



Version number: 1.40 Publication Date: 15/04/2024 Effective Date: 29/04/2024

> LuxTrust S.A IVY Building | 13-15, Parc d'activités | L-8308 Capellen Luxembourg | VAT LU 20976985 | RCS B112233

Business Number N°00135240/0 Phone: +352 26 68 15 – 1

Fax: +352 26 68 15 – 789







# **Document Information**

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

# **Version History**

Version	Who	Date	Reason of modification		
1.0	MSC	29/08/2011	Initial Version DRAFT		
1.01	MSC	27/10/2011	Added CRL validity period, revision		
1.02	MSC	24/11/2011	Modified – Document OIDs for Cas		
1.03	MSC	09/02/2012	Modified – Added LCP for integration purposes.		
1.04	MSC	01/03/2012	Modified:		
			<ul> <li>Added LCP for integration purposes for CSS</li> </ul>		
			Table for OIDs		
			Modification of the CRL issuance algorithm (SHA256 to SHA1)		
1.05	MSC	19/03/2012	Modifications following review by Chris Quaresimin and Laurent Breuskin:		
			Removal of + Nestcape proprietary extension:		
			NetscapeCertificateType: sslClient, smime for non-SSL products		
			Display text for CSS integration product     Carrect CRI and AIA for CSS integration product		
			Correct CRL and AIA for CSS integration product     SSI. Object contificate profile.		
1.06	MSC	26/03/2012	SSL Object certificate profile  Modifications for CSS certificates, signature will be performed using		
1.00	IVISC	20/03/2012	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:		
			<ul> <li>Table for OIDs &amp; LuxTrust CA Hierarchy</li> </ul>		
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		
	IKO		Added CP non SSCD NCP+ Certificates supporting Advanced Electronic Signatures for Mass Signature Services		
			Various syntactical and format corrections		
1.13	CSP Board	23/04/2013	insertion of ILNAS logo including accreditation reference and technical		
1.10	OOI Board	20/04/2010	standards reference		
1.14	YNU	29/11/2013	Update specific requirements for CP under the SSL CA		
1.15	YNU	18/01/2014	Clarification on Mozilla request		
1.16	YNU	05/06/2014	Update Cp		
			- for LuxTrust Global Root Renew		
			- QcS2 et QcS3		
			- Typo Add CP Seal Signature Services		
			Aud OF Seal Signature Services		
1.17	YNU	30/06/2014	Add certificate profile for eID		
		30,00,2011	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		10/10/2011	Opdate AIA III OOL OA		

LuxTrust proprietary Page 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 Board	25/03/2015	Update LT CA				
			- lifetime up to 20 years - AIA				
			Update Display text				
			- EV SSL CP				
			Update eID CP Update ILNAS Logo				
1.22	YNU	03/11/2015	Update Common Names in non SSL certificates				
		1	Remove NetscapeCertType extension from SSL and Object Signing				
			Certificates  Added: OCSP signing Certificate which contains an extension of type id pkix				
			Added: OCSP signing Certificate which contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960				
			,				
1.23	YNU	05/08/2016	Add Timestamping Profile under Global Qualified CA				
1.24	DEL	12/06/2017	Update Signing Server LCP Certificate profil Add:				
		, 55, 2517	LuxTrust Qualified Timestamping Certificate profile with QC				
			statements				
			SPARE LuxTrust Signing Server LCP Certificate Profile     Outlified/Advanced eSeel certificate profiles				
			<ul> <li>Qualified/Advanced eSeal certificate profiles</li> <li>eIDAS qualified certificate profiles</li> </ul>				
			Signing Server Signature and eSeal certificates and QWAC				
		00/5-1-2	certificate and signing stick certificates				
1.25	DEL	30/08/2017	Add Microsoft OIDs in SSL certificates profiles to ensure				
			alignement with Microsoft Trusted Root certificate Program requirements (https://technet.microsoft.com/en-				
			us/library/cc751157.aspx).				
4.00	NDE	0.4/4.4/00.47	ODI IIII ( 1100 L. 110				
1.26	NDE DEL	24/11/2017 15/12/2017	<ul> <li>Increase CRL validity from 4h30min to 8h30min for SSL certificates</li> <li>Update hash functions in accordance with normative requirements</li> </ul>				
	DEL	01/01/2018	Opdate hash functions in accordance with normative requirements     Add Advanced eSeal certificate profile				
	55.	10/00/	·				
1.27	DEL	19/03/2018	Add LuxTrust Corporate CA & Corporate certificate profile     Lindate SSL certificates profiles to support Certificate				
			Update SSL certificates profiles to support Certificate     Transparency				
1.28	DEL	29/06/2018	Change O.I.D in SSL OV certificates				
			Introduce O.I.D prefixed with 2.999     Partitioned CRI S				
1.29	DEL	19/03/2019	Partitioned CRLS  Long tom Timestemping (In Test)				
1.23		10/00/2019	<ul> <li>Long term Timestamping (In Test)</li> <li>Setting an Issue Distribution point (IDP) in Partitioned CRL</li> </ul>				
			New CRL creation				
1.30	DEL	21/10/2019	Long term Timestamping (In production)				
			LCP Certificate Profile Update  Lograding the public key length for the profiles with OID:				
			<ul> <li>Upgrading the public key length for the profiles with OID:</li> <li>1.3.171.1.1.10.3.5 &amp; OID: 1.3.171.1.1.10.3.20 from 2048 bit (RSA)</li> </ul>				
			to Public Key length from 2048 bit up to 4096bit (RSA)				
			Adding Wildcard - LCP certificates supporting Signature,				
1.31	YNU	13/02/2020	Authentication & Encryption				
1.31	1100	13/02/2020	<ul><li>Update key usage for OID. 1.3.171.1.1.10.3.32</li><li>Splitted CRL for OID</li></ul>				
			o 1.3.171.1.10.3.32,				
			0 1.3.171.1.1.10.3.33,				
			<ul> <li>1.3.171.1.1.10.3.18</li> <li>Add Basic contraint to OID</li> </ul>				
			• Add Basic Contraint to OID  • 1.3.171.1.1.10.3.33,				
			o 1.3.171.1.1.10.3.21,				
			0 1.3.171.1.10.3.23,				
1.32	CSP Board	16/11/2020	<ul> <li>1.3.171.1.1.10.3.25</li> <li>Update OI definition</li> </ul>				
1.33	YNU	10/06/2021	Add Qualified eSeal not on QSCD				
1.34	YNU/VMI	18/10/2021	Alignment of level of certification policy (NCP+) referring to OID				
			1.3.171.1.1.10.3.18				
			References update     Typo update				
1.35	YNU	17/03/2022	<ul> <li>Typo update</li> <li>Add 1.3.171.1.1.10.3.38 eID BE delegated Sign QCP-n-qscd</li> </ul>				
	1	, 33, 2322	- Add 1.0.17 1.11.170.0.00 CID DE delegated Digit QOI -11-q3cd				

LuxTrust proprietary





1.36	YNU	01/08/2022	<ul> <li>Add 1.3.171.1.1.10.3.39 LuxTrust PRI/PRO delegated Sign QCP-n-qscd</li> <li>Add 1.3.171.1.1.10.3.40 eID LU delegated Sign QCP-n-qscd</li> <li>Update 3.26, 3.27, 3.28, 3.29 with 2048bit up to 4096bit</li> <li>Replace =010001 by 0x010001</li> </ul>	
1.37	CSP Board	11/10/2022	<ul> <li>Update policy .33 with 5 years validity</li> </ul>	
1.38	CSP Board		Update QcPDS	
1.39	YNU	27/07/2023	Add LTCCA EE NCP+ AATL: 1.3.171.1.1.10.4.3 Dedicated to LuxTrust	
1.40	YNU	10/04/2024	Add LTCCA EE NCP+ AATL: 1.3.171.1.1.10.4.5 Dedicated to BNPP FORTIS	



# **Table of content**

DOCUME	NT INFORMATION	2
VERSION	HISTORY	2
TABLE O	F CONTENT	5
INTELLE	CTUAL PROPERTY RIGHTS	8
REFEREN	ICES	9
INTRODU	CTION	10
1.1	THE LUXTRUST PROJECT	10
1.2	GOAL OF THE LUXTRUST PKI	
1.3	LuxTrust PKI Hierarchy	
LUXTRUS	ST CERTIFICATION AUTHORITIES	11
1.4	TWO-LEVEL CA HIERARCHY	
CERTIFIC	ATE AND CRL PROFILES	12
1.5	CERTIFICATE TYPES	12
1.6	LuxTrust Certification Authorities – Certificates profiles	
1.7	LuxTrust Global Root CA	
1.8	LuxTrust Global Qualified CA	
1.9	LuxTrust SSL CA	
1.10	LuxTrust Corporate CA	
1.10.1	Certificate extensions	24
1.10.2	Algorithm object identifiers	24
1.10.3	Name forms	24
1.10.4	Name constraints	24
1.10.5	Certificate policy object identifier	24
1.10.6	Usage of Policy Constraints extension	24
1.10.7	Policy qualifiers syntax and semantics	24
1.11	LuxTrust End-entity – Certificates profiles	24
1.11.1	Certificate profiles	24
1.11.2	Version number(s)	25
1.11.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	25
1.11.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	28
1.11.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	29
1.11.6	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	32
1.11.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	34
1.11.8	LuxTrust NCP+ Certificates supporting Mass Signature Services	36
1.11.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	38
1.11.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	40
1.11.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration	n purpose
	41	
1.11.12	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	
1.11.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	
1.11.14	LuxTrust non SSCD Mass LRAO QCP Certificates supporting Advanced Electronic Signatures	
1 11 15	LuxTrust elD SSCD OCP+ Certificates supporting Qualified Signatures	48



