QCP+ Certificate Profile							
Attribute	tribute Field IN ¹³ CE ¹⁴ O/M ¹⁵ CO ¹⁶ Value						
Base							
Profile							
Version		✓	False				
					S	Version 3 Value = "2"	

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

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

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



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





LuxTrust SSCD QCP+ Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
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	lue	✓	False						
					D	Issuing CA Signature.			
Issuer	T	√	False		S				
	countryName	✓ ✓			S	LU			
	commonName				S	LuxTrust Global Qualified CA x ¹⁷			
	organizationName	√			S	LuxTrust S.A.			
Validity	T	✓ ✓	False						
	NotBefore				D	Certificate generation process date/time.			
	NotAfter	✓			D	Certificate generation process date/time + 36			
		✓				Months			
Subject	T	•	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
						PRO and PRIVATE products: Concatenatio			
commonName	✓		М	D	of given name(s) and surname(s) as on I.				
	- Commonwanto					card separated by a "Space" character.			
						DDO and DDUATE and due to Character and			
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s			
						as on ID card			
						PRO and PRIVATE products: Surname(s) a			
	surname	✓		M	D	on ID card without indication "épouse", "ép." o			
						similar and the subsequent name(s)			
	countryName	~		М	D	Nationality of holder (ISO3166)			
	emailAddress	✓		0	D	Subject's email address			
						PRIVATE products:			
						Fixed value: "Private Person"			
						PRO products:			
	title	✓		М	D	"Professional Person" (default) or "Professional			
						Administrator"			
						(Other titles possible for special purpos certificates)			
						PRO products only:			
	organizationName	✓		М	D	Name of company/institution as in articles of			
						association or equivalent documents, including			
						the legal form.			
	localityNome	√		N 4		PRO products only: Company/institutio			
	localityName			М	D	country of HQ (as in articles of association)			

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







	LuxTrust SSCD QCP+ Certificate Profile								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	organizationalUnitName 1	~		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).			
	organizationalUnitName 2	~		0	D	PRO products only: Company/institution department or other information item			
subjectPublic	KeyInfo	✓	False						
	Algorithm	√				Public Key: Key length: 2048bit (RSA); public			
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).			
Extensions									
Authority Properties									
authorityKeyl	dentifier	✓	False						
	keyldentifier	V				SHA-1 Hash of the LuxTrust Global Qualified CA public key			
authorityInfoA	Access	√	False						
	AccessMethod	√				Id-ad-2			
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt			
	AccessMethod	√				Id-ad-1			
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸			
cRLDistribution	onPoint	√	False						
	distributionPoint	√			S	17			
	fullName	√				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl			
Subject Properties									
subjectAltNar	ne	√	False						
	Rfc822Name	√		0	D	Certificate Holder's email address			
subjectKeyIde	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 bitstring bits).			
Policy Properties									
keyUsage		✓	True						
	digitalSignature	✓			S	False			

¹⁸ SINCE LTGQCA3







VERSION 1 22

	LuxTrust SSCD QCP+ Certificate Profile							
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value		
	nonRepudiation	✓			S	True		
	keyEncipherment	√			S	False		
	dataEncipherment	√			S	False		
certificatePo	licies	✓	False					
	Policyldentifier	√				1.3.171.1.1.10.3.1		
	policyQualifierID	✓			S	Id-qt-1 (CPS)		
	qualifier	√			S	https://repository.luxtrust.lu		
	policyQualifierID	√			S	Id-qt-2 (User Notice)		
	noticeNumbers							
	DisplayText	√				LuxTrust Qualified Certificate on SSCD		
						compliant with ETSI TS 101 456 QCP+		
						certificate policy. Key Generation by CSP.		
						Sole Authorised Usage: Support of Qualified		
						Electronic Signature.		
	Policyldentifier	✓				0.4.0.1456.1.1		
QualifiedCer	tificateStat							
	QcCompliance	√		М	S	0.4.0.1862.1.1		
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance		
						with [3]		
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance		
						with [3]		
	QcSSCD	√		М	D	0.4.0.1862.1.4		

3.5.4 LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption

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

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

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

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

LuxTrust SSCD NCP+ Certificate Profile								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value		
Base Profile								
Version		✓	False					
					S	Version 3 Value = "2"		
SerialNumber		✓	False					
					FDV	Validated on duplicates.		
signatureAlgor	rithm	√	False					







Attribute Field IN¹® CE¹® O/M¹® CO¹® Value algorithm S OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption. SignatureValue		Lux	Trust S	SSCD I	NCP+ Ce	rtifica	te Profile
SignatureValue	Attribute	Field	IN 13	CE ¹⁴	O/M ¹⁵	CO 16	Value
Separature Validity False D Issuing CA Signature.		algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
Issuer							RSA Encryption.
CountryName	signatureVal	ue	✓	False			
countryName						D	Issuing CA Signature.
commonName organizationName v	issuer		✓	False		S	
Validity		countryName	✓			S	LU
Validity		commonName	√			S	LuxTrust Global Qualified CA x17
NotBefore Y D Certificate generation process date/time.		organizationName	✓			S	LuxTrust S.A.
NotAfter NotAft	Validity		✓	False			
Subject V False Serial Number Sometime + 36 Months		NotBefore	✓			D	Certificate generation process date/time.
SerialNumber		NotAfter	✓			D	Certificate generation process date/time + 36
serialNumber							Months
commonName M D PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character givenName M D PRO and PRIVATE products: Given name(s) as on ID card without indication 'epouse', "ep." or similar and the subsequent name(s) countryName M D Nationality of holder (ISO3166) emailAddress V M D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Professional Person" (default) or "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) organizationName M D PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. PRO products only: Company/institution	subject		✓	False			
commonName V M D of given name(s) and surname(s) as on ID card separated by a "Space" character M D RRO and PRIVATE products: Given name(s) as on ID card PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) countryName V M D Nationality of holder (ISO3166) emailAddress V O D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Fixed value: "Private Person" (Other titles possible for special purpose certificates) organizationName V M D Name of company/institution as in articles of association or equivalent documents, including the legal form. localityName V M D PRO products only: Company/institution		serialNumber	✓		М	D	Serial Number as constructed by LRAO
givenName M							PRO and PRIVATE products: Concatenation
givenName M D RRO and PRIVATE products: Given name(s) as on ID card PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) countryName M D Nationality of holder (ISO3166) emailAddress V D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Fixed value: "Private Person" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. IocalityName V M D PRO products only: Company/institution		commonName	✓		М	D	of given name(s) and surname(s) as on ID
surname M D as on ID card PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) countryName M D Nationality of holder (ISO3166) emailAddress V D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Fixed value: "Private Person" (Other titles possible for special purpose certificates) organizationName M D Name of company/institution as in articles of association or equivalent documents, including the legal form. localityName V M D PRO products only: Company/institution							card separated by a "Space" character
surname M D as on ID card PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) countryName M D Nationality of holder (ISO3166) emailAddress V D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Fixed value: "Private Person" (Other titles possible for special purpose certificates) organizationName M D Name of company/institution as in articles of association or equivalent documents, including the legal form. localityName V M D PRO products only: Company/institution							PRO and PRIVATE products: Given name(s)
surname M		givenName	✓		М	D	
surname M							PRO and PRIVATE products: Surname(s) as
countryName which is a countryName countryName which is a countryName which is a country is a country in the legal form. which is a countryName which is a country in the legal form. which is a countryName which is a country in the legal form. which is a countryName which is a country in the legal form. which is a countryName which is a country in the legal form. which is a countryName which is		surname	✓		М	D	on ID card without indication "épouse", "ép." or
emailAddress V O D Subject's email address PRIVATE products: Fixed value: "Private Person" PRO products: Fixed value: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution							similar and the subsequent name(s)
title M D PRIVATE products: Fixed value: "Private Person" PRO products: (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. PRO products only: Company/institution		countryName	✓		М	D	Nationality of holder (ISO3166)
title M D Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution PRO prod		emailAddress	✓		0	D	Subject's email address
title M D Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution PRO prod							PRIVATE products:
title M D #PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution							
title ✓ M D "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates) PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution PRO produ							
organizationName M D PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. Professional Person** (default) or "Professional Administrator** (Other titles possible for special purpose certificates) Name of company/institution as in articles of association or equivalent documents, including the legal form. PRO products only: Company/institution		444					
organizationName M D Name of company/institution as in articles of association or equivalent documents, including the legal form. PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. PRO products only: Company/institution		TITLE	ľ		IVI		
organizationName M D RO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution PRO products only: Company/institution PRO products PRO pr							"Professional Administrator"
organizationName M D PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution PRO products only: Company/institution PRO products PRO p							(Other titles possible for special purpose
organizationName M D Name of company/institution as in articles of association or equivalent documents, including the legal form. D Name of company/institution as in articles of association or equivalent documents, including the legal form. D PRO products only: Company/institution							certificates)
localityName M D association or equivalent documents, including the legal form. PRO products only: Company/institution							PRO products only:
association or equivalent documents, including the legal form. Description PRO products only: Company/institution PRO products only: Company/institution		organizationName	✓		M	D D	Name of company/institution as in articles of
localityName M D PRO products only: Company/institution		organization i valite			l ivi		association or equivalent documents,
localitvName							including the legal form.
localitvName							PRO products only: Companylinetitytion
		localityName	✓		М	D	country of HQ (as in articles of association)







	LuxT	rust S	SCD N	NCP+ Ce	rtifica	te Profile
Attribute	Field	IN 13	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	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	√		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	lentifier	✓	False			
	keyldentifier	>				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfoA	ccess	√	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx 17.crt
	AccessMethod	>				Id-ad-1
	accessLocation	>				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistributio	nPoint	✓	False			
	distributionPoint	>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNam	ne	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylde	ntifier	✓	False			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False







	Lux	Trust S	SSCD N	NCP+ Ce	rtifica	te Profile
Attribute	Field	IN 13	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	keyEncipherment	✓			S	True
	dataEncipherment	√			S	True
certificatePolic	cies	√	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	√				LuxTrust Certificate on SSCD compliant with
						ETSI TS 102 042 NCP+ certificate policy. Key
						Generation by CSP.
						Sole Authorised Usage: Data or Entity
						Authentication and Data Encryption.
	Policyldentifier	✓				0.4.0.2042.1.2

3.5.5 LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures

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

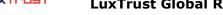
These LuxTrust non SSCD QCP Certificates are compliant with and include the OID reference of the QCP certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.2; cf. [3]).

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

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

	LuxTrust non SSCD QCP Certificate Profile											
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value						
Base Profile												
Version		~	False									
					Ø	Version 3 Value = "2"						
SerialNumbe	SerialNumber		False									
					FDV	Validated on duplicates.						
signatureAlg	orithm	✓	False									
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.						
signatureVal	signatureValue		False									
					D	Issuing CA Signature.						





LuxTrust Global Root CA Certificate Specifications

	LuxT	rust n	on SS	CD QCP	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO16	Value
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	✓		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	*		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	✓		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)







	LuxTı	rust n	on SS	CD QCP	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	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	~		0	D	PRO products only: Company/institution department or other information item
subj	ectPublicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Pro	Authority Properties					
authorityKey	ldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistributi	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Prop	erties					
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyld	lentifier	✓	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).







	LuxTrust non SSCD QCP Certificate Profile											
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value						
Policy Prope	erties											
keyUsage		✓	True									
	digitalSignature	✓			S	False						
	nonRepudiation	✓			S	True						
	keyEncipherment	✓			S	False						
	dataEncipherment	✓			S	False						
certificatePo	licies	✓	False									
	Policyldentifier	✓				1.3.171.1.1.10.3.3						
	policyQualifierID	✓			S	Id-qt-1 (CPS)						
	qualifier	✓			S	https://repository.luxtrust.lu						
	policyQualifierID	✓			S	Id-qt-2 (User Notice)						
	DisplayText	✓				LuxTrust Qualified Certificate not on SSCD compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert						
	Policyldentifier	✓				0.4.0.1456.1.2						
QualifiedCe	rtificateStat											
	QcCompliance	✓		М	S	0.4.0.1862.1.1						
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]						
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]						
	QcSSCD	✓				NOT SET						

3.5.6 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

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

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

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

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





	VERSION 1.24								
	LuxTrust non SSCD NCP Certificate Profile								
Attribute	Attribute Field IN ¹³ CE ¹⁴ O/M ¹⁵ CO ¹⁶ Value								
Race									

	LuxTrust	non S	SSCD 1	NCP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version	T	√	False			
					S	Version 3 Value = "2"
SerialNumbe	er T	✓	False			
		✓			FDV	Validated on duplicates.
signatureAlg		'	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
		✓				with RSA Encryption.
signatureVa	lue		False			Landing OA Oiseastons
		√	F-1		D	Issuing CA Signature.
issuer	assumt a Alama	· ·	False		S	LU
	countryName	✓			S	LuxTrust Global Qualified CA x ¹⁷
		✓			S	LuxTrust Global Qualified CA x LuxTrust S.A.
Validity	organizationName	✓	False		3	Lux Trust S.A.
validity	NotBefore	✓	raise		D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time +
	Novitei					36 Months
subject		√	False			CO MONUS
	serialNumber	✓		М	D	Social Number as constructed by LPAO
	SerialNumber	<u> </u>		IVI	<i>D</i>	Serial Number as constructed by LRAO
						PRO and PRIVATE products:
	commonName	✓		М	D	Concatenation of given name(s) and
						surname(s) as on ID card separated by a
						"Space" character
	givenName	✓		M	D	PRO and PRIVATE products: Given
	giveriivairie			IVI		name(s) as on ID card
						PRO and PRIVATE products: Surname(s)
						as on ID card without indication "épouse",
	surname	✓		М	D	"ép." or similar and the subsequent
						name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	✓		М	D	"Professional Person" (default) or
						"Professional Administrator"
						(Other titles possible for special purpose certificates)





	LuxTrust	non S	SCD N	ICP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	organizationName	~		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	·		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	✓		0	D	PRO products only: Company/institution department or other information item
subjectPublic	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	*				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistributi	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	√		0	D	Certificate Holder's email address
subjectKeyId		√	False			







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

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

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

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

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

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







	LuxTrust					
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	False			
		✓			FDV	Validated on duplicates.
signatureAl		V	False			
	algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA
						with RSA Encryption.
						OID = "1.2.840.113549.1.1.11" -
		√				SHA256 with RSA Encryption.
signatureVa	alue T		False			
laa		✓	F-1-		D	Issuing CA Signature.
Issuer	and Maria	· ·	False		S	
	countryName	· ·			S	LU
	commonName	· ·			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	· ·			S	LuxTrust S.A.
Validity	T v 45 6	· ·	False			
	NotBefore	· ·			D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time
		√				36 Months
subject	T		False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						PRO and PRIVATE products
	commonName	✓		М	D	Concatenation of given name(s) and
	Commonwante			IVI		surname(s) as on ID card separated by
						"Space" character
						PRO and PRIVATE products: Give
	givenName	✓		М	D	name(s) as on ID card
						PRO and PRIVATE products: Surname(s
	surname	✓		М	D	as on ID card without indication "épouse
						"ép." or similar and the subsequer
						name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	✓		М	D	
						"Professional Person" (default) of "Professional Administrator"
						(Other titles possible for special purpos
						certificates)







	LuxTrust Sig	gning	Serve	r NCP (Certific	ate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	organizationName	✓		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	~		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à:" & (Date of birth + 18 years).
	organizationalUnitName 2	✓		0	D	PRO products only: Company/institution department or other information item
subjectPublic	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistributi	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl
Subject Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyId		√	False			







	LuxTrust Si	gning	Serve	r NCP (Certific	cate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the
						least significant 60 bits of the SHA-1 hash
						of the value or subjectPublicKey bit string
						(tag, not including the length and number
						of unused bit-string bits).
Policy						
Properties						
keyUsage	T	√	True			
	digitalSignature	√			S	True
	nonRepudiation				S	True
	keyEncipherment	√			S	True
	dataEncipherment	√			S	True
certificatePo	licies	√	False			
	Policyldentifier	√				1.3.171.1.1.10.3.5
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	√				LuxTrust Certificate not on SSCD
						compliant with ETSI TS 102 042 NCP
						certificate policy. Key Generation by CSP.
						Sole Authorised Usage: Signature, Data or
						Entity Authentication and Data Encryption.
	PolicyIdentifier	√				0.4.0.2042.1.1

3.5.8 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	LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		✓	False								







LuxTrust non	SSCD NCP+ Public	Certi	ficate	Profil	e for	Mass Signature Services
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
					S	Version 3 Value = "2"
SerialNumber		√	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
eignaturer agentami	algorithm				S	OID = "1.2.840.113549.1.1.11" -
	algonum				0	SHA256 with RSA Encryption
sign of tro Volus		√	False			ONAZOO WIII NOA ENCIYPIION
signatureValue			raise			
		✓			D	Issuing CA Signature.
Issuer	1	· ·	False		S	
	countryName				S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	√			D	Certificate generation process
						date/time.
	NotAfter	√			D	Certificate generation process
	1105 1101					date/time + 36 Months
aubiost		✓	False			date/time + 30 Wortins
subject			raise			
						Name commonly used by the subject
	commonName	✓		М	D	to represent itself as stated in ETSI TS
	Commonwanto					119 412-3, the name should not be
						domain-shaped
						Country in which the organization's
						Country in which the organization's
	countryName	✓		М	D	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
						-
						Names as in articles of association,
	organizationName	✓		М	D	including the legal form (as specified in
						the memorandum and articles of
						association or an equivalent document)
						Location in which the organization's
						registered office is established (as
	localityName	✓		М	D	,
	localityName			IVI	D	specified in the memorandum and
						articles of association or an equivalent
						document)
	annonimation of the MAT			_	1	As an action of the Contract
	organizationalUnitName 1	✓		0	D	As provided by Subscriber
		<u> </u>				
	organizationalUnitName 2	✓		0	D	As provided by Subscriber
		L .				
subjectPublicKeyInfo		✓	False			
	algorithm	√				Public Key: Key length: 2048 bit (RSA);





LuxTrust Global Root CA Certificate Specifications

LuxTrust non	SSCD NCP+ Public	Certi	ficate	Profil	e for	Mass Signature Services
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyIdentifier		√	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Globa
						Qualified CA public key
authorityInfoAccess	T	V	False			
	AccessMethod	✓ ✓				ld-ad-2
	accessLocation	V /				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	V				ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint	T	✓ ✓	False			
	distributionPoint	\ \ \ \ \			S	17
	fullName	· ·				http://crl.luxtrust.lu/LTGQCAx 17.crl
Subject Properties		✓				
subjectAltName	T	\ \ \ \	False			
	Rfc822Name	∨		0	D	Certificate Holder's email address
subjectKeyIdentifier	T	V V	False			
	keyldentifier	•			Fixed	The Key Identifier comprises a four-b
						field with a 0100 value, followed by the
						least significant 60 bits of the SHA-
						hash of the value or subjectPublicKe
						bit string (tag, not including the lengt
						and number of unused bit-string bits).
Policy Properties		✓	_			
keyUsage	I	· ·	True		_	
	digitalSignature				S	False
					_	-
	nonRepudiation				S	True
	kov.En sinh sweent	✓				False
	keyEncipherment				S	Faise
	dataEncipherment	✓			S	False
	uatachcipherment				3	Faise
certificatePolicies		√	False			
Octanioator Onoido	Policyldentifier	✓	i disc			1.3.171.1.1.10.3.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers	+			3	10-41-2 (OSEI NOLICE)
	HOUGENUITIDEIS					







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

3.5.9 LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures

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

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

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

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

	LuxTrust Integration Certificate Profile											
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value						
Base												
Profile												
Version		✓	False									
					S	Version 3 Value = "2"						
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	lue	✓	False									
					D	Issuing CA Signature.						
Issuer		✓	False		S							
	countryName	√			S	LU						
	commonName	√			S	LuxTrust Global Qualified CA x ¹⁷						
	organizationName	√			S	LuxTrust S.A.						
Validity		✓	False									
	NotBefore	√			D	Certificate generation process date/time.						
	NotAfter	√			D	Certificate generation process date/time + 36 Months						
Subject	•	✓	False									
	serialNumber	✓		М	D	Serial Number as constructed by LRAO						







	Lux	Trus	t Inte	gratio	n Ce	rtificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	commonName	✓		М	D	Concatenation of given name(s) and surname(s)
	givenName	✓		М	D	TEST ONLY + " " + As provided by Subscriber
	surname	✓		М	D	As provided by Subscriber
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	As provided by Subscriber
	Title	√		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator"
	organizationName	>		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	√		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	~		0	D	PRO products only: Company/institution department or other information item
subjectPublic	cKeyInfo	√	False			
	Algorithm	✓ ✓				Public Key: Key length: 2048bit (RSA); public exponent:
Fatanalan	subjectPublicKey	v		M		Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	Identifier	✓	False			
_	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			







	Lu	xTrus	t Inte	gratio	on Ce	rtificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	AccessMethod	√				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	ame	√	False			
	Rfc822Name	✓		0	D	N/A
subjectKeyl	dentifier	√	False			
	keyldentifier	✓ 			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage	T	· ·	True		_	
	digitalSignature	\ \ \ \			S	False
	nonRepudiation	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \			S	True
	keyEncipherment	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \			S	False
	dataEncipherment	✓			S	False
certificatePo	T	V	False			
	PolicyIdentifier	· ·				1.3.171.1.1.10.3.7
	policyQualifierID	· ·			S	Id-qt-1 (CPS)
	Qualifier	✓ ✓			S	https://repository.luxtrust.lu
	policyQualifierID				S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.3

3.5.10 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.







	LuvTrust	SSCD	CDT I	ntegra	tion Co	ertificate Profile
A 44-Th code						
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profile		√				
Version	T	•	False		_	
		✓			S	Version 3 Value = "2"
SerialNumber	T	· ·	False			
					FDV	Validated on duplicates.
signatureAlgo	rithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValu	е	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36
						Months
Subject		✓	False			
•	serialNumber	√		М	D	Social Number as constructed by LPAO
	Senanumber			IVI	, D	Serial Number as constructed by LRAO
	commonName	√		М	D	LGQCA XX SC PRI V3 (XX a number selected
	Commonwante	·		IVI		internally by LuxTrust)
						LGQCA XX (XX a number selected internally
	givenName	✓		М	D	by LuxTrust)
						by Eax ridsty
	Surname	✓		М	D	SC PRI V3
	countryName	√		М	D	LU
	Country Harris					
	emailAddress	✓		0	D	N/A
	Title	✓		М	D	Private Person
oubleetDubliel		✓	Folos			
subjectPublich	1	· ·	False			Public Koya Koya longth, 2040 hit (DCA) and the
	Algorithm	· ·			-	Public Key: Key length: 2048 bit (RSA); public
F.4	subjectPublicKey	-		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties		✓				
authorityKeylo	1	V	False			
	keyldentifier	•				SHA-1 Hash of the LuxTrust Global Qualified
						CA public key
authorityInfoA	ccess	✓	False			
	AccessMethod	√				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributio	nPoint	✓	False			







	LuxTrust	SSCD	LCP+ I	integra	tion Ce	ertificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	distributionPoint	√			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNan	ne	✓	False			
	Rfc822Name	✓		0	D	N/A
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		√	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePoli	cies	√	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.8
	policyQualifierID	√			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	DisplayText	√				LuxTrust INTEGRATION CERTIFICATE on
						SSCD compliant with ETSI TS 102 042 LCP+
						certificate policy. Key Generation by CSP. Sole
						Authorised Usage: Authentication and
						Encryption for Integration Purposes.
	Policyldentifier	✓]		0.4.0.2042.1.3

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

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

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

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







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

A timila uta		IN ¹³	CE ¹⁴		CO ¹⁶	cate Profile
Attribute	Field	IN13	CE ¹⁴	O/M ¹⁵	COI	Value
Base Profile						
Version		✓	False			
V 0131011			1 4130		S	Version 3 Value = "2"
SerialNumb	er	✓	False			voicion o value 2
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			·
	Algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1
						with RSA Encryption.
						OID = "1.2.840.113549.1.1.11" - if
						SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	· ·			S	LU
	commonName	✓ ✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	V			S	LuxTrust S.A.
Validity	T	V	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
						LGQCA XX CSS (XX a number selected internally by LuxTrust) or Concatenation of
	commonName	✓		М	D	given name(s) and surname(s) separated
						by a "Space" character.
						LGQCA XX (XX a number selected
	givenName	✓		М	D	internally by LuxTrust) or Given name(s
						CSS or Surname(s) as on ID document
	Surname	✓		М	D	without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	✓		М	D	LU or Nationality of holder (ISO3166)
	emailAddress	✓		0	D	N/A
	Title	✓		М	D	Private Person
subjectPubli	icKeyInfo	√	False			
	Algorithm	√				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	√		М		public exponent: Fermat-4 (=010001).







LuxTrust Signing Server LCP Certificate Profile Attribute Field IN13 CE14 O/M15 CO16 Value											
	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Extensions											
Authority											
Properties											
authorityKey		√	False								
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Glob Qualified CA public key					
authorityInfo	Access	✓	False			addinion of the same not					
additionly initio	AccessMethod	✓	1 4.00			ld-ad-2					
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt					
	AccessMethod	√				Id-ad-1					
	accessLocation	√				http://qca.ocsp.luxtrust.lu/					
cRLDistributi		√	False			intp://qoa.oosp.iaxtrust.iu/					
	distributionPoint	√	1 4136		S						
	fullName	√			3	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl					
Subject	Tullivanie					INTERNATIONAL CONTROL					
Properties											
subjectAltNa	me	√	False								
	Rfc822Name	✓		0	D	N/A					
subjectKeyld	lentifier	✓	False								
	keyldentifier	√			Fixed	The Key Identifier comprises a four-b					
						field with a 0100 value, followed by the					
						least significant 60 bits of the SHA-1 has					
						of the value or subjectPublicKey bit strir					
						(tag, not including the length and number					
						of unused bit-string bits).					
Policy											
Properties											
keyUsage		√	True								
	digitalSignature	√			S	True					
	nonRepudiation				S	True					
	keyEncipherment	✓			S	True					
	dataEncipherment	✓			S	True					
certificatePo	licies	✓	False								
<u> </u>	Policyldentifier	✓				1.3.171.1.1.10.3.9					
	policyQualifierID	√			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					







	LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
	DisplayText	✓				INTEGRATION Certificate not on SSCD				
						compliant with ETSI TS 102 042 LCP				
						cert.policy. Key Generation by CSP. Sole				
						Authorised Usage: Signature, Data or				
						Entity Auth. and Data Enc. for integration				
						purposes				
	Policyldentifier	√				0.4.0.2042.1.3				

3.5.12 LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes

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

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

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

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

	LuxTr	ust SSCD	LORA	QCP+	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		√	False			
					S	Version 3 Value = "2"
SerialNumb	er	√	False			
					FDV	Validated on duplicates.
signatureAlg	jorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVa	signatureValue		False			
					D	Issuing CA Signature.
Issuer	•	✓	False		S	
	countryName	√			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x17
	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







	LuxTru	st SSCD	LORA	QCP+	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	commonName	√		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	√		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		М	D	Constructed by LuxTrust
	localityName	√		М	D	Country of RA
	organizationalUnitName	√		М	D	RA code Constructed by LuxTrust
	organizationalUnitName	✓		М	D	RAO code Constructed by LuxTrust
subjectPublic	:KeyInfo	✓	False			
	Algorithm	√				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyl	dentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo/	Access	✓	False			
	AccessMethod	√				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributi	onPoint	✓	False			
	distributionPoint	√			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNa	me	√	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyId	entifier	✓	False			







	LuxTr	ust SSCE	LORA	QCP+	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field
						with a 0100 value, followed by the least
						significant 60 bits of the SHA-1 hash of the
						value or subjectPublicKey bit string (tag, not
						including the length and number of unused
						bit-string bits).
Policy						
Properties						
keyUsage		√	True			
	digitalSignature	√			S	False
	nonRepudiation	√			S	True
	keyEncipherment	√			S	False
	dataEncipherment	✓			S	False
certificatePo	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.10
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				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
QualifiedCe	rtificateStat					
	QcCompliance	✓		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance
						with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance
						with [3]
	QcSSCD	√		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

3.5.13 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.