1.11.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	50
1.11.17	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures	52
1.11.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	54
1.11.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	55
1.11.20	LuxTrust SSL/TLS Standard Server Certificates - LCP certificates supporting Signature, Authentication	& Encryption
	57	
1.11.21	SSL/TLS Extended Validation Server Certificates - EVCP certificates supporting Signature, Auth	
	Encryption	
1.11.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Auth	
	Encryption	
<i>1.11.23</i>	LuxTrust Object (or Code) Signing Certificates	
<i>1.11.24</i>	LuxTrust SSL/TLS Certificate for Client Authentication	
<i>1.11.25</i>	SSL/TLS QCP-w Extended Validation Server Certificates	
<i>1.11.26</i>	Wildcard - LCP certificates supporting Signature, Authentication & Encryption	
1.11.27	LuxTrust SPARE Signing Server LCP Certificate Profile	
1.11.28	LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature	
<i>1.11.29</i>	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	
1.11.30	LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature	
1.11.31	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	
1.11.32	LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature	
1.11.33	LuxTrust Smart Card QCP-n-qscd Certificate Profile	
1.11.34	LuxTrust Smart Card NCP+ Certificate Profile	
<i>1.11.35</i>	LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature	94
1.11.36	LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purposes	96
1.11.37	QCP-n-qscd supporting Qualified Electronic Signature for elD smart cards	97
1.11.38	NCP+ supporting Authentication & Encryption for eID smart cards	99
1.11.39	LuxTrust Signing Server QCP-n-qscd Certificate Profile	100
1.11.40	LuxTrust Signing Server QCP-I-qscd Certificate Profile	102
1.11.41	LuxTrust Signing Stick QCP-n-qscd certificate profile	104
1.11.42	LuxTrust Signing Stick NCP+ Certificate Profile	106
1.11.43	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	107
1.11.44	LuxT LuxTrust Signing Server QCP-I Certificate Profile	110
1.11.45	LuxTrust Signing Server elD BE delegated Sign QCP-n-qscd Certificate Profile	112
1.11.46	LuxTrust Signing Server LuxTrust PRI/PRO delegated Sign QCP-n-qscd Certificate Profile	113
1.11.47	LuxTrust Signing Server elD LU delegated Sign QCP-n-qscd Certificate Profile	115
1.11.48	LuxTrust Corporate LCP Certificate Profile	116
1.11.49	LuxTrust Corporate eSeal LCP Certificate Profile	118
1.11.50	LuxTrust Corporate AATL Certificate Profile	119
1.11.51	BNPPF Corporate AATL Certificate Profile	121
1.12	TIMESTAMPING CERTIFICATE PROFILE	122
1.12.1	Normalized (NCP+) Certificate Policy for LuxTrust Qualified Timestamping	123
1.12.2	Qualified Timestamping Certificate Profile	125
1.12.3	TimeStamp Request and Response Format	126
1.12.4	Certificate extensions	127
1.12.5	Algorithm object identifiers	127
1.12.6	Name forms	127
1.12.7	Name constraints	127
1.12.8	Certificate policy object identifier	127
1.12.9	Usage of Policy Constraints extension	127





<i>1.12.10</i>	Policy qualifiers syntax and semantics	127
1.12.11	Processing semantics for the critical Certificate Policies	127
1.13	CRL PROFILE	128
1.13.1	Version number(s)	129
1.13.2	CRL entry extensions	129
1.14	OCSP PROFILE	129
1.14.1	Version number(s)	129
1.14.2	OCSP extensions	129
1.15	INTEGRATION CERTIFICATES	130

VERSION 1.40



# **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.

LuxTrust proprietary



## 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 replaced by REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 (eIDAS).
- [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 replaced by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR).
- [3] ETSITS 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 du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 1 juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [10] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [11] LuxTrust Time Stamping Policy, latest version in force.
- [12] Guidelines for the Issuance and Management of Extended Validation Certificates. CA/Browser Forum. Latest version in force.
- [13] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force.
- [14] eID Certificate Life Cycle Procedure latest version in force
- [15] RNCID: National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16
- [16] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [17] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [18] Loi du 19 juin 2013 Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques
- [19] EN 319 411 1 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [20] EN 319 411 2 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- [21] According to EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)
- [22] According to EN 319 422 V1.1.1, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (2016-03)
- [23] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)
- [24] According to EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)
- [25] According to EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)
- [26] According to EN 319 412-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (2016-02)
- [27] According to EN 319 412-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)
- [28] According to EN 319 412-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)
- [29] According to EN 319 412-4 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (2016-02)
- [30] According to EN 319 412-5 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements (2016-02)
- [31] European regulation N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)



### INTRODUCTION

#### 1.1The LuxTrust project

The LuxTrust project was created in the form of a Trusted Third Party (hereafter also "TTP"), with an international reach, aiming to establish a national expertise center for Luxembourg. LuxTrust as TTP especially focuses on providing support for any existing business needs in terms of security and promotes new "e-business" and "e-government" opportunities, making the best possible use of existing legal and commercial assets that 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 17/07/2020 [7] itself derived from the (eIDAS) regulation cf.[31]). 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 17/07/2020 [7], is using several Certification Authorities (CAs).

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

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



### **LuxTrust Certification Authorities**

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

### 1.4 Two-level CA hierarchy

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

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

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

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

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

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



# **CERTIFICATE AND CRL PROFILES**

### 1.5 Certificate types

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

CP identification	CP OID	CPS OID	Short Description	Ref.		
LuxTrust Qualified Cer	LuxTrust Qualified Certification Authority					
QCP+ supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.1	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature.  These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures		
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.2	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.  These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption		
QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.3	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate.	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures		
NCP supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.4	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption		
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.5	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a <b>non</b> SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption		
NCP+ supporting Advanced Electronic Mass Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	1.3.171.1.1.1.10.3	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		





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





CP identification	CP OID	CPS OID	Short Description	Ref.
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.14	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., Luxemburgish elD Smart Card), with creation of the keys by the CSP, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption
NCP+ Advanced Electronic Seal Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.15	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Seal Signature Services.	LuxTrust NCP+ Certificates supporting SEAL Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.16	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	1.3.171.1.1.10.3	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 (NCP+) Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.18	1.3.171.1.1.10.3	EN 319 421 compliant.	Normalized (NCP+) 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	1.3.171.1.1.10.3	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-l-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
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),





CP identification	CP OID	CPS OID	Short Description	Ref.
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.31	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons,
LuxTrust Signing Server QCP-n-qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.32	1.3.171.1.1.10.3	Signing Server certificate for qualified signature	LuxTrust Signing Server QCP-n-qscd Certificate profile
LuxTrust Signing Server QCP-I-qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.33	1.3.171.1.1.10.3	Signing Server certificate for qualified eSeal	LuxTrust Signing Server QCP-I-qscd Certificate profile
LuxTrust Signing Stick QCP-n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	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 issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.35	1.3.171.1.1.10.3	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile
LuxTrust Signing Server Advanced Automated eSeal Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.36	1.3.171.1.1.1.10.3	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile
LuxTrust Signing Server QCP-I Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.37	1.3.171.1.1.10.3	Qualified Certificate QCP-I with creation of the keys by the Subscriber, limited to the support of advanced electronic eSeals	LuxTrust Signing Server QCP-I Certificate Profile
LuxTrust Signing Server eID BE delegated Sign QCP- n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.38	1.3.171.1.1.1.10.3	QCP-n-qscd certificate with creation of the keys by LuxTrust, with a key usage that supports qualified electronic signature	LuxTrust Signing Server eID BE delegated Sign QCP-n-qscd Certificate Profile
LuxTrust Signing Server LuxTrust PRI/PRO delegated Sign QCP-n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.39	1.3.171.1.1.1.10.3	QCP-n-qscd certificate with creation of the keys by LuxTrust, with a key usage that supports qualified electronic signature	LuxTrust Signing Server LuxTrust PRI/PRO delegated Sign QCP-n-qscd Certificate Profile

LuxTrust proprietary





CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Signing Server eID LU delegated Sign QCP- n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.40	1.3.171.1.1.1.10.3	QCP-n-qscd certificate with creation of the keys by LuxTrust, with a key usage that supports qualified electronic signature	LuxTrust Signing Server eID LU delegated Sign QCP-n-qscd Certificate Profile
LuxTrust SSL Certificat	tion 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 <b>EVCP</b> compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentication & Encryption
SSL/TLS(+) Extended Validation Server Certificates – EVCP+ issued by LuxTrust SSL CA	1.3.171.1.1.10.5.3	1.3.171.1.1.1.0.5	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





CP identification	CP OID	CPS OID	Short Description	Ref.
Wildcard - LCP certificates supporting Signature, Authentication & Encryption issued by LuxTrust SSL CA	1.3.171.1.1.10.5.7	1.3.171.1.1.1.10.5	Wildcard LCP certificates supporting Signature, Authentication & Encryption	LuxTrust Wildcard - LCP certificates supporting Signature, Authentication & Encryption
LuxTrust Corporate CA				
LuxTrust Corporate LCP Certificate Profile	1.3.171.1.1.10.4.1	1.3.171.1.1.1.10.4	LuxTrust Corporate LCP Certificate Profile	LuxTrust Corporate LCP
issued by Corporate CA			This policy is deprecated and no more used since 2020. There is no valid certificate.	Certificate Profile
LuxTrust Corporate eSeal LCP Certificate	1.3.171.1.1.10.4.2	1.3.171.1.1.1.10.4	LuxTrust Corporate Advanced LCP eSeal Certificate Profile	LuxTrust Advanced LCP
Profile issued by Corporate CA			This policy is deprecated and no more used since 2020. There is no valid certificate.	eSeal Certificate
LuxTrust Corporate AATL Certificate Profile issued by Corporate CA	1.3.171.1.1.10.4.3	1.3.171.1.1.1.10.4	LuxTrust Corporate NCP+ AATL Certificate Profile with 2FA or equivalent identification process	LuxTrust Corporate AATL Certificate
LuxTrust Corporate AATL Certificate Profile issued by Corporate CA	1.3.171.1.1.10.4.5	1.3.171.1.1.1.10.4	BNPPF Corporate NCP+ AATL Certificate Profile with 2FA or equivalent identification process	BNPPF Corporate AATL Certificate

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 (eIDAS) regulation (cf.[31]). 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.