	LuxTrus	t SSC	D LOR	A NCP+	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgo	rithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureValu	e	✓	False			
		,			D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	✓			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	√			S	LuxTrust S.A.
Validity	T	√	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	√		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		M	D	"LuxTrust RA Officer"
	organizationName	✓		M	D	Constructed by LuxTrust
	localityName	✓		M	D	Country of RA
	organizationalUnitName	~		М	D	RA code Constructed by LuxTrust
	organizationalUnitName	√		М	D	RAO code Constructed by LuxTrust
subjectPublicl	KeyInfo	✓	False	_		





LuxTrust Global Root CA Certificate Specifications

	LuxTri	ust SSC	D LOR	A NCP+	Certif	icate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	Algorithm	√				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	√		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties		 				
authorityKeyl		V V	False			
	keyldentifier					SHA-1 Hash of the LuxTrust Global Qualified
		✓				CA public key
authorityInfoA	T	· ·	False			
	AccessMethod	· ·			-	Id-ad-2
	accessLocation	· ·				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	· ·				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribution	T	· ·	False			
	distributionPoint	✓			S	17
	fullName	V				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltNar	ne	√	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		✓	T			
keyUsage		√	True			
	digitalSignature	•			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePoli	icies	√	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				<u> </u>	, , ,







	LuxTrust SSCD LORA NCP+ Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with				
						ETSI TS 102 042 NCP+ certificate policy. Key				
						Generation by CSP.				
						Sole Authorised Usage: Data or Entity				
						Authentication and Data Encryption for LRAO				
						purposes.				
	Policyldentifier	✓				0.4.0.2042.1.2				

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

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

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

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

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

	LuxTrust non SSC	CD QC	P Mas	s LRAO	Signa	tures Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	r	✓	False			
					FDV	Validated on duplicates.
signatureAlgo	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 Global Qualified CA x ¹⁷
	organizationName	√			S	LuxTrust S.A.
Validity		✓	False			







						tures Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) and surname(s as on ID card separated by a "Space" character
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	√		М	D	Surname(s) as on ID card without indicatio "épouse", "ép." or similar and the subsequer name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA officer – LRS"
	organizationName	√		М	D	"RA" & RA number & " – " & Name of th LuxTrust RA
	localityName	√		М	D	Country of RA (as in articles of association)
	organizationalUnitName 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	√		0	D	RAO code Constructed by LuxTrust
sub	ojectPublicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); publi
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Pro	operties					
authorityKey	rldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified Copublic key
authorityInfo	Access	✓	False			
	AccessMethod	√				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸







Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO16	Value
		√		O/IVI	00**	Value
cRLDistribut			False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx 17.crl
Subject Prop	perties					
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	dentifier	✓	False			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field wit a 0100 value, followed by the least significant 6 bits of the SHA-1 hash of the value of subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Prope	erties					
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	√			S	False
	dataEncipherment	✓			S	False
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.12
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust Qualified Certificate not SSCI compliant with ETSI TS101456 QCP certificat policy.Key Generation by CSP.Sole Authorise Usage: Support of Advanced Electroni 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 wit







	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcSSCD	✓				NOT SET				

3.5.15 LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures

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

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

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust eID SSCD QCP+ Certificate Profile								
Attribute	Field	IN ¹⁹	CE ²⁰	O/M ²¹	CO ²²	Value			
Base									
Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	orithm	✓	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with			
						RSA Encryption.			
signatureVal	ue	✓	False						

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

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



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

²¹ O/M: O = Optional, M = Mandatory.





	LuxTrust eID SSCD QCP+ Certificate Profile								
Attribute	Field	IN ¹⁹	CE ²⁰	O/M ²¹	CO ²²	Value			
					D	Issuing CA Signature.			
Issuer		√	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x ²³			
	organizationName	✓			S	LuxTrust S.A.			
Validity	<u>, </u>	√	False						
	NotBefore	√			D	Certificate generation process date/time.			
	NotAfter	V			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate			
Subject	T	√	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) separated by the space character			
	givenName	✓		М	D	Given name(s) as on ID card or as provided by the RNCID			
	Surname	√		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID			
	countryName	✓		М	D	LU			
	emailAddress	✓		0	D	Subject's email address			
	Title	✓		М	D	"Private Person"			
	organizationalUnitName 1	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).			
subjectPublic	cKeyInfo	√	False						
	Algorithm	√				Public Key: Key length: 2048bit up to 4096bit			
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).			
Extensions									
Authority Properties									
authorityKey	Identifier	√	False						
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA x public key			
authorityInfo	Access	√	False						
	AccessMethod	√	1			Id-ad-2			
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt			
	AccessMethod	√				ld-ad-1			
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸			
cRLDistributi	onPoint	√	False						
	distributionPoint	✓			S				

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







	LuxTrust eID SSCD QCP+ Certificate Profile								
Attribute	Field	IN ¹⁹	CE ²⁰	O/M ²¹	CO ²²	Value			
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl			
Subject Properties									
subjectAltNar	ne	✓	False						
	Rfc822Name	✓		0	D	Subject 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 bitstring bits).			
Policy Properties									
keyUsage		✓	True						
	digitalSignature	✓			S	False			
	nonRepudiation	✓			S	True			
	keyEncipherment	√			S	False			
	dataEncipherment	✓			S	False			
certificatePoli	cies	✓	False						
	Policyldentifier	✓				1.3.171.1.1.10.3.13			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	Qualifier	✓			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	√				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualified Electronic Signature.			
	Policyldentifier	✓				0.4.0.1456.1.1			
QualifiedCert	ificateStat								
	QcCompliance	✓		М	S	0.4.0.1862.1.1			
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]			
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]			
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }			

3.5.16 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]).





LuxTrust Global Root CA Certificate Specifications

VFRSION 1 24

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust SSCD NCP+ Certificate Profile								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumber	SerialNumber		False						
					FDV	Validated on duplicates.			
signatureAlgo	rithm	✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with			
						RSA Encryption.			
signatureValu	е	√	False						
					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	✓			D	Certificate generation process date/time +			
						maximum 120 Months;			
						Certificate generation process date/time + 1			
						day for PSEUDONYM Certificate			
subject		✓	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character			
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID			







	LuxTrust SSCD NCP+ Certificate Profile								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	surname	✓		M	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID			
	countryName	✓		М	D	LU			
	emailAddress	√		0	D	Subject's email address			
	title	√		М	D	"Private Person"			
	organizationalUnitName 1	√		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).			
subjectPublich	KeyInfo	✓	False						
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit			
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).			
Extensions									
Authority Properties									
authorityKeylo	dentifier	✓	False						
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA x public key			
authorityInfoA	ccess	✓	False						
	AccessMethod	✓				Id-ad-2			
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17_crt			
	AccessMethod	√				Id-ad-1			
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸			
cRLDistributio	I	✓	False						
	distributionPoint	∨			S	17			
Subject Properties	fullName	·				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl			
subjectAltNam	ne	✓	False						
	Rfc822Name	√		0	D	Subject 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		✓	True						
	digitalSignature	✓			S	True			
	nonRepudiation				S	False			
	keyEncipherment	✓]		S	True			





LuxTrust Global Root CA Certificate Specifications

VFRSION 1 24

	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
	dataEncipherment	✓			S	True				
certificatePoli	cies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.14				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	√			S	https://repository.luxtrust.lu				
	policyQualifierID	√			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with				
						ETSI TS 102 042 NCP+ certificate policy. Key				
						Generation by CSP.				
						Sole Authorised Usage: Data or Entity				
						Authentication and Data Encryption.				
	Policyldentifier	√				0.4.0.2042.1.2				

3.5.17 LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures

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

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

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

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

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

The certificate re-key is not allowed.

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



	LuxTrust eID SSCD LCP Integration Signature Certificate Profile								
Attribute	Field	IN ²⁴	CE ²⁵	O/M ²⁶	co ²⁷	Value			
Base									
Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	gorithm	✓	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with			
						RSA Encryption.			
signatureVa	lue	✓	False						
					D	Issuing CA Signature.			
Issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x ²⁸			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	✓			D	Certificate generation process date/time + 12			
						Months;			
						Certificate generation process date/time + 1			
						day for PSEUDONYM Certificate			
Subject	T	✓	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	✓		М	D	Concatenation of given name(s) and			
						surname(s) separated by the space character			
	givenName	✓		М	D	specimen-x provided by the RNCID			
	surname	✓		М	D	specimen-x as provided by the RNCID			
	countryName	✓		М	D	LU			
	emailAddress	√		0	D	specimen-x Subject's email address as provided by the RNCID			
	title	✓		М	D	"Private Person"			
	organizationalUnitName 1	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).			
subjectPubli	cKevinfo	✓	False						
,	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bi			
	subjectPublicKey	√	+	M		(RSA); public exponent: Fermat-4 (=010001).			
		1				,, p p			

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

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



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

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

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





Attribute	Field	IN ²⁴	CE ²⁵	O/M ²⁶	CO ²⁷	Value
Extensions	riold			O/III		Yalas
Authority						
Properties						
authorityKey	Identifier	✓	False			
authorityrtey	keyldentifier	✓	1 alse			SHA-1 Hash of the LuxTrust Global Qualifie
	Keylderidhei					CA x public key
authorityInfo	Arrass	✓	False			Or the public Key
authoritynno	AccessMethod	✓	1 alse			Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
aDI Diatributi		✓	Folso			mtp://qca.ocsp.iuxtrust.iu/
cRLDistributi	1	√	False		C	
	distributionPoint	√			S	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
0 11 1	fullName	•				http://crl.luxtrust.lu/LTGQCAxcrl
Subject						
Properties		✓				
subjectAltNa			False	_		
	Rfc822Name	,		0	D	specimen-x Subject's email address
		✓				provided by the RNCID
subjectKeyld		· ·	False			
	keyldentifier	,			Fixed	The Key Identifier comprises a four-bit fie
						with a 0100 value, followed by the lea
						significant 60 bits of the SHA-1 hash of t
						value or subjectPublicKey bit string (tag, r
						including the length and number of unused l
						string bits).
Policy						
Properties		-				
keyUsage	T		True			
	digitalSignature	√			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	√			S	False
	dataEncipherment	✓			S	False
certificatePol	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.16
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	√				LuxTrust INTEGRATION CERTIFICATE
						eID SSCD compliant with ETSI TS 102 0
						LCP certificate policy. Key Generation by CS
						Sole Authorised Usage: Electronic signatu
						for Integration Purposes.
		1				







	LuxTrust eID SSCD LCP Integration Signature Certificate Profile									
Attribute	Field	IN ²⁴	CE ²⁵	O/M ²⁶	co ²⁷	Value				
	QcCompliance	✓		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance				
						with [3]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance				
						with [3]				
	QcSSCD	√		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }				

3.5.18 LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption

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

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

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

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

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

The certificate re-key is not allowed.