### 1.6LuxTrust Certification Authorities - Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

### 1.7LuxTrust Global Root CA

LuxTrust Global Root CA							
Base Profile	OID	Include d	Critical	Value			
Version		Х		V3			
SerialNumber		Х		As provided by CA or by LuxTrust S.A.			
SignatureAlgorithm							
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed		
SignatureValue		Х		Issuing CA Signature			
Validity							
NotBefore		Х		Key Generation Process Date/Time			
NotAfter		Х		Key Generation Process Date/Time + 10;20 years	Fixed		
SubjectPublicKeyInfo		Х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (0x010001).  20 years certificate requires a 4096 key length.			
Issuer							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }			LuxTrust Global Root x <sup>1</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
CertificatePolicies <sup>2</sup>	{id-ce 32}	Х	FALSE				
policyldentifier		Х		1.3.171.1.1.1.10	Fixed		
policyQualifiers				N/a			
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed		
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed		
KeyUsage	{id-ce 15}	Х	TRUE⁴				

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

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



LuxTrust Global Root CA								
Base Profile	OID	Include d	Critical	Value				
CertificateSigning				Set	Fixed			
crlSigning				Set	Fixed			
authorityKeyldentifier	{id-ce 35}	X	FALSE					
Keyldentifier		X		SHA-1 Hash				
subjectKeyldentifier	{id-ce 14}	X	FALSE					
Keyldentifier		Х		SHA-1 Hash				
BasicConstraints	{id-ce 19}	Х	TRUE⁴					
CA		X		TRUE	Fixed			
pathLenConstraint		X		None	Fixed			

# 1.8LuxTrust Global Qualified CA

LuxTrust Global Qualified CA							
Base Profile	OID	Include d	Critical	Value			
Version		Х		V3			
SerialNumber		Х		As provided by CA or by LuxTrust S.A.			
SignatureAlgorithm							
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed		
SignatureValue		Х		Issuing LTGRCA Signature			
Validity							
NotBefore		Х		Key Generation Process Date/Time			
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed		
SubjectPublicKeyInfo		Х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (0x010001).  20 years certificate requires a 4096 key length.			
Issuer							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA x <sup>1</sup>	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			



LuxTrust Global Qualified CA							
Base Profile	OID	Include d	Critical	Value			
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed		
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed		
KeyUsage	{id-ce 15}	Х	TRUE⁴				
keyCertSign				Set	Fixed		
crlSign				Set	Fixed		
authorityKeyldentifier	{id-ce 35}	Х	FALSE				
Keyldentifier		Х		SHA-1 Hash of Authority public key			
authorityInfoAccess <sup>3</sup>	{id-pe 1}		False				
AccessMethod	{Id-ad-1}						
accessLocation		Х		http://ltgroot.ocsp.luxtrust.lu	Fixed		
AccessMethod	{Id-ad-2}		False				
accessLocation		х		http://ca.luxtrust.lu/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/LTGRCAx1.crl	Fixed		
BasicConstraints	{id-ce 19}	Х	TRUE <sup>4</sup>	N/A			
CA		Х		TRUE	Fixed		
pathLenConstraint		Х		0 (Zero)	Fixed		

### 1.9LuxTrust SSL CA

LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value				
Version		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			

 $<sup>^3</sup>$  Since LuxTrust Global Qualified CA 3

<sup>&</sup>lt;sup>4</sup> Criticality of this extension should be carefully considered with regards to the compliance with RFC 5280 stating in its section 4.2.1.10 that "This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates".





LuxTrust SSL CA						
Base Profile	OID	Included	Critical	Value		
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (0x010001).  20 years certificate requires a 4096 key length.		
Issuer						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed	
organizationName		Х		LuxTrust S.A.	Fixed	
Subject						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }			LuxTrust SSL CA x <sup>1</sup>	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	TRUE⁴			
keyCertSign				Set	Fixed	
crlSign				Set	Fixed	
authorityKeyldentifier	{id-ce 35}	Х	FALSE			
Keyldentifier		Х		SHA-1 Hash of Authority public key		
authorityInfoAccess <sup>5</sup>	{id-pe 1}		False			
AccessMethod	{Id-ad-1}	V		http://ltgroot.goog.luytrugt.lu	Fixed	
accessLocation AccessMethod	{Id-ad-2}	Х	False	http://ltgroot.ocsp.luxtrust.lu	FIXEU	
accessLocation	[ uu z]	Х	. 2.00	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/LTGRCAx1.crl	Fixed	
BasicConstraints	{id-ce 19}	Х	TRUE⁴	N/a	<u> </u>	

<sup>&</sup>lt;sup>5</sup> Since LuxTrust SSL CA 4



LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value				
CA		X		TRUE	Fixed			
pathLenConstraint		Х		0 (Zero)	Fixed			

# 1.10 LuxTrust Corporate CA

LuxTrust Corporate CA						
Base Profile	OID	Included	Critical	Value		
Version		Х		V3		
SerialNumber		Х		Random CSN		
SignatureAlgorithm						
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed	
SignatureValue		Х		Issuing LTGRCA2 Signature		
Validity						
NotBefore		Х		Key Generation Process Date/Time		
NotAfter		х		Key Generation Process Date/Time +up to 20 years	Fixed	
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (0x010001).  20 years certificate requires a 4096 key length.		
Issuer						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }	Х		LuxTrust Global Root 2	Fixed	
organizationName		Х		LuxTrust S.A.	Fixed	
Subject						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }			LuxTrust Corporate CA x	Fixed	
organizationName		Х		LuxTrust S.A.	Fixed	
CertificatePolicies	{id-ce 32}	Х	FALSE			
policyldentifier		Х		1.3.171.1.1.10.4	Fixed	
policyQualifiers				N/a		
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed	
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed	
KeyUsage	{id-ce 15}	Х	TRUE4			
keyCertSign				Set	Fixed	
crlSign				Set	Fixed	



LuxTrust Corporate CA							
Base Profile	OID	Included	Critical	Value			
authorityKeyIdentifier	{id-ce 35}	×	FALSE				
Keyldentifier		Х		SHA-1 Hash of Authority public key			
authorityInfoAccess	{id-pe 1}		False				
AccessMethod	{Id-ad-1}						
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed		
AccessMethod	{Id-ad-2}		False				
accessLocation		х		http://ca.luxtrust.lu/LTGRCA2.crt	Fixed		
subjectKeyIdentifier	{id-ce 14}	X	FALSE				
Keyldentifier		×		SHA-1 Hash of Subject public key			
cRLDistributionPoints	{id-ce 31}	X	FALSE				
distributionPoint							
FullName		X		http://crl.luxtrust.lu/LTGRCA2.crl	Fixed		
BasicConstraints	{id-ce 19}	Х	TRUE	N/A			
CA		Х	_	TRUE	Fixed		
pathLenConstraint		Х		0 (Zero)	Fixed		

#### 1.10.1 Certificate extensions

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

#### 1.10.2 Algorithm object identifiers

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

### 1.10.3 Name forms

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

#### 1.10.4 Name constraints

Name constraints are supported as per RFC 5280.

### 1.10.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

#### 1.10.6 Usage of Policy Constraints extension

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

### 1.10.7 Policy qualifiers syntax and semantics

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

### 1.11 LuxTrust End-entity - Certificates profiles

### 1.11.1 Certificate profiles

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

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

 LuxTrust SSCD Smartcards: These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies





- One LuxTrust QCP+<sup>6</sup> Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy OID 1.3.171.1.10.3.1, and
- One LuxTrust NCP+<sup>7</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.10.3.2.

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

- LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.26.
- LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1]
  (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP<sup>6</sup> Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.11.0.3.3, and
  - One LuxTrust NCP<sup>7</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.10.3.4.
- LuxTrust Signing Server Accounts (Virtual Smartcards): These centralised virtual user signature creation devices
  contain one certificate, associated to one key pair, according to one specific certificate policy
  - One LuxTrust NCP<sup>7</sup> certificate for Natural Persons for the combined purposes of electronic signature, data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.5.
- LuxTrust eSeal Smart card-based certificates: The eSeal smart card exists in two versions: advanced and qualified.

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

- LuxTrust Qualified eSeal Certificate Profile supporting digital signature under the Certificate Policy OID 1.3.171.1.10.3.21
- LuxTrust Advanced eSeal Certificate Profile supporting authentication under the Certificate Policy OID 1.3.171.1.1.0.3.22

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

- LuxTrust Advanced eSeal Certificate Profile supporting signature under the Certificate Policy OID 1.3.171.1.1.10.3.23.
- LuxTrust Advanced eSeal Certificate Profile supporting authentication under the Certificate Policy OID 1.3.171.1.10.3.24.

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 1.3.171.1.10.5.5.

#### 1.11.2 Version number(s)

X.509 v3 is supported and used.

### 1.11.3 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]).

<sup>&</sup>lt;sup>6</sup> As defined by ETSI TS 101 456 (cf. [3]).

<sup>&</sup>lt;sup>7</sup> As defined in ETSI TS 102 042 (cf. [4]).





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

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

LuxTrust SSCD QCP+ Certificate Profile								
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value		
Base Profile								
Version		✓	False					
					S	Version 3 Value = "2"		
SerialNumbe	er	✓	False					
					FDV	Validated on duplicates.		
signatureAlg	Algorithm	✓	False		S	OID = "1.2.840.113549.1.1.11" - SHA256		
	Algoridiiii				3	with RSA Encryption.		
signatureVal	lue	✓	False			•		
					D	Issuing CA Signature.		
Issuer		<b>√</b>	False		S			
	countryName	✓ ✓			S	LU		
	commonName				S	LuxTrust Global Qualified CA x <sup>1</sup>		
N. P. P.	organizationName	<b>√</b>			S	LuxTrust S.A.		
Validity	NotBefore	<b>✓</b>	False			Contitionto gonoration processo data/time		
	NotAfter	<b>√</b>			D D	Certificate generation process date/time.  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	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card		
	surname	<b>✓</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)		
	countryName	✓		М	D	Nationality of holder (ISO3166)		
	emailAddress	✓		0	D	Subject's email address		
						PRIVATE products:		
						Fixed value: "Private Person"		
						PRO products:		
	title	<b>✓</b>		М	D	"Professional Person" (default) or "Professional Administrator"		
						(Other titles possible for special purpose certificates)		
					-	PRO products only:		
	organizationName	<b>~</b>		М	D	Name of company/institution as in articles of association or equivalent documents, including the legal form.		
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)		

 $<sup>^{8}</sup>$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{9}</sup>$  CE = Critical Extension.

 $<sup>^{10}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{11}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	Lux <sup>-</sup>	Trust SS	CD QC	P+ Cert	ificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Attribute	organizationalUnitName	<b>√</b>	<u> </u>	M for PRO prod., conditional (O) for	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:
				PRIV prod.)		If the holder is underage: "Mineur jusqu'à : & (Date of birth + 18 years).  PRO products only:
	organizationalUnitName 2	<b>~</b>		0	D	Company/institution department or othe information item
subjectPubli		<b>√</b>	False			D 15 14 14 10 10 10 17 (DOA)
	Algorithm subjectPublicKey	<b>✓</b>		N 4		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions	SubjectPublickey	V		М		exponent. Fermat-4 (0x010001).
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Globa Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	✓ ✓				ld-ad-2 http://ca.luxtrust.lu/LTGQCAx.crt
	accessLocation AccessMethod	<b>∨</b>				Id-ad-1
	accessLocation	· ·				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut		✓	False			http://qca.ocsp.iuxtrust.iu/
CICEDISTIBUT	distributionPoint	· ·	i aise		S	
	fullName	· ✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		<b>✓</b>	False		Fixed	The Manual design assessment of the big Col
Policy	keyldentifier	v			Tixeu	The Key Identifier comprises a four-bit field with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, no including the length and number of unused bit-string bits).
Properties						
keyUsage	•	✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
a autiti - : t =	dataEncipherment	<b>√</b>			S	False
certificatePo	Policyldentifier	<b>✓</b>	False			1 2 171 1 1 10 2 1
	policyQualifierID	<b>∨</b>			S	1.3.171.1.1.10.3.1 Id-qt-1 (CPS)
	qualifier	<b>→</b>			S	https://repository.luxtrust.lu
	policyQualifierID	· ✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>√</b>				LuxTrust Qualified Certificate on SSCI 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						
	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	✓		M	D	0.4.0.1862.1.4





#### 1.11.4 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.

	Lu	xTrust :	SSCD N	ICP+ Ce	rtificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base						
Profile		<b>√</b>	E-I			
Version		· ·	False		S	Version 3 Value = "2"
SerialNumbe	er	<b>√</b>	False		3	version 3 value – 2
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
issuer	a a untru Mama	✓ ✓	False		S	LU
	countryName commonName	V /			S	
		· ·			S	LuxTrust Global Qualified CA x <sup>1</sup> LuxTrust S.A.
Validity	organizationName	<b>▼</b>	False		3	Luxiiust S.A.
, amanty	NotBefore	<b>√</b>	1 4100		D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 36 Months
subject	•	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		M	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:  Fixed value: "Private Person"
						PRO products:
	title	✓		М	D	"Professional Person" (default) or "Professional Administrator"
						(Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		M	D	PRO products only: Company/institution country of HQ (as in articles of association)



	Lux	Trust S	SSCD N	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
	organizationalUnitName 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitName 2	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPubli	icKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	vldentifier	<b>√</b>	False			
dutilontyrto	keyldentifier	<b>√</b>	1 0100			SHA-1 Hash of the LuxTrust Global
						Qualified CA public key
authorityInfo		✓	False			·
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓ ✓				ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut		<b>√</b>	False			
	distributionPoint fullName	✓ ✓			S	
01-11	TullName	<b>V</b>				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties						
subjectAltNa		✓	False			
subjectKeylo	Rfc822Name	✓ ✓	F-1	0	D	Certificate Holder's email address
	keyldentifier	· ·	False		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
, ,	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.2
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	qualifier	✓ ✓			S	https://repository.luxtrust.lu
	policyQualifierID noticeNumbers	· ·	<del>                                     </del>		S	Id-qt-2 (User Notice)
	DisplayText	<b>√</b>				LuxTrust Certificate on SSCD compliant with ETSITS 102 042 NCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity
	Policyldentifier	<b>√</b>	<del>                                     </del>			Authentication and Data Encryption.
	Policyldentifier	<b>Y</b>		<u> </u>		0.4.0.2042.1.2

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

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





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

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

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

						cate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base Profi	le					
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	✓	False			
					FDV	Validated on duplicates.
signatureA	Mgorithm	✓	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	<b>✓</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	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." o similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	<b>√</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) of "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.



	LuxTrust non SSCD QCP Certificate Profile										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
	localityName	<b>√</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)					
	organizationalUnitName 1	<b>*</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).					
	organizationalUnitName 2	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item					
sub	jectPublicKeyInfo	✓	False								
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public					
	subjectPublicKey	✓		М		exponent: Fermat-4 (0x010001).					
Extensions											
Authority P	roperties										
authorityKe	eyldentifier	✓	False								
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key					
authorityInfoAccess		<b>✓</b>	False								
	AccessMethod	<b>✓</b>				Id-ad-2					
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt					
	AccessMethod	✓				Id-ad-1					
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3					
cRLDistrib	utionPoint	✓	False								
	distributionPoint	✓			S						
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl					
Subject Pro	pperties										
subjectAltN	lame	✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKey	ldentifier	✓	False								
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).					
Policy Prop	perties										
keyUsage		✓	True								
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificateP	olicies	✓	False								
	Policyldentifier	✓				1.3.171.1.10.3.3					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					



	LuxTrust non SSCD QCP Certificate Profile										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	DisplayText	<b>✓</b>				LuxTrust Qualified Certificate not on SSCD compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert					
	Policyldentifier	✓				0.4.0.1456.1.2					
QualifiedCe	ertificateStat										
	QcCompliance	✓		М	S	0.4.0.1862.1.1					
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcSSCD	✓				NOT SET					

#### 1.11.6 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 1.3.171.1.110.3.4>.

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

	LuxTrust non SSCD NCP Certificate Profile										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg		✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	lue	✓	False								
					D	Issuing CA Signature.					
issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Global Qualified CA x1					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	<b>~</b>			D	Certificate generation process date/time + 36 Months					
subject		✓	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	<b>✓</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character					



	LuxTrus	t non S	SSCD N	NCP Cer	tificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	✓		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	<b>✓</b>		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<b>✓</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	~		0	D	PRO products only: Company/institution department or other information item
subjectPubl	icKeyInfo	<b>√</b>	False			
	algorithm subjectPublicKey	<b>✓</b>		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions	SubjectFublickey	•		IVI		public exponent. Ferniat-4 (0x010001).
Authority						
Properties authorityKey	vldentifier	<b>✓</b>	False			
adinomyne	keyldentifier	· ·	1 4130			SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key
authorityInfo		<b>√</b>	False			Lil ad O
	AccessMethod accessLocation	✓ ✓				Id-ad-2  http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	· ·				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3
cRLDistribu		<b>√</b>	False			
	distributionPoint	<b>✓</b>			S	
Subject	fullName	•				http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Subject Properties						
subjectAltNa		<b>V</b>	False			
subjectKeylo	Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
SubjectNeyl	keyldentifier	<b>V</b>	raise		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 NCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	<b>√</b>			S	True				
	nonRepudiation				S	False				
	keyEncipherment	<b>✓</b>			S	True				
	dataEncipherment	<b>√</b>			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	<b>✓</b>				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption.				
	Policyldentifier	✓				0.4.0.2042.1.1				

# 1.11.7 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 Signing Server NCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.5" – 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 x1				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	<b>~</b>			D	Certificate generation process date/time + 36 Months				
subject		✓	False							



	LuxTrust S	Signing	Serve	r NCP C	ertifica	te Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	~		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	<b>✓</b>		0	D	Subject's email address
	title	<b>√</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>✓</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<b>✓</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	~		0	D	PRO products only: Company/institution department or other information item
subjectPubli		✓ ✓	False			Dublic Kour Kourlaneth, 2040 hit (DCA) up
	algorithm subjectPublicKey	<b>✓</b>		М		Public Key: Key length: 2048 bit (RSA) up to 4096bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	rldentifier	<b>√</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access AccessMethod	✓ ✓	False			Id-ad-2
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>✓</b>	<b> </b>			Id-ad-1
	accessLocation	<b>✓</b>	1			http://qca.ocsp.luxtrust.lu/3
cRLDistribut		✓	False			
	distributionPoint	<b>√</b>			S	
Cubicat	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCA.crl
Subject Properties						
subjectAltNa	ime	<b>√</b>	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		✓	False			



	LuxTrust Signing Server NCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	<b>√</b>			S	True				
	nonRepudiation				S	True				
	keyEncipherment	<b>✓</b>			S	True				
	dataEncipherment	<b>~</b>			S	True				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.5				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>√</b>				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Signature, Data or Entity Authentication and Data Encryption.				
	Policyldentifier	✓				0.4.0.2042.1.1				

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

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

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

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

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

LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services						
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x1
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months
subject		✓	False			



LuxTrust r	on SSCD NCP+ Public	: Cert	ificate	Profile	for Ma	ass Signature Services
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	commonName	<b>✓</b>		M	D	Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped
	countryName	✓		M	D	Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	emailAddress	✓		0	D	Subject's email address if available
	organizationName	<b>✓</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	localityName	<b>✓</b>		М	D	Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	<b>✓</b>		0	D	As provided by Subscriber
	organizationalUnitName 2	<b>✓</b>		0	D	As provided by Subscriber
subjectPublicKeyInfo		<b>√</b>	False			
	algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions Authority Properties						
authorityKeyldentifier		<b>√</b>	False			
	keyldentifier	<b>V</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfoAccess	AccessMethod	<b>√</b>	False			ld-ad-2
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistributionPoint		✓	False			
<u> </u>	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties		<b>√</b>	Fels			
subjectAltName	Rfc822Name	<b>✓</b>	False	0	D	Certificate Holder's email address
subjectKeyldentifier	NICOZZINGINE	·	False	-		Octunicate Floraci 3 ciriali address
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	digitalSignatura	<b>√</b>	True		S	False
	digitalSignature					1 alse
	nonRepudiation keyEncipherment	<b>✓</b>			S	True False
	dataEncipherment	<b>✓</b>			S	False
	- P					
certificatePolicies	Policyldentifier	<b>√</b>	False			1.3.171.1.1.10.3.6



LuxTrust n	LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>✓</b>				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Advanced electronic massive signature services.				
	Policyldentifier	✓				0.4.0.2042.1.2				

### 1.11.9 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 <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumb	er	✓	False								
					FDV	Validated on duplicates.					
signatureAl		✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	lue	✓	False								
_					D	Issuing CA Signature.					
Issuer	T	<b>√</b>	False		S						
	countryName	<b>√</b>			S	LU					
	commonName	✓			S	LuxTrust <b>Global Qualified</b> CA x <sup>1</sup>					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months					
Subject		✓	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	~		М	D	Concatenation of given name(s) and surname(s)					
	givenName	~		М	D	TEST ONLY + " " + As provided by Subscriber					
	surname	✓		М	D	As provided by Subscriber					
	countryName	✓		М	D	LU					
	emailAddress	✓		0	D	As provided by Subscriber					



	Lux	Trus	t Integ	ration	Certifi	cate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	Title	<b>√</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator"
	organizationName	<b>√</b>		M	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).
	organizationalUnitName 2	<b>√</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
-	subjectPublicKey	<b>✓</b>		М		exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	keyldentifier	√ √	False			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		<b>√</b>	False			11. 10
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut	distributionPoint	✓ ✓	False		S	
	fullName	<b>√</b>			<u> </u>	http://orld.codmonth./LTCCCA.cl
Subject	Tumamo					http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Properties			F-1:			
subjectAltNa	me Rfc822Name	<b>√</b>	False	0	D	N/A
subjectKeylo		<b>√</b>	False		U	IWA
oubjective yill	keyldentifier	<b>√</b>	i disc		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			
,	digitalSignature	<b>√</b>			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePo		<b>√</b>	False			1 2 474 4 4 40 2 7
	Policyldentifier policyQualifierID	✓ ✓			S	1.3.171.1.1.10.3.7 Id-qt-1 (CPS)
	Qualifier	<b>∨</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>√</b>			_	0.4.0.2042.1.3