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

	LuxTrust eID SSCD LCP Integration AE Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumber	SerialNumber		False								
					FDV	Validated on duplicates.					
signatureAlgo	rithm	✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with					
						RSA Encryption.					
signatureValu	е	✓	False								
					D	Issuing CA Signature.					
issuer		✓	False		S						
	countryName	✓			S	LU					







	LuxTrust eID				_	
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						Months;
						Certificate generation process date/time +
						day for PSEUDONYM Certificate
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						Concatenation of given name(s) a
	commonName	✓		М	D	surname(s) separated by the space charact
		,				
	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
	emailAddress	√		0	D	provided by the RNCID
	title	✓		М	D	"Private Person"
						If the holder is underage: "Mineur jusqu'à :
	organizationalUnitName 1	✓		0	D	(Date of birth + 18 years).
subjectPublic	-KeyInfo	√	False			
Subjectrubild	algorithm	√	i aise			Public Key: Key length: 2048 bit up to 4096
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (=010001
Extensions	subject ublickey			IVI		(NOA), public exponent. I enhat-4 (-01000)
Authority Properties						
authorityKeyl	Identifier	✓	False			
authontyreyi	keyldentifier	√	i aise			SHA-1 Hash of the LuxTrust Global Qualit
	Regidentine					CA x public key
authorityInfo/	Annoes	✓	False			GATA PUBLIC ROY
uddiontyllilo/	AccessMethod	✓	1 4130			Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistributi		√	False			http://qca.ocsp.idxtrust.iu/
	distributionPoint	✓	1 0130		S	
	fullName	√			5	http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject	IUIIIVaIIIC					THEP.//CH.HUXHUSE.HU/ETGQCAX .CH
Properties						
subjectAltNai	me	✓	False			
oabjoot-iii1ai	Rfc822Name	✓	1 6136	0	D	specimen-x Subject's email address
	INCOLLINGING					provided by the RNCID
subjectKeyld		√	False			<u> </u>







	LuxTrust eID	SSCD		tegratio	on AE (Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	co ¹⁶	Value
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field
						with a 0100 value, followed by the least
						significant 60 bits of the SHA-1 hash of the
						value or subjectPublicKey bit string (tag, not
						including the length and number of unused
						bit-string bits).
Policy						
Properties		√				
keyUsage			True			
	digitalSignature	√			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePol	icies	√	False			
	Policyldentifier	√				1.3.171.1.1.10.3.17
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on
						eID SSCD compliant with ETSI TS 102 042
						LCP certificate policy. Key Generation by
						CSP. Sole Authorised Usage: Authentication
						and Encryption for Integration Purposes
	Policyldentifier	✓				0.4.0.2042.1.2

3.5.19 LuxTrust NCP+ Certificates supporting SEAL Signature Services

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

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

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

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







LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumber		✓	False						
					FDV	Validated on duplicates.			
signatureAlgorithm		✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" -			
						SHA256 with RSA Encryption			
signatureValue		✓	False						
					D	Issuing CA Signature.			
Issuer		✓	False		S	3 - 3 - 3 - 3 - 3			
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷			
		√			S	LuxTrust S.A.			
Volidity	organizationName	√	Ealer		3	Lux Hust S.A.			
Validity	Na4Dafana	✓	False		_	Out!			
	NotBefore				D	Certificate generation process			
		√				date/time.			
	NotAfter				D	Certificate generation process			
		✓				date/time + 36 Months			
subject	T	•	False						
						Name commonly used by the subject			
	oommonNome	√		N4	n	to represent itself as stated in ETSI TS			
	commonName			M	D	119 412-3, the name should not be			
						domain-shaped			
						Country in which the approximation's			
						Country in which the organization's			
	countryName	✓		М	D	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			
	emailAddress	ļ .				Oubject's email address if available			
						Names as in articles of association,			
	organizationName	√		М	D	including the legal form (as specified in			
	Organizationivanie	•		IVI	D	the memorandum and articles of			
						association or an equivalent document)			
						Location in which the organization's			
	In a life Alama	√			-	registered office is established (as			
	localityName	, v		M	D	specified in the memorandum and			
						articles of association or an equivalent			
						document)			
	organizational Inithiams 4	✓			Г.	As provided by Subscriber			
	organizationalUnitName 1	•		0	D	As provided by Subscriber			
	organizationalUnitName 2	✓		0	D	As provided by Subscriber			





LuxTrust Global Root CA Certificate Specifications

Attribute	SSCD NCP+ Publ	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	Field	IN13		O/M ¹⁵	CO®	Value
subjectPublicKeyInfo	T	· ·	False			
	algorithm	•				Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	, i		М		public exponent: Fermat-4 (=010001)
Extensions						
Authority Properties						
authorityKeyIdentifier		*	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Glob
						Qualified CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltName		√	False			
oubjood untuino	Rfc822Name	✓	1 4130	0	D	Certificate Holder's email address
aubicat/outdontifics	Nicozzinaine	✓	False	U	D	Certificate Florder's erriali address
subjectKeyIdentifier	11446	✓	raise		Fired	The Kennelder (Consequence Consequence
	keyldentifier				Fixed	The Key Identifier comprises a four-
						field with a 0100 value, followed by t
						least significant 60 bits of the SHA
						hash of the value or subjectPublicK
						bit string (tag, not including the leng
						and number of unused bit-string bits).
Policy Properties						
keyUsage		V	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	keyEncipherment	√			S	False
	dataEncipherment	✓			S	False
	•					
certificatePolicies	1	√	False			
3.0.00	Policyldentifier	✓				1.3.171.1.1.10.3.15
	. Undyradination					
	nolicyOuglifierID	✓			Q	I Id-at-1 (CPS)
	policyQualifierID qualifier	✓			S S	Id-qt-1 (CPS) https://repository.luxtrust.lu







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

3.5.20 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 Se	erver L	.CP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust SSL CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						12;24;36 Months
subject		√	False			







	LuxTrust	SSL Se	erver L	.CP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	countryName	✓		М	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	✓		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	✓		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName1	✓		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber
	commonName	✓		М	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or IP address or unique name of server.
	serialNumber	✓		0	D	Serial Number as provided by subscriber
	emailAddress	~		0	D	Subject's email address
subjectPublic	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	ldentifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	√				http://ssl.ocsp.luxtrust.lu ²⁹
	AccessMethod	√				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx17.crt
cRLDistribut	ionPoint	√	False			
	distributionPoint	V			S	
	fullName	√				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl

²⁹ Since SSL CA 2





LuxTrust Global Root CA Certificate Specifications

VERSION 1.24

			VERSIC	ON 1.24		
	LuxTrust	SSL Se	erver l	_CP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	*		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of



server.





	LuxTrust	SSL Se	erver L	.CP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-URL	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
subjectKeylo	dentifier	√	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).







	LuxTrus	t SSL S	erver L	.CP Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO16	Value
Policy						
Properties						
keyUsage	keyUsage		True			
	digitalSignature	✓			S	True
	nonRepudiation	~			S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo	certificatePolicies		False			
	Policyldentifier	✓				1.3.171.1.1.10.5.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	√				LuxTrust Standard SSL/TLS Server
						Certificate. Not supported by SSCD, Key
						Generation by Subscriber. GTC, CP and
						CPS on http://repository.luxtrust.lu.
						Signed by a SSL CA.
	Policyldentifier	√				0.4.0.2042.1.3
Extended K	ey Usage	✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	True

3.5.21 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,





L'UXTUUST

VFRSION 1 24

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:
 - 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 Exten	ded V	alidati	on Ser	ver C	ertificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber	,	✓	False			
					FDV	Validated on duplicates.
signatureAlgo	rithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" -
						SHA256 with RSA Encryption.
signatureValu	e	✓	False			
					D	Issuing CA Signature.
issuer		√	False		S	
	countryName	√			S	LU
	commonName	✓			S	LuxTrust SSL CA x ¹⁷
	organizationName	√			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time
		✓				+ 12;24 Months
subject	Т	•	False			
	countryName			М	D	Country in which the company's or
	(OID: 2.5.4.6)					institution's registered office is
		✓				established (as specified in the
						memorandum and articles of
						association). (ISO3166)
	jurisdictionOfIncorporationCount			М	D	Contains the country information
	ryName					specified using the applicable ISO
	(OID: 1.3.6.1.4.1.311.60.2.1.3)					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			М	D	State or Province in which the
	(OID: 2.5.4.8)					company's registered office is
	(0.512.61.116)	✓				established (as specified in the
						memorandum and articles of association
						or an equivalent document)
	jurisdisctionOfIncorporationState			0	D	Contains the jurisdiction for the
	OrProvinceName					applicable Incorporating Agency or
	(OID: 1.3.6.1.4.1.311.60.2.1.2)					Registration Agency at the state or
	(OID. 1.3.0.1.4.1.311.00.2.1.2)	✓				province level MUST include both
						country and state or province
						information,
				L		







	SSL/TLS Exten	ded Va	alidatio	on Ser	ver Ce	ertificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	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)	~		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)	√		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)	✓		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.







SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	postalCode			0	D	Postal code of the subject place of			
	(OID: 2.5.4.17)	✓				business.			
	streetAddress	✓		0	D	Number and Street of the physical			
	(OID: 2.5.4.9)					location of the subject			
subjectPublic	KeyInfo	✓	False						
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);			
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).			
Extensions									
Authority									
Properties	. 46	/							
authorityKeyl		-	False			2112 4 11 1 5 11 1 7 1 221 22			
	keyldentifier					SHA-1 Hash of the LuxTrust SSL CA public key			
authorityInfo/	Access	√	False						
	AccessMethod	✓				ld-ad-1			
	accessLocation	√				http://ssl.ocsp.luxtrust.lu 29			
	AccessMethod	✓				Id-ad-2			
	accessLocation	√				http://ca.luxtrust.lu/LTSSLCAx 17.crt			
cRLDistribution	onPoint	√	False						
	distributionPoint	✓			S				
	fullName	√				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl			
Subject Properties									
subjectAltNar	me	✓	False						
	SubjectAltName-dNSName	~		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for 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			







	SSL/TLS Exten	ded Va	alidatio	on Ser	ver C	ertificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	*		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.





LuxTrust Global Root CA Certificate Specifications

	SSL/TLS Extended Validation Server Certificates								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.			
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	T	√	True						
	digitalSignature	✓			S	True			
	nonRepudiation	√			S	False			
	keyEncipherment	✓			S	True			
	dataEncipherment	✓			S	True			
certificatePoli	cies	√	False						
	Policyldentifier	✓				1.3.171.1.1.10.5.2			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	policyQualifierID	√			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	V				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	√				0.4.0.2042.1.4			
Extended Key	/ Usage	√	False						
	serverAuth	✓			S	True			
	clientAuth	✓			S	True			
	emailProtection	✓			S	False			





3.5.22 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]);





LuxTrust Global Root CA Certificate Specifications

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

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

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

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

Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profile						
Version	<u>.</u>	~	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11"
						SHA256 with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	V			S	LU
	commonName	✓			S	LuxTrust SSL CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	\			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12;24 Months
Subject	•	✓	False			
	countryName			М	D	Country in which the company's or
	(OID: 2.5.4.6)					institution's registered office is
	(5.5.2.0110)	✓				established (as specified in the
						memorandum and articles o
						association). (ISO3166)





SSL	/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	jurisdictionOfIncorporationCountryNa me (OID: 1.3.6.1.4.1.311.60.2.1.3)	√		М	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	√		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdisctionOfIncorporationStateOrPro vinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	√		0	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName (2.5.4.7)	√		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionOfIncorporationLocalityNam e (1.3.6.1.4.1.311.60.2.1.1)	√		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	√		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein







SSI	_/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	businessCategory (OID: 2.5.4.15)	√		M	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	*		М	D	See EV Guidelines [13]: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.
						For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	√		0	D	Number and Street of the physical location of the subject
subjectPublic	KeyInfo	√	False			
	Algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeylo	dentifier	√	False			
	keyldentifier	V				SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfoA	access	✓	False			
	AccessMethod	√				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 29





LuxTrust Global Root CA Certificate Specifications

SS	L/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	AccessMethod	√				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx 17.crt
cRLDistributi	onPoint	✓	False			
	distributionPoint	√			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx 17.crl
Subject						
Properties						
subjectAltNa	me	✓	False			
	SubjectAltName-dNSName	√		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	*		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.







SS	L/TLS Extended Validation	Serve	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exact
						DNS for a Web Server or IP address
		✓				or unique name of server, owned or
		•				controlled by the subject and to be
						associated with the Subject's server.
						Wildcard name not allowed for
						EVCP+ Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exact
						DNS for a Web Server or IP address
		√				or unique name of server, owned or
		•				controlled by the subject and to be
						associated with the Subject's server.
						Wildcard name not allowed for
						EVCP+ Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exact
						DNS for a Web Server or IP address
						or unique name of server, owned or
		✓				controlled by the subject and to be
						associated with the Subject's server.
						Wildcard name not allowed for
						EVCP+ Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exact
						DNS for a Web Server or IP address
						or unique name of server, owned or
		✓				controlled by the subject and to be
						associated with the Subject's server.
						Wildcard name not allowed for
						EVCP+ Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exact
						DNS for a Web Server or IP address
						or unique name of server, owned or
		✓				controlled by the subject and to be
						associated with the Subject's server.
						Wildcard name not allowed for
						EVCP+ Certificates.







SS	L/TLS Extended Validation	Serv	er Cert	ificate	s on S	Secure User Device
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain
						Name) of application/server – Exac
						DNS for a Web Server or IP address
		√				or unique name of server, owned o
						controlled by the subject and to be
						associated with the Subject's server
						Wildcard name not allowed fo
						EVCP+ Certificates.
subjectKeylo	dentifier	√	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four
						bit field with a 0100 value, followed
						by the least significant 60 bits of the
						SHA-1 hash of the value o
						subjectPublicKey bit string (tag, no
						including the length and number o
						unused bit-string bits).
Policy						
Properties keyUsage		✓	True			
Reyosage	digitalSignature	√	Truc		S	True
	alghaioighaiaio					Truc
	nonRepudiation	√			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	√			S	True
	dataEnophomon					Truc
certificatePo	licies	✓	False			
	PolicyIdentifier	√				1.3.171.1.1.10.5.3
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓				ETSI TS 102 042 EVCP+ complian
						certificate signed by a SSL CA. Ke
						generation by the Subscriber or
						Secure Device. Intended to be used
						for authenticating servers accessible
						through the Internet.
	Policyldentifier	√				0.4.0.2042.1.5
Extended Ke	ey Usage	✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False







3.5.23 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>.