### 1.11.10 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.

	LuxTru	st SSC	D LCP+	Integrat	ion Ce	rtificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False		ED)/	Malada da a desalta da
oianotura Ala	n a rith na	<b>✓</b>	Folos		FDV	Validated on duplicates.
signatureAl		· ·	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	Algorithm				3	RSA Encryption.
signatureVa	lue	<b>✓</b>	False			NOA Encryption.
Signatureva			1 0.00		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	leading of Colgnatare.
	countryName	<b>✓</b>	1 4.00		S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	<b>✓</b>	+		S	LuxTrust S.A.
Validity	o gamzanom ame	· /	False		-	Edition O.A.
· ananty	NotBefore	<b>√</b>	1 4100		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36
						Months
Subject	1	✓	False			
•	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
	Scriditalibei			141		· · · · · · · · · · · · · · · · · · ·
	commonName	✓		М	D	LGQCA XX SC PRI V3 (XX a number selected internally by LuxTrust)
	givenName	<b>√</b>		М	D	LGQCA XX (XX a number selected internally by LuxTrust)
	Surname	✓		М	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	N/A
	Title	✓		М	D	Private Person
subjectPubl		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		M		exponent: Fermat-4 (0x010001).
Extensions						
Authority						
Properties	uldontifier	<b>√</b>	Folso			
authorityKe		V /	False			CLIA 4 Lloop of the LuxTrust Clabel Qualified
	keyldentifier	•				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	<b>√</b>	False			On public Rey
add.only.mi	AccessMethod	· /	1 4130			ld-ad-2
	accessLocation	<b>√</b>	†			http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>✓</b>	+			Id-ad-1
	accessLocation	<b>→</b>	+			
•DI D!=:-!!			Fals :			http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribu		✓ ✓	False			
	distributionPoint	<b>✓</b>	-		S	
	fullName	<b>v</b>				http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl



	LuxTrus	st SSCI	LCP+	Integrat	ion Cer	rtificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Subject						
Properties						
subjectAltNa		<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeylo		✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.8
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	<b>✓</b>				LuxTrust INTEGRATION CERTIFICATE on SSCD compliant with ETSI TS 102 042 LCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Authentication and Encryption for Integration Purposes.
	Policyldentifier	✓				0.4.0.2042.1.3

# 1.11.11 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.

LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	gorithm	✓	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.			
signatureVal	lue	✓	False						
•					D	Issuing CA Signature.			
Issuer		✓	False		S				
•	countryName	✓			S	LU			



	Luxiru		_			te Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
Validity.	organizationName	✓ ✓	Falsa		S	LuxTrust S.A.
Validity	NotBefore	<b>✓</b>	False		D	Certificate generation process date/time
	NotAfter	<b>√</b>			D	Certificate generation process date/time
						36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	LGQCA XX CSS (XX a number selecte internally by LuxTrust) Concatenation of given name(s) ar surname(s) separated by a "Space character.
	givenName	~		М	D	LGQCA XX (XX a number selecte internally by LuxTrust) or Give name(s) as on ID document
	Surname	~		М	D	CSS or Surname(s) as on ID docume without indication "épouse", "ép." similar and the subsequent name(s)
	countryName	✓		М	D	LU or Nationality of holder (ISO3166)
	emailAddress	<b>√</b>	1	0	D	N/A
			-	-		
	Title	✓		М	D	Private Person
subjectPubl		<b>✓</b>	False			Dublic Koy Koy longth, 2049 bit /DCA
	Algorithm subjectPublicKey	<b>✓</b>		M		Public Key: Key length: 2048 bit (RSA public exponent: Fermat-4 (0x010001).
Extensions	Subjecti ubilottey			IVI		pasie experient: Ferrial T (exercee t):
Authority						
Properties	Adam (IC) a m		E-I			
authorityKe	keyldentifier	<b>√</b>	False			SHA-1 Hash of the LuxTrust Glob
	Royladinandi					Qualified CA public key
authorityInfo		✓	False			
	AccessMethod	✓ ✓				ld-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod accessLocation	<b>✓</b>			1	Id-ad-1
cRLDistribu		<b>✓</b>	False			http://qca.ocsp.luxtrust.lu/3
CKLDISTIBU	distributionPoint	<b>V</b> ✓	raise		S	
	fullName	· ·				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject						IND.//OH.Idxtrdot.id/E1OQO/IX
Properties						
subjectAltNa		✓	False		_	N/A
subjectKeyl	Rfc822Name	✓ ✓	False	0	D	N/A
<u>oudjootheyr</u>	keyldentifier	· ·	1 4136		Fixed	The Key Identifier comprises a four-lifeld with a 0100 value, followed by the least significant 60 bits of the SHA-1 has of the value or subjectPublicKey bit strir (tag, not including the length and numb of unused bit-string bits).
Policy						and the same of th
Properties			T			
keyUsage	digitalSignature	✓ ✓	True		S	True
						1140
	nonRepudiation				S	True
	keyEncipherment	<b>*</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo	olicies	✓	False			



	LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>✓</b>				INTEGRATION Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Signature, Data or Entity Auth. and Data Enc. for integration purposes				
	Policyldentifier	<b>√</b>				0.4.0.2042.1.3				

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

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

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

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

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

	LuxTrust SSCD LORA QCP+ Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg		✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	✓	False							
			<b>_</b>		D	Issuing CA Signature.				
Issuer		<b>√</b>	False		S					
	countryName	<b>√</b>			S	LU				
	commonName	· ·			S	LuxTrust Global Qualified CA x <sup>1</sup>				
	organizationName	<b>✓</b>			S	LuxTrust S.A.				
Validity	LN 45 f	<b>√</b>	False							
	NotBefore NotAfter	✓ ✓			D D	Certificate generation process date/time.				
	Notatter				D	Certificate generation process date/time + 36 Months				
Subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.				
	givenName	✓		М	D	Given name(s) as on ID card				
	Surname	<b>✓</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)				
	countryName	✓		М	D	Nationality of holder (ISO3166)				
	emailAddress	<b>✓</b>		0	D	Subject's email address				
	Title	✓		М	D	"LuxTrust RA Officer"				
	organizationName	✓		М	D	Constructed by LuxTrust				



	LuxTrust SSCD LORA QCP+ Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	localityName	✓		М	D	Country of RA				
	organizationalUnitName 1	<b>√</b>		М	D	RA code Constructed by LuxTrust				
	organizationalUnitName 2	✓		М	D	RAO code Constructed by LuxTrust				
subjectPubli		✓	False							
	Algorithm subjectPublicKey	<b>√</b>		N 4		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (0x010001).				
Extensions	SubjectFublickey	•		M		exponent. Fermat-4 (0x010001).				
Authority										
Properties										
authorityKey		✓	False							
	keyldentifier	<b>√</b>	Falsa			SHA-1 Hash of the LuxTrust Global Qualified CA public key				
authorityInfo	AccessMethod	<b>✓</b>	False			ld-ad-2				
	accessLocation	<b>∨</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt				
-	AccessMethod	<b>√</b>				Id-ad-1				
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>				
cRLDistribut		<b>√</b>	False			http://qca.ocsp.idxtrust.id/				
CIVEDISTIBUT	distributionPoint	<u>√</u>	1 disc		S					
-	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl				
Subject Properties										
subjectAltNa		✓	False							
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address				
subjectKeylo	dentifier keyldentifier	<b>√</b>	False		Fixed	The Key Identifier comprises a four-bit field				
	Reyldentiller	·			Tixod	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	digitalCignatura	<b>√</b>	True			Falsa				
	digitalSignature nonRepudiation	✓			S	False True				
	keyEncipherment	· ✓			S	False				
-	dataEncipherment	✓			S	False				
certificatePo		✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.10				
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)				
	Qualifier policyQualifierID	✓ ✓			S	https://repository.luxtrust.lu Id-qt-2 (User Notice)				
	noticeNumbers	•			3	lu-qi-2 (Oser Notice)				
	DisplayText	<b>√</b>				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Support of Qualified Electronic Signature for LRAO purposes				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCer										
	QcCompliance QcLimitValue	✓		М О	S D	As provided by LuxTrust S.A. in compliance				
	QcRetentionPeriod			0	D	with [3] As provided by LuxTrust S.A. in compliance with [3]				
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }				
						(				





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

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

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

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

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

	LuxTrus	st SSC	D LOR	A NCP+	Certific	cate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base						
Profile						
Version		✓	False			
0 1 - 1 1 1 1			F-1		S	Version 3 Value = "2"
SerialNumbe	er I	✓	False		FDV	Validated on duplicates.
signatureAlg	orithm	<b>√</b>	False		FDV	Validated on duplicates.
SignatureAig	Algorithm	•	1 4130		S	OID = "1.2.840.113549.1.1.11" - SHA256
	7.1g0.1					with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	N (D (	<b>√</b>	False			0.45
	NotBefore	✓ ✓			D	Certificate generation process date/time.
	NotAfter	•			D	Certificate generation process date/time + 36 Months
Subject		<b>√</b>	False			IVIOLITIES
Jubject		· ✓	i aise		_	Operical Nationals are a secretaristic at the st DAO
	serialNumber	<b>V</b>		М	D	Serial Number as constructed by LRAO
	commonName	✓		M	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	✓		M	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		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 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	✓		М	D	RAO code Constructed by LuxTrust
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		M		exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	<b>√</b>	False			
authorityney	Mentillei	,	i aise			



	LuxTru	st SSC	D LOR	A NCP+	Certific	cate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/3
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False			
	keyldentifier	Ť			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.11
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers DisplayText	<b>*</b>				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity Authentication and Data Encryption for LRAO purposes.
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

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

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

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

	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile								
Attribute	Attribute Field IN <sup>8</sup> CE <sup>9</sup> O/M <sup>10</sup> CO <sup>11</sup> Value								
Base Profile									
Version	Version		False						
					S	Version 3 Value = "2"			



LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
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 <sup>1</sup>			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 36 Months			
Subject		✓	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character			
	givenName	✓		М	D	Given name(s) as on ID card			
	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 – LRS"			
	organizationName	✓		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA			
	localityName	✓		М	D	Country of RA (as in articles of association)			
	organizationalUnitName 1	<b>✓</b>		М	D	RA code Constructed by LuxTrust			
	organizationalUnitName 2	<b>√</b>		0	D	RAO code Constructed by LuxTrust			
sub	jectPublicKeyInfo	<b>✓</b>	False						
	Algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA); public			
	subjectPublicKey	✓		М		exponent: Fermat-4 (0x010001).			
Extensions									
Authority P	roperties								
authorityKe	eyldentifier	✓	False						
	keyldentifier	✓				SHA-1 Hash of the <b>LuxTrust Global Qualified</b> CA public key			
authorityInf	oAccess	✓	False						
	AccessMethod	<b>√</b>				Id-ad-2			
		✓				http://ca.luxtrust.lu/LTGQCAx1.crt			



	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
	AccessMethod	✓				Id-ad-1					
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>					
cRLDistribu	utionPoint	✓	False								
	distributionPoint	✓			S						
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx1.crl					
Subject Pro	pperties										
subjectAltN	lame	✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKey	ldentifier	✓	False								
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).					
Policy Prop	perties										
keyUsage		✓	True								
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificateP	olicies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.12					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	<b>✓</b>				LuxTrust Qualified Certificate not SSCD compliant with ETSI TS101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Support of Advanced Electronic Signature for Mass LRAO purposes					
	Policyldentifier	✓				0.4.0.1456.1.2					
QualifiedCe	ertificateStat										
	QcCompliance	✓		М	S	0.4.0.1862.1.1					
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcSSCD	✓				NOT SET					

### 1.11.15 LuxTrust elD SSCD QCP+ Certificates supporting Qualified Signatures

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

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





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

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

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

The certificate re-key is not allowed.

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

	LuxTr	ust eID S	SCD Q	CP+ Ce	rtificat	te Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base						
Profile Version		<b>√</b>	False			
Version		•	i aise		S	Version 3 Value = "2"
SerialNumbe	er	<b>√</b>	False			voidien o value 2
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
_		,			D	Issuing CA Signature.
Issuer	- a company Allama	<b>√</b>	False		S	
	countryName commonName	<b>✓</b>			S	LU
						LuxTrust Global Qualified CA x <sup>1</sup>
Valialita	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NotBefore	<b>✓</b>	False		D	Contificate governtion process data/time
	NotAfter	<b>*</b>			D	Certificate generation process date/time.  Certificate generation process date/time + maximum 120 Months;  Certificate generation process date/time + 1 day for PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	✓		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	<b>√</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"Private Person"
	organizationalUnitName 1	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓		_		ld-ad-1





	LuxTrust elD SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value				
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3				
cRLDistribut	ionPoint	✓	False							
	distributionPoint	✓			S					
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl				
Subject Properties										
subjectAltNa		✓	False							
	Rfc822Name	✓		0	D	Subject email address				
subjectKeyld		✓	False							
	keyldentifier	<b>*</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	<b>✓</b>			S	False				
	nonRepudiation	<b>✓</b>			S	True				
	keyEncipherment	<b>√</b>			S	False				
	dataEncipherment	<b>√</b>			S	False				
certificatePo		<b>√</b>	False			101711110010				
	Policyldentifier	<b>√</b>			_	1.3.171.1.1.10.3.13				
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers DisplayText	<b>*</b>				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Support of Qualified Electronic Signature.				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCer										
	QcCompliance	✓		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcSSCD	✓		M	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }				

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

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

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

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

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

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



	Lux	Trust	SSCDN	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Base						
Profile Version		<b>√</b>	False			
Version		•	raise		S	Version 3 Value = "2"
SerialNumbe	r	✓	False			voision o value 2
					FDV	Validated on duplicates.
signatureAlg		✓	False			OID = "1.2.840.113549.1.1.11" - SHA256 w
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 W RSA Encryption.
signatureVal	ue	✓	False			NOA Elicrypholi.
					D	Issuing CA Signature.
issuer	T	<b>√</b>	False		S	
	countryName commonName	✓ ✓			S	LU
		<b>V</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>
Validity	organizationName	<b>V</b> ✓	False		- 5	LuxTrust S.A.
validity	NotBefore	·	i aise		D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time maximum 120 Months; Certificate generation process date/time + day for PSEUDONYM Certificate
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) a surname(s) separated by the space characteristics.
	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 indicat "épouse", "ép." or similar and the subsequ name(s) or as provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	Subject's email address
	title	<b>√</b>		M	D	"Private Person"
	organizationalUnitName	✓		0	D	If the holder is underage: "Mineur jusqu'à : (Date of birth + 18 years).
subjectPubli	cKevinfo	<b>√</b>	False			(Zate or zinar i re yearo).
subjecti ubii	algorithm	√ ·	1 also			Public Key: Key length: 2048 bit up to 4096
	subjectPublicKey	<b>√</b>		М		(RSA); public exponent: Ferma (0x010001).
Extensions Authority						
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualif
	A	-	Гаја			CA x public key
authorityInfo	AccessMethod	<b>√</b>	False			ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	· ·			1	http://gca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut		<b>√</b>	False			TREAT GOLDOOD TUNIT GOLTU
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties						7
subjectAltNa		✓	False			
	Rfc822Name	<b>√</b>		0	D	Subject email address
subjectKeyld		<b>√</b>	False		F	71 17 17 17 17
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit fi with a 0100 value, followed by the le significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag, including the length and number of unus bit-string bits).



	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	True				
	nonRepudiation				S	False				
	keyEncipherment	✓			S	True				
	dataEncipherment	✓			S	True				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.14				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>√</b>				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity Authentication and Data Encryption.				
	Policyldentifier	✓				0.4.0.2042.1.2				

### 1.11.17 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 <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	signatureAlgorithm		False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	ue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				



Subject   Subj		LuxTrust eID SS	SCD LCP	Integra	tion Sig	nature	e Certificate Profile
Subject   Subject   SerialNumber   V   False   SerialNumber   V   False   SerialNumber   V   False   SerialNumber   V   M   D   SerialNumber   SerialNumbe	Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Subject  Subject  SerialNumber   SerialNumber   SerialNumber   SerialNumber   SerialNumber   SerialNumber   SerialNumber   SerialNumber   SerialNumber   M D SerialNumber as constructed by LRAO  Concateration of given name(s) sumame(s) separated by the space clara   givenName   Surname   Surname   Surname   Surname   Surname   Surname   Surname   Surname   Surname   Subject by the RNCID  Subject semail address   False   SubjectPublicKeyInfo   SubjectPublicKeyInfo   SubjectPublicKeyInfo   SubjectPublicKeyInfo   SubjectPublicKey   SubjectPublicKey   M (RSA); public exponent: Fermat-4 (0x0100   Extensions   Authority   Properties   SubjectPublicKey   False   AccessMethod		NotAfter	✓			D	Certificate generation process date/time + 12
Subject							
Subject							
SerialNumber	Subject	<u> </u>	✓	False			day for i Scoboli i wi certificate
commonName		serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
givenName		Scriantamber			101		, ,
surname		commonName	✓		М	D	Concatenation of given name(s) and surname(s) separated by the space character
CountryName		givenName	✓		М	D	specimen-x provided by the RNCID
emailAddress		surname	✓		М	D	specimen-x as provided by the RNCID
title		countryName	✓		М	D	LU
organizationalUnitName 1  organizationalUnitName 1  organizationalUnitName 1  if the holder is underage: "Mineur jusqu's (Date of birth + 18 years).  If the holder is underage: "Mineur jusqu's (Date of birth + 18 years).  Algorithm		emailAddress	<b>√</b>		0	D	specimen-x Subject's email address as provided by the RNCID
SubjectPublicKeyInfo		title	✓		М	D	"Private Person"
Algorithm			✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
Algorithm	subjectPubli		✓	False			
Extensions   Authority   Properties   authority/Reyldentifier		Algorithm					Public Key: Key length: 2048bit up to 4096bit
Authority   Properties   authorityKeyldentifier		subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (0x010001).
Properties   authorityKeyIdentifier   Fixed   SHA-1 Hash of the LuxTrust Global Qual CAx public key							
authorityKeyIdentifier							
Reyldentifier		dentifier	✓	False			
AccessMethod   Acce			✓				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
accessLocation	authorityInfo	Access	✓	False			or the public hely
AccessMethod / Id-ad-1 accessLocation / Id-ad-1 http://gca.ocsp.luxtrust.lu/Errorl Bookmark efined.  CRLDistributionPoint / False  distributionPoint / Subject Properties subjectAltName / False    Rfc82Name / False    SubjectKeyldentifier / False    keyldentifier / False    Fixed    Refull Add-1 http://crl.luxtrust.lu/LTGQCAx Id-1 http://crl.luxtrust.lu							ld-ad-2
CRLDistributionPoint		accessLocation	✓				
CRLDistributionPoint							
distributionPoint fullName		accessLocation	✓				
Subject   Properties   Subject   National Properties   Subject   Properties   Subject   National Properties   Subject   National Properties   Subject   National Properties   Subject   National Properties   National Pr	cRLDistribut			False			
Subject Properties subjectAltName  Rfc822Name  Rfc822Name  Rfc822Name  Rfc822Name  False  Rfc822Name  False  Fixed  The Key Identifier comprises a four-bit with a 0100 value, followed by the significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag including the length and number of unuser string bits).  Policy Properties  keyUsage  digitalSignature nonRepudiation keyEncipherment dataEncipherment  dataEncipherment  Fixed  The Key Identifier comprises a four-bit with a 0100 value, followed by the significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag including the length and number of unuser string bits).  Policy Properties  keyUsage   True  S False  nonRepudiation  V S False  certificatePolicies  False  PolicyQualifier  V False  PolicyQualifierID  V S Id-qt-1 (CPS) qualifier  DisplayText  LuxTrust INTEGRATION CERTIFICATE elD SSCD compliant with ETSI TS 102						S	
Properties   SubjectAltName   V   False   SubjectAltName   V   False   Provided by the RNCID		fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Rfc822Name	Subject						
Rfc822Name		l ma	-/	Falco			
SubjectKeyIdentifier   False   Fixed   Fixed   The Key Identifier comprises a four-bit with a 0100 value, followed by the significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag including the length and number of unuser string bits).    Policy	SubjectAlliva			i aise	0	D	specimen-x Subject's email address as
Reyldentifier   Fixed   The Key Identifier comprises a four-bit with a 0100 value, followed by the significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag including the length and number of unuser string bits).    Policy	subject/ov/s		-/	Folso			
with a 0100 value, followed by the significant 60 bits of the SHA-1 hash of value or subjectPublicKey bit string (tag including the length and number of unuser string bits).    Policy Properties	Subjectivelyic		<b>✓</b>	raise		Fixed	The Key Identifier comprises a four-hit field
Properties   ReyUsage   V True   S False   S							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-
CertificatePolicies							
nonRepudiation				True			
ReyEncipherment   V	_						
CertificatePolicies   V							
CertificatePolicies       PolicyIdentifier     ✓       policyQualifierID     ✓       qualifier     ✓       policyQualifierID     ✓       noticeNumbers     ✓       DisplayText     ✓       LuxTrust INTEGRATION CERTIFICATE eID SSCD compliant with ETSI TS 102							
PolicyIdentifier   ✓	certificatePo			False			
qualifier     ✓     S     https://repository.luxtrust.lu       policyQualifierID     ✓     S     Id-qt-2 (User Notice)       noticeNumbers     User Notice     LuxTrust INTEGRATION CERTIFICATE       DisplayText     ✓     LuxTrust INTEGRATION CERTIFICATE       eID SSCD compliant with ETSI TS 102							
policyQualifierID ✓ S Id-qt-2 (User Notice) noticeNumbers DisplayText ✓ LuxTrust INTEGRATION CERTIFICATE elD SSCD compliant with ETSI TS 102							
noticeNumbers  DisplayText  ✓  LuxTrust INTEGRATION CERTIFICATE eID SSCD compliant with ETSI TS 102				ļ			
DisplayText   ✓ LuxTrust INTEGRATION CERTIFICATE eID SSCD compliant with ETSI TS 102			· ·			8	iu-qr-∠ (User Notice)
			<b>*</b>				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Electronic signature for Integration Purposes