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

	Lu	xTrust I	CP Code	Signing (Certificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base Profil	е					
Version		✓	False			
					S	Version 3 Value = "2"
SerialNuml	per	✓	False			
					FDV	Validated on duplicates.
signatureA	lgorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust SSL CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12; 24; 36 months
Subject		✓	False			
	countryName	✓		М	D	Country in which the company's 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





LuxTrust Global Root CA Certificate Specifications

	LuxTrust LCP Code Signing Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
						office is established (as specified in the memorandum and articles of association or an equivalent document)					
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)					
	organizationalUnitName1	✓		0	D	As provided by Subscriber					
	organizationalUnitName2	~		0	D	As provided by Subscriber					
	commonName	√		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)					
	serialNumber	√		0	D	NA or Serial Number as provided by subscriber					
	emailAddress	✓		0	D	Subject's email address if available					
subjectPub	licKeyInfo	✓	False								
	Algorithm	✓				Public Key: Key length: 2048 (RSA); public					
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).					
Extensions	1										
Authority P	roperties										
authorityKe	eyldentifier	✓	False								
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA public key					
authorityInf	foAccess	✓	False								
	AccessMethod	✓				Id-ad-1					
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 29					
	AccessMethod	✓				Id-ad-2					
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx17.crt					
CRLDistrib	utionPoint	✓	False								
	distributionPoint	✓			S						
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx 17.crl					
Subject Pro	operties										
subjectAltN	lame	✓	False								
	Rfc822Name	✓		0	D	Subject's email address					







LuxTrust LCP Code Signing Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
subjectKey	subjectKeyldentifier		False						
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).			
Policy Prop	erties								
keyUsage		✓	True						
	digitalSignature	✓			S	True			
	nonRepudiation	~			Ø	False			
	keyEncipherment	✓			S	False			
	dataEncipherment	~			Ø	False			
certificateP	olicies	✓	False						
	Policyldentifier	~			S	1.3.171.1.1.10.5.4			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	Qualifier	~			S	http://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	√			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on http://repository.luxtrust.lu . Signed by an SSL CA.			
	Policyldentifier	✓			S	0.4.0.2042.1.3			
Extended k	Key Usage	✓	False						
	Object Signing	✓			S	Set			

3.5.24 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., <1.3.171.1.1.10.5.5>.







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

	LuxTrust	e Profile				
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	√	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal		✓	False			Will NOA Encryption.
Signatureval	ue		i aise		D	Issuing CA Signature.
Issuer		✓	False		S	issuing CA Signature.
ISSUEI	countryName	✓	i aise		S	LU
	commonName	✓			S	LuxTrust SSL CA
	organizationName	✓			S	LuxTrust S.A.
Validity	Organizationivame	✓	False		3	Luxitust 3.A.
validity	NotBefore	✓	1 alse		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
	Nobalies					12; 24; 36 Months
Subject		√	False			
	countryName	~		М	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	~		0	D	As provided by Subscriber
	organizationalUnitName 2	✓		0	D	As provided by Subscriber
	commonName	✓		М	D	As provided by Subscriber
	serialNumber	✓		0	D	Serial Number as provided by subscriber
	emailAddress	✓		0	D	Subject's email address
		√				2,2000



LuxTrust Global Root CA Certificate Specifications

	LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
subjectPublic	cKeyInfo	✓	False							
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA)				
	subjectPublicKey	√		М		public exponent: Fermat-4 (=010001).				
Extensions										
Authority										
Properties										
authorityKey	Identifier	✓	False							
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA				
						public key				
authorityInfo		V	False							
	AccessMethod	✓				Id-ad-1				
	accessLocation	√				http://ssl.ocsp.luxtrust.lu 29				
	AccessMethod	√				ld-ad-2				
	accessLocation	√				http://ca.luxtrust.lu/LTSSLCAx ¹⁷ .crt				
cRLDistribut		V	False							
	distributionPoint	√			S	17				
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx 17.crl				
Subject										
Properties		✓								
subjectAltNa		•	False							
	Rfc822Name	✓		0	D	Certificate Holder's email address				
subjectKeylo	lentifier	√	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	T	✓	True							
	digitalSignature				S	True				
		✓								
	nonRepudiation	•			S	False				
		✓				-				
	keyEncipherment				S	True				
	detellarial	✓				Tour				
	dataEncipherment				S	True				
and Carter		✓	F-1-							
certificatePo		· ·	False			4 2 474 4 4 40 5 5				
	PolicyIdentifier	· ·				1.3.171.1.1.10.5.5				
	policyQualifierID	· ·			S	Id-qt-1 (CPS)				
	Qualifier	· ·			S	https://repository.luxtrust.lu				
	policyQualifierID				S	Id-qt-2 (User Notice)				
	noticeNumbers	1								







	LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
	DisplayText	·				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	✓				0.4.0.2042.1.3				
Extended Ke	ey Usage	✓	False							
	serverAuth	✓			S	False				
	clientAuth	✓			S	True				
	emailProtection	✓			S	True				

3.5.25 SSL/TLS QCP-w Extended Validation Server Certificates

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

	SSL/TLS QCP-w Extended Validation Server Certificates								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumber	•	✓	False						
					FDV	Validated on duplicates.			
signatureAlgo	rithm	✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" -			
						SHA256 with RSA Encryption.			
signatureValu	е	√	False						
					D	Issuing CA Signature.			
issuer		√	False		S				
	countryName	√			S	LU			
	commonName	√			S	LuxTrust SSL CA x ¹⁷			
	organizationName	√			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	√			D	Certificate generation process date/time			
						+ 12;24 Months			
subject		✓	False						
	countryName			М	D	Country in which the company's or			
	(OID: 2.5.4.6)					institution's registered office is			
	(0.5. 2.0.7.0)	✓				established (as specified in the			
						memorandum and articles of			
						association). (ISO3166)			







	SSL/TLS QCP-w Ex	ctende	d Valid	dation	Serve	er Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	jurisdictionOfIncorporationCount ryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	√		М	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	√		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdisctionOfIncorporationState OrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	√		0	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName (2.5.4.7)	✓		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionOfIncorporationLocalit yName (1.3.6.1.4.1.311.60.2.1.1)	✓		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	✓		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	√		М	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity







	SSL/TLS QCP-w Ex	ctende	d Valid	dation	Serve	er Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	serialNumber			M	D	See EV Guidelines [13] :
	(OID: 2.5.4.5)	√		IVI	U	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.
						have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	√		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	√		0	D	Number and Street of the physical location of the subject
subjectPublic	KeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeylo	dentifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust SSL CA public key
authorityInfoA	ccess	✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	√				http://ssl.ocsp.luxtrust.lu 29
	AccessMethod	√				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTSSLCAx 17.crt
cRLDistributio	onPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx ¹⁷ .crl
Subject Properties						
subjectAltNan	ne	√	False			







	SSL/TLS QCP-w Ex	ctende	d Valid	lation	Serve	er Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName	*		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique 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.







	SSL/TLS QCP-w Ex	ctende	d Valid	dation	Serve	er Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not
	SubjectAltName-dNSName	√		0		allowed for EV SSL 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
	SubjectAltName-dNSName	✓		0		allowed for EV SSL 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 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.
subjectKeyIde		√	False			
	keyldentifier	v			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
_	digitalSignature	√			S	True
	nonRepudiation	√			S	False
	keyEncipherment	√			S	True
	dataEncipherment	✓			S	False
certificatePolic	cies	✓	False			







	SSL/TLS QCP-w	Extende	ed Valid	dation	Serve	er Certificates
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	Policyldentifier	✓				
						1.3.171.1.1.10.5.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	✓				
						0.4.0.194112.1.4
	Policyldentifier	✓				0.4.0.2042.1.5
Extended Ke	y Usage	✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False
QualifiedCert	tificateStat	~	False			
	QcCompliance	√		М	S	True
	(0.4.0.1862.1.1)					
	QcPDS	√		М	S	https://www.luxtrust.lu/upload/data/repos
	(0.4.0.1862.1.5)					itory/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		М	S	id-etsi-qct-web
						(0.4.0.1862.1.6.3)

3.5.26 LuxTrust SPARE Signing Server LCP Certificate Profile

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

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

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

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







Attribute	Field	IN ¹⁸	CE ¹⁹	O/M ²⁰	CO ²¹	Value
signatureAlgorithm		√	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256
						with RSA Encryption.
signatureValue		√	False			
					D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	√			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x
	organizationName	√			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36 Months
Subject		√	False			
	serialNumber	√		М	D	Serial Number as constructed by LRAO
	commonName	*		М	D	LGQCA XX CSS (XX a number selected internally by LuxTrust) or Concatenation of given name(s) and surname(s) separated by a "Space" character.
	givenName	✓		М	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s) as on IL document
	Surname	✓		М	D	CSS or Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	√		М	D	LU or Nationality of holder (ISO3166)
	emailAddress	✓		0	D	N/A
	Title	√		М	D	Private Person
subjectPublic	KeyInfo	✓	False			





	SPARI	E LuxTru	ıst Signin	g Server L0	CP Certific	ate Profile
Attribute	Field	IN ¹⁸	CE ¹⁹	O/M ²⁰	CO ²¹	Value
	Algorithm	√				Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	√		М		public exponent. Fernal-4 (-010001).
Extensions						
Authority Properties						
authorityKeylde	ntifier	√	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfoAcc	authorityInfoAccess		False			
	AccessMethod	√				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ²² .crt
	AccessMethod	√				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ²³
cRLDistributionF	Point	√	False			
	distributionPoint	√			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ²² .crl
Subject Properties						
subjectAltName		√	False			
	Rfc822Name	√		0	D	N/A
subjectKeyldent	ifier	√	False			
	keyldentifier	V			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						







	SPARE LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN ¹⁸	CE ¹⁹	O/M ²⁰	CO ²¹	Value				
keyUsage		√	True							
	digitalSignature	~			S	True				
certificatePolicie	es	√	False							
	Policyldentifier	√				1.3.171.1.1.10.3.20				
	policyQualifierID	√			S	Id-qt-1 (CPS)				
	Qualifier	√			S	https://repository.luxtrust.lu				
	policyQualifierID	√			S	Id-qt-2 (User Notice)				
	DisplayText	✓				LuxTrust SPARE Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity Auth.				
	Policyldentifier	√				0.4.0.2042.1.3				

3.5.27 LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature

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

This profile aims at issuing qualified electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified eseals supported by Qualified Certificate compliant with ETSI EN 319 411-2 [20] QCP-I-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.21>.

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



		LuxTı	rust Qı	ıalified	eSEAL	. Certificate Profile
Attribute	Field	IN ³⁰	CE ³¹	O/M ³²	CO33	Value
Base						
Profile						
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 Global Qualified CA x ³⁴
	organizationName	√			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)

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



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

 $^{^{31}}$ CE = Critical Extension.

³² O/M: O = Optional, M = Mandatory.

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





İ						
	organisationIdentifier (2.5.4.97)	✓		М	О	Shall contain information using the following structure in the presented order: - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	√		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
	serialNumber	√		М	D	Serial Number as constructed by LRAO
subjectPublic	-	√	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public
	subjectPublicKey	٧		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties	lde atten	√	F .			
authorityKey		V	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		∨	False			
	AccessMethod					ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt





VFRSION 1 24

	AccessMethod	✓				Id-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ³⁵
cRLDistribut		√	False			Thips://goa.ooop.iaxa.goa.ia/
OI (EDISTIDA	distributionPoint	√	1 disc		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx17.crl
Cubicot	iuiiivaiiie					TILLD.//CIT.luxtirust.lu/ETGQCAXT7.CIT
Subject						
Properties	dan###	√	F-I			
subjectKeylo		/	False		F	T. 14 11 115 6 111 5 11 111 0400
	keyldentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100
						value, followed by the least significant 60 bits of the SHA-1
						hash of the value or subjectPublicKey bit string (tag, not
						including the length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		√	True			
	digitalSignature	√			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	√			S	False
certificatePo	licies	✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.21
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	√				0.4.0.194112.1.3
QualifiedCe		√	False			
	QcCompliance (0.4.0.1862.1.1)	✓		М	S	True
	QcSSCD (0.4.0.1862.1.4)	V		М	S	True
	QcPDS (0.4.0.1862.1.5)	*		M	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType	✓		М	S	id-etsi-qct-eseal

³⁵ SINCE LTGQCA3





VERSION 1.24

3.5.28 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

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

	Lu	xTrust	NCP+	Certific	ate Pr	ofile for authentication
Attribute	Field	IN ³⁶	CE ³⁷	O/M ³⁸	CO ³⁹	Value
Base Profile						
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 Global Qualified CA x ⁴⁰
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)

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



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

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

³⁸ O/M: O = Optional, M = Mandatory.

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





	organisationIdentifier (2.5.4.97)	✓		Σ	D	Shall contain information using the following structure in the presented order: - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
	serialNumber	√		М	D	Serial Number as constructed by LRAO
subjectPublic	KeyInfo	√	False			
	Algorithm	*				Public Key: Key length: 2048bit up to 4096bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	dentifier	√	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	\	False			
	AccessMethod	V				ld-ad-2
•		✓				





VERSION 1.24

cRLDistributionPoint	essLocation				Id-ad-1
cRLDistributionPoint distribut fullNa Subject Properties subjectKeyldentifier keylden Policy	sslocation				
distribut fullNa Subject Properties subjectKeyldentifier keylden Policy					http://qca.ocsp.luxtrust.lu/ ⁴¹
Subject Properties subjectKeyldentifier keylden	✓	False			
Subject Properties subjectKeyldentifier keylden	tionPoint			S	
Properties subjectKeyldentifier keylden Policy	ame				http://crl.luxtrust.lu/LTGQCAx17.crl
subjectKeyIdentifier keyIden					
Policy	√	False			
	ntifier 🗸		Fi	ixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
keyUsage	✓	True			
digitalS	ignature 🗸			S	True
nonRep	oudiation			S	False
keyEnc	ipherment			S	True
dataEnd	cipherment			S	False
certificatePolicies	✓	False			
Policyld	dentifier				1.3.171.1.1.10.3.22
policyQ	ualifierID			S	Id-qt-1 (CPS)
qualifier				S	https://repository.luxtrust.lu
policyQ	ualifierID			S	Id-qt-2 (User Notice)
Policyld	lentifier 🗸				0.4.0.2042.1.2

3.5.29 LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature

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





		LuxTr	ust Ad	vanced	eSEAL	Certificate Profile
Attribute	Field	IN ⁴²	CE ⁴³	O/M ⁴⁴	CO ⁴⁵	Value
Base						
Profile						
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 Global Qualified CA x ⁴⁶
	organizationName	✓			S	LuxTrust S.A.
Validity	1	✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)

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



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

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

⁴⁴ O/M: O = Optional, M = Mandatory.