	LuxTrust eID SSCD LCP Integration Signature Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCer	QualifiedCertificateStat									
•	QcCompliance	✓		M	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance				
						with [3]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance				
						with [3]				

### 1.11.18 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 <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version	•	✓	False							
					S	Version 3 Value = "2"				
SerialNumb	er	✓	False							
					FDV	Validated on duplicates.				
signatureAl	<u> </u>	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	✓	False							
					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	<b>~</b>			D	Certificate generation process date/time + 12 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate				
subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) separated by the space character				
	givenName	✓		М	D	specimen-x provided by the RNCID				
	surname	✓		М	D	specimen-x provided by the RNCID				



	LuxTrust el	SSCE	LCP I	ntegratio	n AE Ce	ertificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	specimen-x Subject's email address as provided by the RNCID
	title	✓		М	D	"Private Person"
	organizationalUnitName 1	<b>√</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli		✓	False			
	algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit up to 4096bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey		✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfo		✓	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod accessLocation	<b>√</b>				Id-ad-1
- DI Di-(-il		<b>√</b>	F-1			http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut	distributionPoint	<b>✓</b>	False		S	
	fullName	<i>'</i>			3	http://crl.luxtrust.lu/LTGQCAx1.crl
Subject	ramamo	·				nttp://cn.iuxtrust.iu/LTGQCAX .cn
Properties						
subjectAltNa	me Rfc822Name	<b>√</b>	False	0	D	anaciman y Cubicatia amail address as
	Ricozzinailie	•			D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo		✓	False			
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
, ,	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo		<b>√</b>	False			
	PolicyIdentifier	<b>√</b>			-	1.3.171.1.1.10.3.17
	policyQualifierID qualifier	<b>✓</b>			S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	noticeNumbers					- 1 - ()
		✓				LuxTrust INTEGRATION CERTIFICATE on
	DisplayText	·				eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Authentication and Encryption for Integration Purposes

## 1.11.19 LuxTrust NCP+ Certificates supporting SEAL Signature Services

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





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

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

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

LuxTrust r	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ass Signature Services
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	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	T	✓	False		_	
					D	Issuing CA Signature.
Issuer	I	<b>✓</b>	False		S	
	countryName	<b>✓</b>			S	LU
	commonName				S	LuxTrust Global Qualified CA x <sup>1</sup>
[	organizationName	✓			S	LuxTrust S.A.
Validity	I Nat Batana	<b>✓</b>	False		_	0-400-1-
	NotBefore				D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
subject		✓	False			
	commonName	<b>✓</b>		М	D	Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped
	countryName	<b>✓</b>		М	D	Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	emailAddress	✓		0	D	Subject's email address if available
	organizationName	<b>✓</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	localityName	~		М	D	Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName 1	<b>✓</b>		0	D	As provided by Subscriber
	organizationalUnitName 2	<b>√</b>		0	D	As provided by Subscriber
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	<b>√</b>		М		public exponent: Fermat-4 (0x010001).
Extensions						`



LuxTrust r	non SSCD NCP+ Pub	lic Cert	ificate	Profile	for Ma	ass Signature Services
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Authority Properties						
authorityKeyldentifier		✓	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfoAccess		✓	False			
•	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3
cRLDistributionPoint		<b>✓</b>	False			TREP://qod.ocop.ndxtrdot.nd/
CINEDISTRIBUTION ONL	distributionPoint	· /	1 4130		S	
	fullName	· /				http://crl.luxtrust.lu/LTGQCAx1.crl
Cubicat Duamenties	Tamvame					http://ch.iuxtrust.iu/LTGQCAX .ch
Subject Properties subject AltName		1	Fala:			
SubjectAitName	Diagoniama	V /	False		_	Contificate Haldow's amount address
	Rfc822Name	<b>→</b>	Fala a	0	D	Certificate Holder's email address
subjectKeyldentifier	keyldentifier	V /	False		Fixed	The Key Identifier comprises a four-bit
						field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation				S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePolicies		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.15
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	<b>✓</b>				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Advanced electronic seal signature services.
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2

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

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

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

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

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

	LuxTrust SSL Server LCP Certificate Profile								
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
Base									
Profile									
Version									
					S	Version 3 Value = "2"			





	LuxTrust	SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" -
signatureVal		<b>√</b>	False			SHA256 with RSA Encryption.
Signatureval	ue 	•	raise		D	Issuing CA Signature.
issuer		✓	False		S	recalling of Congrictation
	countryName	✓			S	LU
	commonName	<b>✓</b>			S	LuxTrust <b>SSL</b> CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		<b>√</b>	False		_	
	NotBefore	✓			D	Certificate generation process
	NotAfter	<b>✓</b>			D	date/time.  Certificate generation process
	Notate					date/time + 12;24;36 Months
subject		✓	False			, ,
	countryName			М	D	Country in which the company's or
	,					institution's registered office is
		✓				established (as specified in the
						memorandum and articles of association). (ISO3166)
				-		association). (1505100)
	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)
	Commonivanie			IVI		of application/server – Exact and full
		<b>✓</b>				URL for a Web Server or IP address or
						unique name of server.
	serialNumber	,		0	D	Serial Number as provided by
		<b>*</b>				subscriber
	emailAddress			0	D	Subject's email address
		✓				Cabjeet o chail address
subjectPubli		✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA);
Futaratan	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).
Extensions Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA
			F			public key
authorityInfo	Access AccessMethod	✓ ✓	False			Id-ad-1
	accessLocation	<b>✓</b>		<del> </del>		http://ssl.ocsp.luxtrust.lu <sup>12</sup>
	AccessMethod	<b>√</b>		-		Id-ad-2
	accessLocation	<b>✓</b>		-		http://ca.luxtrust.lu/LTSSLCAx <sup>1</sup> .crt
cRLDistribut		<b>√</b>	False			mup.//ca.iuxirusi.iu/LT33LCAX .CII
CIVEDISHIDUI	distributionPoint	<b>✓</b>	1 0130		S	
			<u> </u>	1		<u>l</u>

<sup>&</sup>lt;sup>12</sup> Since SSL CA 2



	LuxTrust	SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx.crl
SCTs		✓	False	М	D	Values returned by Log Servers
Subject Properties						
subjectAltNa	ame	<b>√</b>	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
					1	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
	Cultinat Althorna dNCNama					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
	SubjectAltName-dNSName			0		name of server.  FQDN (Fully Qualified Domain Name)
	SubjectAttName-dNSName	<b>√</b>				of application/server – Exact DNS for a
		•				Web Server or IP address or unique
	SubjectAltName-dNSName			0		name of server.  FQDN (Fully Qualified Domain Name)
		<b>√</b>				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-URL			0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full
		✓				second URL for a Web Server or IP
	Out to a (Alch)				1	address or unique name of server.
	SubjectAltName-URL			0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full
		<b>√</b>				second URL for a Web Server or IP
	SubjectAltName-URL			0		address or unique name of server.  FQDN (Fully Qualified Domain Name)
	SubjectAttivatile-UKL	<b>√</b>				of application/server – Exact and full
		•				second URL for a Web Server or IP
	SubjectAltName-URL			0		address or unique name of server.  FQDN (Fully Qualified Domain Name)
	Casjoornittuille-OitE	<b>√</b>				of application/server - Exact and full
		•				second URL for a Web Server or IP
	SubjectAltName-URL			0		address or unique name of server.  FQDN (Fully Qualified Domain Name)
		✓				of application/server - Exact and full
					1	second URL for a Web Server or IP address or unique name of server.



	LuxTrust SSL Server LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	SubjectAltName-URL	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.				
	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	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy Properties										
keyUsage		✓	True							
.,	digitalSignature	<b>√</b>			S	True				
	nonRepudiation	<b>√</b>			S	False				
	keyEncipherment	<b>√</b>			S	True				
	dataEncipherment	<b>√</b>			S	True				
certificatePo		✓	False							
	Policyldentifier	✓				1.3.171.1.10.5.1				
	policyQualifierID	<b>√</b>	1	1	S	Id-qt-1 (CPS)				
	qualifier	<b>√</b>	1	1	S	https://repository.luxtrust.lu				
	Policyldentifier Policyldentifier	<b>√</b>				0.4.0.2042.1.7 2.23.140.1.2.2				
Extended Ke	l ey Usage	<b>✓</b>	False							
	serverAuth	<b>√</b>			S	True				
	clientAuth	✓			S	True				
	emailProtection	✓			S	True				

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

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

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

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

### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

Identify the legal entity that controls a Web site: Provide a reasonable assurance to the user of an Internet browser
that the Web site the user is accessing is controlled by a specific legal entity identified in the EV SSL Certificate by name,





address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and

• Enable encrypted communications with a Web site: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

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

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

#### Prohibited Certificate uses:

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

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

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

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

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

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

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

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

	SSL/TLS Extended Validation Server Certificates								
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	jorithm	✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	ue	✓	False						
					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	<b>√</b>			S	LU			
	commonName	<b>√</b>			S	LuxTrust <b>SSL</b> CA x <sup>1</sup>			





SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
	organizationName	✓			S	LuxTrust S.A.			
Validity	_	✓	False						
	NotBefore	✓			D	Certificate generation process date/time			
	NotAfter	✓			D	Certificate generation process date/time + 12;24 Months			
subject		✓	False						
	countryName (OID: 2.5.4.6)	✓		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles association). (ISO3166)			
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	<b>~</b>		М	D	Contains the country information specified using the applicable ISC country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates a the country level, at state/pr.			
	stateOrProvinceName (OID: 2.5.4.8)	<b>√</b>		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)			
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	<b>✓</b>		0	D	Contains the jurisdiction for the applicable Incorporating Agency of Registration Agency at the state of province level MUST include both country and state or province information.			
	localityName (2.5.4.7)	<b>√</b>		М	D	Location in which the company' registered office is established (a specified in the memorandum an articles of association or an equivaler document)			
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>√</b>		0	D	Jurisdiction for the applicabl Incorporating Agency or Registratio Agency at the locality level MUST includ the country and state or provinc information, where the state or provinc regulates the registration of the entities at the locality level, as well as the locality information.			
	organizationName (OID: 2.5.4.10)	<b>√</b>		М	D	Full legal organization name as listed in the official records of the Incorporating of Registration Agency in the Subject' Jurisdiction of Incorporation of Registration or as otherwise verified by the CA as provided herein.			
	businessCategory (OID: 2.5.4.15)	<b>√</b>		М	D	Depending on the Subject qualifications this field contains one of the followin String:  Private Organization Government Entity			