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



	organisationIdentifier (2.5.4.97)	>		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
	serialNumber	√		M	D	Serial Number as constructed by LRAO
subjectPubli	cKeyInfo	√	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	dentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			
,	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	√				Id-ad-1
	Accessivieurou					lu-au-1





VERSION 1 24

	accessLocation	√			http://qca.ocsp.luxtrust.lu/ ⁴⁷
cRLDistribut	tionPoint	✓	False		
	distributionPoint	√		S	
	fullName	√			http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties					
subjectKeyl	dentifier	✓	False		
	keyldentifier	*		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties					
keyUsage		✓	True		
	digitalSignature	✓		S	False
	nonRepudiation	~		S	True
	keyEncipherment	✓		S	False
	dataEncipherment	√		S	False
certificatePo	olicies	√	False		
	Policyldentifier	√			1.3.171.1.1.10.3.23
	policyQualifierID	√		S	Id-qt-1 (CPS)
	qualifier	√		S	https://repository.luxtrust.lu
	policyQualifierID	√		S	Id-qt-2 (User Notice)
	Policyldentifier	√			0.4.0.2042.1.2

3.5.30 LuxTrust Advanced eSEAL - Certificate Profile supporting authentication

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





		LuxTr	ust Ad	vanced	eSEAL	Certificate Profile
Attribute	Field	IN ⁴⁸	CE ⁴⁹	O/M ⁵⁰	CO ⁵¹	Value
Base						
Profile						
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 Global Qualified CA x ⁵²
	organizationName	✓			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)

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



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

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

⁵⁰ O/M: O = Optional, M = Mandatory.

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



	organisationIdentifier (2.5.4.97)	✓		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	√		0	D	Company/institution department or other information item
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
subjectPubli	cKeyInfo	✓	False			
	Algorithm	\				Public Key: Key length: 2048bit up to 4096bit (RSA); public
	subjectPublicKey	\		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	•	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	Accessiviculou					14-44-1





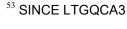
VERSION 1.24

	accessLocation	√			http://gca.ocsp.luxtrust.lu/ ⁵³
cRLDistributi	onPoint	√	False		
	distributionPoint	√		S	
	fullName	√			http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties					
subjectKeyId	 lentifier	√	False		
	keyldentifier	✓		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties					
keyUsage		√	True		
	digitalSignature	√		S	True
	nonRepudiation	√		S	False
	keyEncipherment	√		S	True
	dataEncipherment	✓		S	False
certificatePol	licies	✓	False		
	PolicyIdentifier	~			1.3.171.1.1.10.3.24
	policyQualifierID	✓		S	Id-qt-1 (CPS)
-	qualifier	√		S	https://repository.luxtrust.lu
	policyQualifierID	√		S	Id-qt-2 (User Notice)
	Policyldentifier	√			0.4.0.2042.1.2

3.5.31 LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature

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

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





	Lux	Trust Ac	dvance	d Autoi	mated	eSEAL Certificate Profile
Attribute	Field	IN ⁵⁴	CE ⁵⁵	O/M ⁵⁶	CO ⁵⁷	Value
Base						
Profile						
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.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁵⁸
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 24 Months
Subject		√	False			
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).
countryName ✓		✓		М	D	the country in which the subject (legal person) is established (ISO3166)

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



 $^{^{54}\,\}mathrm{IN}$ = Included: Attribute / field included within the certify cate profile.

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

⁵⁶ O/M: O = Optional, M = Mandatory.

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



	organisationIdentifier (2.5.4.97)	*		M	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier. Shall contain the full registered name of the subject (legal
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
subjectPubli	cKeyInfo	√	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	√	False			
	AccessMethod	√				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
		<u> </u>	<u> </u>	<u> </u>	1	





		1 .	1	1	1	
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ⁵⁹
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject						
Properties						
subjectKeyle	subjectKeyldentifier		False			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100
						value, followed by the least significant 60 bits of the SHA-1
						hash of the value or subjectPublicKey bit string (tag, not
						including the length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		√	True			
	digitalSignature	✓			S	False
	nonRepudiation	√			S	True
	keyEncipherment	√			S	False
	dataEncipherment	√			S	False
certificatePo	olicies	√	False			
	Policyldentifier	√				
						1.3.171.1.1.10.3.25
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

⁵⁹ SINCE LTGQCA3







VFRSION 1 24

3.5.32 LuxTrust Smart Card QCP-n-qscd Certificate Profile

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

	LuxTrust Smart Card QCP-n-qscd Certificate Profile										
Attribute	Field	IN ⁶⁰	CE ⁶¹	O/M ⁶²	CO 63	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								
					FDV	Validated on duplicates.					
signatureA	lgorithm	√	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureV	alue alue	√	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	√			S	LuxTrust Global Qualified CA x ⁶⁴					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	√			D	Certificate generation process date/time.					
	NotAfter	✓			D	Certificate generation process date/time + 36 Months					
Subject		√	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.					
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) as on ID card					
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)					
	countryName	✓		М	D	Nationality of holder (ISO3166)					
	emailAddress	✓		М	D	Subject's email address					

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



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

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

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

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





	LuxTr	ıst Sı	mart C	ard QC	P-n-	qscd Certificate Profile
Attribute	Field	IN ⁶⁰	CE ⁶¹	O/M ⁶²	CO 63	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	√		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	√		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitN ame 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).
	organizationalUnitN ame 2	√		0	D	PRO products only: Company/institution department or other information item
subjectPub	licKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent:
	subjectPublicKey	✓		М		Fermat-4 (=010001).
Extensio ns						
Authority Propertie s						
authorityKe	eyldentifier	√	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	foAccess	V	False			
	AccessMethod	V				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	V				ld-ad-1
	accessLocation	V				http://qca.ocsp.luxtrust.lu/ ⁶⁵
cRLDistrib	utionPoint	✓	False			

⁶⁵ SINCE LTGQCA3







	LuxTrust Smart Card QCP-n-qscd Certificate Profile										
Attribute	Field	IN ⁶⁰	CE ⁶¹	O/M ⁶²	CO 63	Value					
	distributionPoint	✓			S						
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl					
Subject Propertie s											
subjectAltN	lame	✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKey	dentifier	✓	False								
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).					
Policy Propertie s											
keyUsage		✓	True								
	digitalSignature	√			S	False					
	nonRepudiation	√			S	True					
	keyEncipherment	√			S	False					
	dataEncipherment	✓			S	False					
certificateF	Policies	√	False								
	Policyldentifier	√				1.3.171.1.10.3.26					
	policyQualifierID	√			S	Id-qt-1 (CPS)					
	qualifier	√			S	https://repository.luxtrust.lu					
	policyQualifierID	√			S	Id-qt-2 (User Notice)					
	Policyldentifier	✓				0.4.0.194112.1.2					
QualifiedC	ertificateStat	√	False								
	QcCompliance (0.4.0.1862.1.1)	√		М	S	True					
	QcSSCD (0.4.0.1862.1.4)			М	S	True					
	QcPDS (0.4.0.1862.1.5)	√		М	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf					
	QcType (0.4.0.1862.1.6)	√		М	S	id-etsi-qct-esign					







VFRSION 1 24

3.5.33 LuxTrust Smart Card NCP+ Certificate Profile

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

	Lux	kTru:	st Sma	rt Card	NCP+ Ce	ertificate Profile
Attribute	Field	IN 66	CE ⁶⁷	O/M ⁶⁸	CO ⁶⁹	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False			
					FDV	Validated on duplicates.
signatureA	Igorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureV	alue	✓	False			
					D	Issuing CA Signature.
Issuer		√	False		S	
	countryName	✓			S	LU
	commonName	√			S	LuxTrust Global Qualified CA x ⁷⁰
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36 Months
Subject	l	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	~		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	√		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		М	D	Subject's email address

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

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



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

⁶⁸ O/M: O = Optional, M = Mandatory.

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





	Lux	Trus	st Sma	rt Card	NCP+ Ce	rtificate Profile
Attribute	Field	IN 66	CE ⁶⁷	O/M ⁶⁸	CO ⁶⁹	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	✓		M	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	√		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitN ame 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).
	organizationalUnitN ame 2	✓		0	D	PRO products only: Company/institution department or other information item
subjectPub	olicKeyInfo	√	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions Authority Propertiens						
authorityKe	eyldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	foAccess	√	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ⁷¹

⁷¹ SINCE LTGQCA3







	Lux	cTru:	st Sma	rt Card		ertificate Profile
Attribute	Field	IN 66	CE ⁶⁷	O/M ⁶⁸	CO ⁶⁹	Value
cRLDistrib	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Propertie						
s						
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	dentifier	✓	False			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value o subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		✓	True			
	digitalSignature	√			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificateP	Policies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.27
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	V				0.4.0.2042.1.2

3.5.34 LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature

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

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





signatureValue		LuxTrust Smar	t Car	d LORA	NCP+	- Sign	ature Certificate Profile
Profile Pro	Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Version	Base						
	Profile						
SerialNumber	Version		✓	False			
False Fiber Fib						S	Version 3 Value = "2"
signatureAlgorithm Algorithm Algorit	SerialNumbe	r	✓	False			
Algorithm Faise S						FDV	Validated on duplicates.
SignatureValue	signatureAlge	orithm	✓	False			
Signature		Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
Issuer							Encryption.
	signatureVal	ue	✓	False			
countryName						D	Issuing CA Signature.
CountryName	Issuer			False		S	
CommonName		countryName	✓			S	LU
Validity		commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
NotBefore Y		organizationName	✓			S	LuxTrust S.A.
NotAfter NotAfter V False Subject SerialNumber Subject SerialNumber M D SerialNumber as constructed by LRAO Concatenation of given name(s) and sumame(s) and no ID card separated by a "Space" character. Given name(s) as on ID card Sumame Sumame M D Given name(s) as on ID card without indication name(s) Sumame Sumame(s) as on ID card without indication name(s) Sumame(s) as on ID card without	Validity		✓	False			
Subject Subject Subje		NotBefore	✓			D	Certificate generation process date/time.
serialNumber		NotAfter	✓			D	Certificate generation process date/time + 36 Months
commonName M	Subject		✓	False			
commonName M		serialNumber	✓		М	D	Serial Number as constructed by LRAO
Surname		commonName	✓		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
Surname M D "épouse", "ép." or similar and the subsequer name(s)		givenName	✓		М	D	Given name(s) as on ID card
emailAddress		Surname	✓		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
Title		countryName	✓		М	D	Nationality of holder (ISO3166)
organizationName M		emailAddress	✓		0	D	Subject's email address
localityName organizationalUnitName 1 organizationalUnitName 2 M D RA code Constructed by LuxTrust Algorithm Algorithm subjectPublicKey M D RAC code Constructed by LuxTrust Public Key: Key length: 2048bit (RSA); public subjectPublicKey exponent: Fermat-4 (=010001).		Title	✓		М	D	"LuxTrust RA Officer"
organizationalUnitName 1 organizationalUnitName 2 M D RA code Constructed by LuxTrust RAO code Constructed by LuxTrust subjectPublicKeyInfo False Algorithm SubjectPublicKey M Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).		organizationName	✓		М	D	Constructed by LuxTrust
The subject Public Key Info Algorithm Subject Public Key M D RA code Constructed by Lux Trust M D RAO code Constructed by Lux Trust False Public Key: Key length: 2048bit (RSA); public subject Public Key Exponent: Fermat-4 (=010001).		localityName	✓		М	D	Country of RA
subjectPublicKeyInfo Algorithm SubjectPublicKey M D RAO code Constructed by LuxTrust Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).			✓		М	D	RA code Constructed by LuxTrust
Algorithm Algorithm SubjectPublicKey M Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).			✓		М	D	RAO code Constructed by LuxTrust
subjectPublicKey M exponent: Fermat-4 (=010001).	subjectPublic	KeyInfo	✓	False			
subjectPublicKey M exponent: Fermat-4 (=010001).		_	✓				Public Key: Key length: 2048bit (RSA); public
			✓		М		•
EXCENSIONS	Extensions						





Attribute	Field	IN13	CE ¹⁴	O/M ¹⁵	CO16	Value
Authority	110.0			G/III		Value
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified C.
						public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	1	✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with
						0100 value, followed by the least significant 60 bits
						the SHA-1 hash of the value or subjectPublicKey b
						string (tag, not including the length and number
						unused bit-string bits).
Policy						
Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo	-	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.28
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2







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

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

	LuxTrust Smart C	Card	LORA	NCP+	- auther	ntication Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version	1	✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er T	✓	False			
		✓			FDV	Validated on duplicates.
signatureAlg		· ·	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	-	✓				Encryption.
signatureVa	lue T	•	False		_	
		✓			D	Issuing CA Signature.
Issuer		· ·	False		S	
	countryName	· ·			S	LU LuxTrust Global Qualified CA x ¹⁷
	commonName	√			S	
\/alidih:	organizationName	√	False		S	LuxTrust S.A.
Validity	NotBefore	✓	raise		D	Cartificate generation process data/time
	NotAfter	√			D	Certificate generation process date/time. Certificate generation process date/time + 36 Months
Subject	NotAitei	√	False		D	Certificate generation process date/time + 30 Months
Gubject	a a dalbh mah a a	√	1 alse			Optical Number of a second set of the URAC
	serialNumber	· ·		М	D	Serial Number as constructed by LRAO
	commonName	√		М	D	Concatenation of given name(s) and surname(s) as
	Commonwame			IVI		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	~		М	D	Country of RA
	organizationalUnitName	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName	~		М	D	RAO code Constructed by LuxTrust





	Lux Trust Smart	Card	LORA	NCP+	- authe	ntication Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); pub
	subjectPublicKey	~		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified (
						public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties						
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	1	✓	False			
,	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with
	,					0100 value, followed by the least significant 60 bits
						the SHA-1 hash of the value or subjectPublicKey
						string (tag, not including the length and number
						unused bit-string bits).
Policy						and the same grant,
Properties						
keyUsage		√	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	√			S	False
certificatePo		√	False		3	1 GISC
oei iiiicaleru	Policyldentifier	✓	1 0150			1.3.171.1.1.10.3.29
		√			-	
	policyQualifierID	· ·			S	Id-qt-1 (CPS)
	Qualifier	· ·			S	https://repository.luxtrust.lu
	policyQualifierID	· ·			S	Id-qt-2 (User Notice)
	PolicyIdentifier	V				0.4.0.2042.1.2







VFRSION 1 24

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

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

	LuxTrust	eID Sn	nart Ca	ard Q0	CP-n-q	scd Certificate Profile
Attribute	Field	IN ⁷²	CE ⁷³	O/M 74	CO ⁷⁵	Value
Base						
Profile						
Version		✓	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	lue	✓	False			
					D	Issuing CA Signature.
Issuer	T	V	False		S	
	countryName	✓			S	LU
	commonName	V			S	LuxTrust Global Qualified CA x ⁷⁶
	organizationName	✓			S	LuxTrust S.A.
Validity	1	V	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + maximum
						120 Months;
						Certificate generation process date/time + 1 day for
		✓				PSEUDONYM Certificate
Subject	T		False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	√		М	D	Concatenation of given name(s) and surname(s)
	Commonwante			101		separated by the space character
	givenName	✓		М	D	Given name(s) as on ID card or as provided by the
						RNCID
						Surname(s) as on ID card without indication "épouse",
	Surname	✓		М	D	"ép." or similar and the subsequent name(s) or as
						provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	√		0	D	Subject's email address

 $^{^{72}}$ IN = Included: Attribute / field included within the certificate profile.

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



 $^{^{73}}$ CE = Critical Extension.

 $^{^{74}}$ O/M: O = Optional, M = Mandatory.

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



	LuxTrust e			ard QC		scd Certificate Profile
Attribute	Field	IN ⁷²	CE ⁷³	O/M 74	CO ⁷⁵	Value
	Title	✓		М	D	"Private Person"
	organizationalUnitName	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date o birth + 18 years).
subjectPubl	licKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extension s						
Authority Properties						
authorityKe	yldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfo	oAccess	√	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribu	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Properties						
subjectAltN	ame	✓	False			
	Rfc822Name	✓		0	D	Subject email address
subjectKeyl	dentifier	√	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓	<u> </u>		S	False
certificatePo	olicies	✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.30
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)





VFRSION 1 24

	LuxTrust	eID Sn	nart Ca	rd Q0	CP-n-q	scd Certificate Profile
Attribute	Field	IN ⁷²	CE ⁷³	O/M 74	CO ⁷⁵	Value
	Policyldentifier	✓				0.4.0.194112.1.2
QualifiedCe	ertificateStat	✓	False			
	QcCompliance	✓		М	S	
	(0.4.0.1862.1.1)					True
	QcSSCD	✓		М	S	True
	(0.4.0.1862.1.4)					
	QcPDS	✓		М	S	https://www.luxtrust.lu/upload/data/repository/PD
	(0.4.0.1862.1.5)					S.pdf
	QcType (0.4.0.1862.1.6)	*		М	S	id-etsi-qct-esign

3.5.37 NCP+ supporting Authentication & Encryption for eID smart cards

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

	LuxTrus	t eID S	mart c	ard N	CP+ C	ertificate Profile
Attribute	Field	IN ⁷⁷	CE ⁷⁸	O/M 79	CO ₈₀	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	SerialNumber		False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
						Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	√			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁸¹
	organizationName	√			S	LuxTrust S.A.

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

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



 $^{^{78}\,\}mathrm{CE}$ = Critical Extension.

⁷⁹ O/M: O = Optional, M = Mandatory.

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



Attribute	Field	IN ⁷⁷	CE ⁷⁸	O/M	CO ₈₀	Value
Allribute	Field	IIN	CE	79		value
Validity	I.	√	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + maximu
						120 Months;
						Certificate generation process date/time + 1 day PSEUDONYM Certificate
Subject		√	False			1 GEOSTINI GSTAIRGANG
-	serialNumber	√		М	D	Serial Number as constructed by LRAO
						Concatenation of given name(s) and surname
	commonName	✓		М	D	separated by the space character
	givenName	✓		М	D	Given name(s) as on ID card or as provided by RNCID
	Surname	√		М	_	Surname(s) as on ID card without indication "épous
	Surname			IVI	D	"ép." or similar and the subsequent name(s) or provided by the RNCID
	countryNome	✓		М	D	LU
	countryName	,		IVI	Ь	
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"Private Person"
	organizationalUnitName					If the holder is underage: "Mineur jusqu'à : " & (Date
	1	√		0	D	birth + 18 years).
subjectPubli	cKeyInfo	✓	False			
•	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RS.
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	Identifier	√	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInfo	Access	√	False			
	AccessMethod	√				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut		√	False			
	distributionPoint	√			S	17
	fullName	√				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Properties		✓				







	LuxTrus	t eID S	mart c	ard N	CP+ C	ertificate Profile
Attribute	Field	IN ⁷⁷	CE ⁷⁸	O/M 79	CO ⁸⁰	Value
	Rfc822Name	✓		0	D	Subject email address
subjectKeylo	dentifier	√	False			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100
						value, followed by the least significant 60 bits of the
						SHA-1 hash of the value or subjectPublicKey bit string
						(tag, not including the length and number of unused
						bit-string bits).
Policy						
Properties						
keyUsage		✓	True			
	digitalSignature	√			S	True
	nonRepudiation	√			S	False
	keyEncipherment	√			S	True
	dataEncipherment	√			S	False
certificatePo	licies	√	False			
	PolicyIdentifier	√				1.3.171.1.1.10.3.31
	policyQualifierID	√			S	Id-qt-1 (CPS)
	Qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	PolicyIdentifier	√				0.4.0.2042.1.2

3.5.38 LuxTrust Signing Server QCP-n-qscd Certificate Profile

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

	LuxTrust Si	gning	Serve	r QCP	-n-qsc	d Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M¹	CO ¹⁶	Value
				5		
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	√	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	√	False			
	algorithm				S	
						OID = "1.2.840.113549.1.1.11" - if SHA256 with
						RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	







	LuxTrust S	igning	Serve	r QCP	-n-qsc	d Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹	CO ¹⁶	Value
	countryName	√			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ¹⁷
	organizationName	√			S	LuxTrust S.A.
Validity	•	√	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 3 Months
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID car separated by a "Space" character
	givenName	~		М	D	PRO and PRIVATE products: Given name(s) a on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as 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 purpos certificates)
	organizationName	V		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	D	PRO products only: Company/institution country of HQ (as in articles of association)







	LuxTrust Signature	gning	Serve	r QCP	-n-qsc	d Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M¹ 5	CO ¹⁶	Value
	organizationalUnitName 1	√		M for PRO prod ., cond i-tiona I (O) for PRI V prod .)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName	✓		0	D	PRO products only: Company/institution department or other information item
subjectPubli	-Kevinfo	✓	False			
Subjecti ubii	algorithm	✓	1 alse			Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						process process and the control of t
Authority Properties						
authorityKey	Identifier	✓	False			
•	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl
Subject Properties						
subjectAltNa	me	√	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	lentifier	✓	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).







	LuxTrust Signing Server QCP-n-qscd Certificate Profile								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹	CO ¹⁶	Value			
Policy Properties									
keyUsage		√	True						
	digitalSignature	~			S	True			
	nonRepudiation				S	True			
	keyEncipherment	√			S	True			
	dataEncipherment	✓			S	False			
certificatePolicies		√	False						
	PolicyIdentifier	√				1.3.171.1.1.10.3.32			
	policyQualifierID	√			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	PolicyIdentifier	✓				0.4.0.194112.1.2			
QualifiedCertificateStat		✓	False						
	QcCompliance (0.4.0.1862.1.1)	√		М	S	True			
	QcSSCD (0.4.0.1862.1.4)	√		М	S	True			
	QcPDS (0.4.0.1862.1.5)	V		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf			
	QcType (0.4.0.1862.1.6)	√		М	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)			

3.5.39 LuxTrust Signing Server QCP-l-qscd Certificate Profile

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

LuxTrust Signing Server QCP-I-qscd Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value				
Base										
Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumber		✓	False							





VFRSION 1 24

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







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





	LuxTrust	Signin	g Serv	er QCF	-l-qsc	d Certificate Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA)
	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).
Extension						
s						
Authority						
Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√	1			Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ ¹⁸
cRLDistribut		✓	False			
	distributionPoint	√			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCA ¹⁷ .crl
Subject	Tamvarro					THE PROPERTY OF THE PROPERTY O
Properties						
subjectKeylo	dentifier	√	False			
Subjectivelyi	keyldentifier	✓	1 alse		Fixed	The Key Identifier comprises a four-bit field with a
	Regidentine				Tixeu	0100 value, followed by the least significant 60 bits
						of the SHA-1 hash of the value of
						subjectPublicKey bit string (tag, not including the
						length and number of unused bit-string bits).
Policy						longer and number of anasca sit saming sits).
Properties						
•		/	Truo			
keyUsage	digitalSignature	-	True		S	True
	digitaiSignature				5	True
	Ddl-dl				0	F.II.
	nonRepudiation	✓			S	False
	keyEncipherment	· ✓			S	False
	dataEncipherment	<i>'</i>			S	False
certificatePo	1	· ·	False			
	Policyldentifier	•				
						1.3.171.1.10.3.33
		✓	-			
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier		1		S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.194112.1.3
Qualifie	l dCertificateStat	✓	False			
	QcCompliance	✓		M	S	True
	(0.4.0.1862.1.1)			1**		1.43







	LuxTrust Signing Server QCP-l-qscd Certificate Profile										
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value					
	QcSSCD (0.4.0.1862.1.4)	√		М	S	True					
	QcPDS (0.4.0.1862.1.5)		√		S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf					
	QcType (0.4.0.1862.1.6)	√		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)					

3.5.40 LuxTrust Signing Stick QCP-n-qscd certificate profile

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

	LuxTru	st Sig	ning S	tick Q	CP-n-	qscd Certificate Profile
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value
Base Profile						
Version		√	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False			
					FDV	Validated on duplicates.
signatureA	lgorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	~			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁸⁶
	organizationName	~			S	LuxTrust S.A.
Validity		√	False			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36 Months
Subject		√	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO

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



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

 $^{^{83}}$ CE = Critical Extension.

⁸⁴ O/M: O = Optional, M = Mandatory.

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





	LuxTrus	st Sig	ning S	tick Q0	CP-n-	qscd Certificate Profile
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	со	Value
					85	
	commonName	√		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	~		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	√		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitN ame 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).
	organizationalUnitN ame 2	~		0	D	PRO products only: Company/institution department or other information item
subjectPub	licKeyInfo	V	False			
	Algorithm	√				Public Key: Key length: 2048bit (RSA); public exponent:
	subjectPublicKey	√		M		Fermat-4 (=010001).
Extensio ns						
Authority						
Propertie s						







	LuxTru	st Sig	ning S	tick Q	CP-n-	qscd Certificate Profile
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value
authorityKe	eyldentifier	√	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	l foAccess	√	False			
	AccessMethod	√				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/87
cRLDistribu	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject Propertie s		√				
subjectAltN	l	V	False			
	Rfc822Name	V ✓		0	D	Certificate Holder's email address
subjectKey	Identifier keyldentifier	V	False		Fixed	The Key Identifier comprises a four-bit field with a 0100
Policy	·					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).
Propertie s						
keyUsage	,	V	True			
	digitalSignature	✓			S	False
	nonRepudiation	V			S	True
	keyEncipherment	✓			S	False
_	dataEncipherment	V			S	False
certificateP	ı	✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.34
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	V			S	Id-qt-2 (User Notice)
	PolicyIdentifier	✓				0.4.0.194112.1.2
QualifiedCe	ertificateStat	√	False			
	QcCompliance (0.4.0.1862.1.1)	√		М	S	True
	QcSSCD (0.4.0.1862.1.4)			М	S	True

⁸⁷ SINCE LTGQCA3







	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribute	Field	IN ⁸²	CE ⁸³	O/M ⁸⁴	CO 85	Value					
	QcPDS (0.4.0.1862.1.5)	√		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf					
	QcType (0.4.0.1862.1.6)	√		М	S	id-etsi-qct-esign					

3.5.41 LuxTrust Signing Stick NCP+ Certificate Profile

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

	Lux	Trus	t Signi	ng Stick	NCP+ Ce	ertificate Profile
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	CO ⁹¹	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNuml	ber	√	False			
					FDV	Validated on duplicates.
signatureA	lgorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x ⁹²
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO

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

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



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

⁹⁰ O/M: O = Optional, M = Mandatory.

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





	Lux1	rus	t Signi	ng Stick	NCP+ Ce	ertificate Profile
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	CO ⁹¹	Value
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	√		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	✓		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitN ame 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).
	organizationalUnitN ame 2	✓		0	D	PRO products only: Company/institution department or other information item
subjectPub	1	√	False			
	Algorithm	✓ ✓				Public Key: Key length: 2048bit (RSA); public
Extensio ns	subjectPublicKey	-		M		exponent: Fermat-4 (=010001).







	Lux	Γrus	t Signi	ng Stick	NCP+ C	ertificate Profile
Attribute	Field	IN 88	CE ⁸⁹	O/M ⁹⁰	CO ⁹¹	Value
Authority						
Propertie						
S						
authorityKe	yldentifier	√	False			
	keyldentifier	\				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	oAccess	✓	False			
	AccessMethod	√				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx ¹⁷ .crt
	AccessMethod	√				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/93
cRLDistribu	rtionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx ¹⁷ .crl
Subject						
Propertie						
s						
subjectAltN	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	Identifier	√	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a
						0100 value, followed by the least significant 60 bits
						of the SHA-1 hash of the value or
						subjectPublicKey bit string (tag, not including the
						length and number of unused bit-string bits).
Policy						
Propertie						
S						
keyUsage		V	True			
	digitalSignature	√			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificateP	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.35
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	√				0.4.0.2042.1.2

⁹³ SINCE LTGQCA3







3.6 Timestamping Certificate Profile

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

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

	LuxTrus	t Time	stampi	ng Cer	tificat	e Profile
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		√	False			
					S	Version 3 Value = "2"
SerialNumbe	er -	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	√	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
issuer		√	False		S	
	countryName	√			S	LU
	commonName	✓			S	LuxTrust Global Timestamping CA x ¹⁷
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						60 Months
subject	I	✓	False			
	commonName	✓		М	D	tts.luxtrust.lu
	localityName	✓		М	D	Capellen
	organizationName	✓		М	D	LuxTrust S.A.
	organizationalUnitName 1	✓		М	D	PKI Entity
	countryName	✓		0	D	LU
subjectPublic	cKeyInfo	√	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	Identifier	✓	False			





LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
	keyldentifier	✓				SHA-1 Hash of the LuxTrus			
						Timestamping CA public key			
authorityInfo	Access	√	False						
	AccessMethod	✓				ld-ad-2			
	accessLocation	✓				http://ca.luxtrust.lu/LTGTSACAx17.crt			
	AccessMethod	✓				ld-ad-1			
	accessLocation	√				http://ocsp.luxtrust.lu			
cRLDistribut	ionPoint	✓	False						
	distributionPoint	√			S				
	fullName	✓				http://crl.luxtrust.lu/LTGTSACAx ¹⁷ .crl			
Subject									
Properties									
subjectAltNa	ame	✓	False						
,	Rfc822Name	√		0	D	info@luxtrust.lu			
subjectKeylo		✓	False		_				
	keyldentifier	✓	. 4.55		Fixed	The Key Identifier comprises a four-b			
	Royldonanoi				I IXCC	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						of unused bit-string bits).			
Properties									
keyUsage		√	True						
Reyosage	digitalSignature	√	Tiue		S	True			
	nonRepudiation	✓			S	False			
	·	✓							
	keyEncipherment	√			S	False			
-	dataEncipherment	√			S	False			
Extended Ke		· ·	False		_				
	TimeStamping				S	Set			
	(1.3.6.1.5.5.7.3.8)	✓							
Private Key	Usage Period		False						
	Usage period (2.5.29.16)			М	D	Certificate generation process date/time			
						12 Months			
certificatePo	licies	√	False						
	Policyldentifier	√				1.3.171.1.1.10.8.1			
	policyQualifierID	√			S	Id-qt-1 (CPS)			
	qualifier	√			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	√				LuxTrust LCP certificate compliant wit			
						ETSI TS 102 042. Sole authorised usage			
						Signature of LuxTrust Trusted Time Stam			
						tokens generated by LuxTrust time			
						stamping authority.			
	Policyldentifier	✓	 			0.4.0.2042.1.3			









3.6.1 Normalized Certificate Policy for LuxTrust Qualified Timestamping

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

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

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

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

	Normaliz	ed Certif	icate Pol	icy for Lu	xTrust C	Qualified Timestamping
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	algorithm				s	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	algorium				3	Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60
	Nobaltel	·				Months
subject		✓	False			
	organisationIdentifier	✓		М	D	VATLU-20976985
	(2.5.4.97)			101		VATEO-20070303
	commonName	✓		М	D	LuxTrust Qualified Timestamping
	organizationName	✓		М	D	LuxTrust S.A.
	countryName	✓		М	D	LU
subjectPublic	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						





VFRSION 1 24

	Normalized Certificate Policy for LuxTrust Qualified Timestamping								
Attribute	Field	IN ¹³	CE ¹⁴	O/M ¹⁵	CO ¹⁶	Value			
authorityKeyldentifier		✓	False						
	keyldentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA			
authorityInfo/	Access	✓	False						
	AccessMethod	✓				Id-ad-2			
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt			
	AccessMethod	✓				Id-ad-1			
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/			
cRLDistribution	onPoint	✓	False						
	distributionPoint	✓			S				
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl			
Subject									
Properties									
subjectAltNar	me	✓	False						
	Rfc822Name	✓		0	D	info@luxtrust.lu			
subjectKeyId	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		✓	True						
	digitalSignature	✓			S	True			
	nonRepudiation	✓			S	False			
	keyEncipherment	✓			S	False			
	dataEncipherment	✓			S	False			
Extended Ke	y Usage	✓	True						
	TimeStamping (1.3.6.1.5.5.7.3.8)	✓			S	Set			
Private Key U	Jsage Period	✓	False						
	Usage period (2.5.29.16)	✓		М	D	Certificate generation process date/time + 12 Months			
certificatePol	icies	✓	False						
	Policyldentifier	✓				1.3.171.1.1.10.3.18			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	PolicyIdentifier	✓				0.4.0.2042.1.2			

3.6.2 Qualified Timestamping Certificate Profile

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







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

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

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

	Qua	alified C	ertificate	Policy fo	r for Lux	Trust Qualified Timestamping
Attribute	Field	IN1	CE1	O/M1	CO1	Value
		3	4	5	6	
Base						
Profile						
Version		✓	Fals			
	,		е			
					S	Version 3 Value = "2"
SerialNumb	er	✓	Fals			
			е			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	Fals			
	Г		е			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
		✓				Encryption.
signatureVa	ilue	•	Fals			
			е		_	
		✓	F-1-		D	Issuing CA Signature.
issuer			Fals		S	
	countryName	√	е		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity	organization (amo	✓	Fals			Lakingstont
· anany			е			
	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		√	Fals			
-			е			
	organisationIdentifie					
	r	✓			_	VATLU-20976985
		•		М	D	
	(2.5.4.97)					
	commonName	√		М	D	
	COMMINIMATINE			IVI		LuxTrust Qualified Timestamping
	organizationName	✓		М	D	LuxTrust S.A.
	countryName	✓		М	D	LU
subjectPubl	icKeyInfo	✓	Fals			
			е			





	Qu	анпеа С		Policy IC	I IOI LUX	Trust Qualified Timestamping
Attribute	Field	IN1	CE1	O/M1	CO1	Value
		3	4	5	6	
	algorithm	✓				Public Key: Key length: up to 3072 bit (RSA)
-	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extension						
s						
Authority						
Properties						
authorityKey	/Identifier	✓	Fals			
			е			
	keyldentifier	✓				
	•					SHA-1 hash of the LuxTrust Global Qualified CA
authorityInfo	Access	✓	Fals			
			е			
	AccessMethod	✓				Id-ad-2
=	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
-	AccessMethod	✓				Id-ad-1
-	accessLocation	✓				http://qca.ocsp.luxtrust.lu/
cRLDistribut	ionPoint	✓	Fals			
			е			
	distributionPoint	✓			S	
-	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
						1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
Subject						
Properties						
subjectAltNa	ıme	√	Fals			
			е			
	Rfc822Name	✓		0	D	info@luxtrust.lu
subjectKeylo		✓	Fals			
,			е			
	keyldentifier	√			Fixed	The Key Identifier comprises a four-bit field with a 0100
	,					value, followed by the least significant 60 bits of the SHA-
						hash of the value or subjectPublicKey bit string (tag, not
						including the length and number of unused bit-string bits).
Policy						and the state of t
Properties						
keyUsage		✓	True			
,, = 39-	digitalSignature	✓			S	True
-	nonRepudiation	✓			S	False
-	keyEncipherment	✓			S	False
-	dataEncipherment	✓			S	False
Extended Ke	-	✓	True		3	1 4100
	TimeStamping	✓	True		S	Set
LXterided IXt		1	ĺ		٥	JEI
Exterided N						
	(1.3.6.1.5.5.7.3.8) Usage Period	✓	Fals	_		







	Q	ualified (Certificate	e Policy fo	or for Lux	Trust Qualified Timestamping
Attribute	Field	IN1	CE1	O/M1	CO1	Value
		3	4	5	6	
	Usage period	✓		М	D	Certificate generation process date/time + 12 Months
	(2.5.29.16)					
certificatePo	olicies	√	Fals			
			е			
	Policyldentifier	√				1.3.171.1.1.10.3.19
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers					
	Policyldentifier	√				0.4.0.194112.1.1
certificatePo	olicies	✓				
	QcТуре	✓		М	S	id-etsi-qct-eseal
	(0.4.0.1862.1.6)					(0.4.0.1862.1.6.2)
	QcCompliance	✓		М	S	True
	(0.4.0.1862.1.1)					
	QcPDS	√		М	S	https://www.luxtrust.lu/upload/data/repository/GTC_F_v2_4
	(0.4.0.1862.1.5)					.pdf
	(0.4.0.1862.1.5)					.pdf

3.6.3 TimeStamp Request and Response Format

3.6.3.1 TimeStamp Request Format

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

	LuxTrust Time Stamp Request
Field	Value / comment
Document Hash	Hash of the document on which the TimeStamp must be computed
Hash OID	(SHA-1/SHA-256/SHA-512) Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.
Policy OID	1.3.171.1.1.10.3.18.1 The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.
Should TSA Certificate be included?	TRUE/FALSE
Request Extensions	Value *







LuxTrust Time Stamp Request							
Field Value / comment							
None	None						

^{*}no extension is required to be supported

3.6.3.2 TimeStamp Response Format

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

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

^{*}no extension is required to be generated, no extension shall be critical

3.7 Certificate extensions

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

3.8 Algorithm object identifiers

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

3.9 Name forms

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



3.10 Name constraints

Name constraints are supported as per RFC 5280.

3.11 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

3.12 Usage of Policy Constraints extension

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

3.13 Policy qualifiers syntax and semantics

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

3.14 Processing semantics for the critical Certificate Policies

Not applicable.

3.15 CRL profile

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

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

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

LuxTrust CRL Profile							
Field	Comments						
Version	v2						
Signature	Same signature algorithm as related CA						
Issuer	<subjectca></subjectca>						
thisUpdate	<creation time=""></creation>						
nextUpdate	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""></creation></pre>						
	<creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" p="" subordinate<="" time=""></creation>						
	Qualified and SSL CAs>						
	<creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation>						
revokedCertificates							
userCertificate	<certificate number="" serial=""></certificate>						
revocationDate	<revocation time=""></revocation>						
crlEntryExtensions							
reasonCode	<pre></pre> <pre></pre> <pre></pre> <pre></pre>						
crlExtensions							







	LuxTrust CRL Profile					
Field		Comments				
	cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>				
	authorityKeyldentifier	Non-critical <ca assigned="" number="" unique=""></ca>				

3.15.1 Version number(s)

See section 3.4.

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

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

3.15.2 CRL entry extensions

See section 3.4.

3.16 OCSP profile

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

3.16.1 Version number(s)

See section 3.5.

3.16.2 OCSP extensions

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

	LuxTrust OCSP Certificate Profile								
Attribute	Field	IN18	CE19	O/M20	CO21	Value			
Base Profile									
Version		•	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	•	False						
					FDV	Validated on duplicates.			
signatureAlg	orithm	•	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	ue	•	False						
					D	Issuing LTGRCA Signature			
issuer		•	False		S				
	countryName	•			S	LU			
	commonName	•			S	LuxTrust Global Root x			
	organizationName	•			S	LuxTrust S.A.			
Validity		•	False						
	NotBefore	•			D	Certificate generation process date/time.			
	NotAfter	•			D	Certificate generation process date/time + maximum 12 Months			





LuxTrust OCSP Certificate Profile									
Attribute	Field	IN18	CE19	O/M20	CO21	Value			
subject		•	False						
	countryName	•		М	D	LU			
	organizationName	•		М	D	LuxTrust S.A.			
	organizationalUnitName 1	•		0	D	Pki entity			
	commonName	•		М	D	LuxTrust S.A. OCSP Server 2			
subjectPublicKeyInfo		•	False						
	algorithm	•				Public Key: Key length: 2048 bit (RSA			
	subjectPublicKey	•		М		public exponent: Fermat-4 (=010001).			
Extensions									
Authority									
Properties									
authorityKe	yldentifier	•	False						
	keyldentifier	•				SHA-1 Hash of the LuxTrust LTGR x (
						public key			
id-ocsp-noc	heck	•	False						
		•			S	NULL			
Subject									
Properties									
subjectKeyl	dentifier	•	False						
	keyldentifier				Fixed	The Key Identifier comprises a four- field with a 0100 value, followed by t least significant 60 bits of the SHA-1 ha of the value or subjectPublicKey bit stri			
						(tag, not including the length and numl of unused bit-string bits).			
Policy									
Properties			-						
keyUsage	T	•	True						
	digitalSignature				S	True			
	nonRepudiation	•			S	False			
	keyEncipherment	•			S	False			
	dataEncipherment				S	False			
certificatePolicies			False						
	Policyldentifier					1.3.171.1.1.1.0.1.0			
	policyQualifierID				S	Id-qt-1 (CPS)			
	qualifier				S	https://repository.luxtrust.lu			
	policyQualifierID	•			S	Id-qt-2 (User Notice)			
	noticeNumbers				1	<u> </u>			





LuxTrust OCSP Certificate Profile									
Attribute	Field	IN18	CE19	O/M20	CO21	Value			
	DisplayText					LuxTrust S.A. Online Certificate Status Server. IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported.			
	Policyldentifier	•				0.4.0.2042.1.3			
Extended Key Usage		•	False						
	OCSPSigning	•			S	True			