	SSL/TLS Ex	tended \	/alidatio	on Serve	er Cert	ificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	serialNumber			М	D	See EV Guidelines [13] :
	(OID: 2.5.4.5)	<b>~</b>				For Private Organizations, this field MUST contain the Registration (o 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 SHALI enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode			0	D	Postal code of the subject place of
	(OID: 2.5.4.17)	✓				business.
	streetAddress			0	D	Number and Street of the physica
	(OID: 2.5.4.9)	✓				location of the subject
subjectPubli	cKevinfo	<b>✓</b>	False			
Subjecti ubii	algorithm	· ·	i aisc			Public Key: Key length: 2048 bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	<b>√</b>	False			
uumonnyntoj	keyldentifier	<b>✓</b>	1 4100			SHA-1 Hash of the LuxTrust SSL CA
						public key
authorityInfo		<b>√</b>	False			
	AccessMethod accessLocation	<b>V</b> ✓				ld-ad-1 http://ssl.ocsp.luxtrust.lu 12
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTSSLCAx <sup>1</sup> .crt
cRLDistribut	tionPoint	<b>✓</b>	False			intp://od.idxtrdot.id/E1OOEO/tX
	distributionPoint	<b>✓</b>	1 4100		S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTSSLCAx1.crl
SCTs		✓	False	М	D	Values returned by Log Servers
Subject Properties						
subjectAltNa		✓	False			
	SubjectAltName-dNSName	<b>✓</b>		M		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Well 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 We 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 Ext	ended \	/alidatio	on Serv	er Cert	ificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
7.11.10000	SubjectAltName-dNSName	√		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyld	entifier	<b>√</b>	False			
	keyldentifier	<b>\</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	di nita 10i nu atau	<b>√</b>	True		-	Tour
	digitalSignature nonRepudiation	✓ ✓			S	True False
	keyEncipherment	<b>v</b> ✓			S	True
	dataEncipherment	<b>√</b>			S	True
eortific - t - P	lision		F-1-			
certificatePo	licies Policyldentifier	✓ ✓	False			13171111052
	policyQualifierID	<b>∨</b>			S	1.3.171.1.1.10.5.2 Id-qt-1 (CPS)
	qualifier	<b>V</b> ✓	<del>                                     </del>		S	https://repository.luxtrust.lu
	quainiei		I	l	<u> </u>	intpo.//Tepooltory.luxtruot.lu



	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	Policyldentifier	✓				0.4.0.2042.1.4				
	Policyldentifier	✓				2.23.140.1.1				
Extended Ke	y Usage	<b>✓</b>	False							
	serverAuth	✓			S	True				
	clientAuth	✓			S	True				
	emailProtection	✓			S	False				

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

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

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

### Prohibited Certificate uses:

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

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

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

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

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

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





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

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

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

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

Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base	1 1010		<u> </u>			Value
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	False			
					FDV	Validated on duplicates.
signatureA		✓	False		_	
	Algorithm				S	OID = "1.2.840.113549.1.1.11" SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer	1	<b>✓</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	·			S	LuxTrust <b>SSL</b> CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False		_	
	NotBefore	<b>√</b>			D	Certificate generation proces date/time.
	NotAfter	<b>√</b>			D	Certificate generation proces date/time + 12;24 Months
Subject		✓	False			
	countryName (OID: 2.5.4.6)	<b>✓</b>		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles or association). (ISO3166)
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	✓		М	D	Contains the country information specified using the applicable ISC country code for the jurisdiction of Incorporation for the Incorporation Agency or Jurisdiction of Registration for a Registration Agency that operates at the countril level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	<b>✓</b>		М	D	State or Province in which th company's registered office i established (as specified in th memorandum and articles cassociation or an equivaler document)
	jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	<b>~</b>		0	D	Contains the jurisdiction for the applicable Incorporating Agency of Registration Agency at the state of province level MUST include bot country and state or province information,



	SSL/TLS Extended Validation	Serve	er Certif	icates	on Sec	eure User Device
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	localityName (2.5.4.7)	<b>✓</b>		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>*</b>		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	<b>√</b>		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein
	businessCategory (OID: 2.5.4.15)	<b>✓</b>		М	D	Depending on the Subject qualifications, this field contains one of the following String:  • Private Organization  • Government Entity
	serialNumber (OID: 2.5.4.5)	<b>✓</b>		M	D	See EV Guidelines [13]:  For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.  For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	<b>√</b>		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	<b>✓</b>		0	D	Number and Street of the physical location of the subject
subjectPubli	cKeyInfo Algorithm subjectPublicKey	✓ ✓ ✓	False	M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (0x010001).
Extensions Authority						
Properties						
authorityKey	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfo		<b>√</b>	False			14 04 4
	AccessMethod	✓		]		ld-ad-1



	SSL/TLS Extended Validation	n Serv	er Certi	ficates	on Sec	cure User Device
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	accessLocation	<b>√</b>		0,111		http://ssl.ocsp.luxtrust.lu 12
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx1.crt
cRLDistribu	tionPoint	<b>√</b>	False			IREP.// Od. Idaki dot. Id/ ET GOLO/ IX
CINEDISTIBLE	distributionPoint	· /	1 also		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCAx1.crl
Subject						TREP.//OHIIGARI GOLIG/ET GOLO/ IX 1.011
Properties						
subjectAltN	ame	<b>✓</b>	False			
·	SubjectAltName-dNSName	<b>√</b>		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for 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	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.



	SSL/TLS Extended Validation	Serve	er Certif	ficates	on Sec	cure User Device
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	SubjectAltName-dNSName	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>*</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	·		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
subjectKeylo		✓	False			
	keyldentifier				Fixe d	The Key Identifier comprises a four- bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						,
keyUsage		<b>✓</b>	True			
.,	digitalSignature	<b>✓</b>			S	True
	nonRepudiation	<b>~</b>			S	False
	keyEncipherment	<b>✓</b>			Ø	True
	dataEncipherment	<b>✓</b>			S	True
certificatePo		✓	False			
	Policyldentifier	<b>✓</b>				1.3.171.1.1.10.5.3
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
Extended Ke	Policyldentifier	<b>✓</b>	False			0.4.0.2042.1.5
			1 4.00			
	serverAuth	<b>√</b>			S	True
	clientAuth	<b>√</b>		ļ	S	True
	emailProtection	✓		<u> </u>	S	False

## 1.11.23 LuxTrust Object (or Code) Signing Certificates

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

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

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., <1.3.171.1.1.10.5.4>. This profile is not currently implemented.

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



	Lu	xTrust l	_CP Code	Signing C	ertificate I	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base Profi	ile			I		
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	SerialNumber		False			
					FDV	Validated on duplicates.
signature/	signatureAlgorithm		False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature\	/alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust <b>SSL</b> CA x <sup>1</sup>
	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	<b>√</b>		М	D	Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	<b>✓</b>		0	D	
	localityName	✓		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	<b>√</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association of an equivalent document)
	organizationalUnitName1	✓		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber
	commonName	<b>✓</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association of an equivalent document)
	serialNumber	<b>√</b>		0	D	NA or Serial Number as provided by subscriber
	emailAddress	✓		0	D	Subject's email address if available
subjectPu	blicKeyInfo	✓	False			
Algorithm subjectPublicKey		✓				Public Key: Key length: 2048 (RSA); public
		✓		М		exponent: Fermat-4 (0x010001).
Extension	s					
Authority	Properties					
authorityK	(eyldentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key



LuxTrust LCP Code Signing Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value			
authoritylı	authorityInfoAccess		False						
	AccessMethod	✓				Id-ad-1			
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 12			
	AccessMethod	✓				ld-ad-2			
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx1.crt			
CRLDistril	butionPoint	✓	False						
	distributionPoint	✓			S				
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx1.crl			
Subject Pi	roperties								
subjectAlt	Name	✓	False						
	Rfc822Name	✓		0	D	Subject's email address			
subjectKe	yldentifier	✓	False						
	keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).			
Policy Pro	perties								
keyUsage		✓	True						
	digitalSignature	✓			S	True			
	nonRepudiation	✓			S	False			
	keyEncipherment	✓			S	False			
	dataEncipherment	✓			S	False			
certificate	Policies	✓	False						
	Policyldentifier	✓			S	1.3.171.1.1.10.5.4			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	Qualifier	✓			S	http://repository.luxtrust.lu			
	policyQualifierID	✓			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	<b>✓</b>			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on <a href="http://repository.luxtrust.lu">http://repository.luxtrust.lu</a> . Signed by an SSL CA.			
	Policyldentifier	✓			S	0.4.0.2042.1.3			
Extended	Key Usage	✓	False						
	Object Signing	✓			S	Set			

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

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

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

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





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

			Ol:	00.0	ere	D. Cl.
	LuxTrus					
Attribute Base	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Profile						
Version		✓	False			
0					S	Version 3 Value = "2"
SerialNumbe	er 	✓	False		FDV	Validated on duplicates.
signatureAlg	ı Jorithm	<b>✓</b>	False		TDV	validated on duplicates.
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVal	ue 	✓	False		D	Issuing CA Signature.
Issuer		<b>✓</b>	False		S	issuing on dignature.
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust <b>SSL</b> CA <sup>1</sup>
	organizationName	<b>√</b>	<u> </u>		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Cortificate generation process data/time
	NotAfter	V /			D	Certificate generation process date/time.  Certificate generation process date/time +
						12; 24; 36 Months
Subject		✓	False			
	countryName			М	D	Country in which the company's or
		✓				institution's registered office is established
						(as specified in the memorandum and articles of association). (ISO3166)
						articles of accordance (1). (1999-199)
	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)
	annoningtion Name			М	D	, ,
	organizationName			IVI		Names as in articles of association, including the legal form (as specified in
		<b>✓</b>				the memorandum and articles of
						association or an equivalent document)
	organizationalUnitName 1			0	D	As provided by Subscriber
	3	<b>✓</b>				, , , , , , , , , , , , , , , , , , , ,
	organizationalUnitName 2	<b>√</b>		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
		✓				,
		1	<b>.</b>			
subjectPubli	cKeyInfo Algorithm	✓ ✓	False			Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	<b>✓</b>		M	†	public exponent: Fermat-4 (0x010001).
Extensions						
Authority						
Properties authorityKey	Identifier	<b>✓</b>	Eolog			
authorityNey	keyldentifier	<b>✓</b>	False			SHA-1 Hash of the LuxTrust SSL CA
						public key
authorityInfo		<b>√</b>	False			
	AccessMethod	<b>√</b>			-	ld-ad-1
	accessLocation	<b>√</b>		1	1	http://ssl.ocsp.luxtrust.lu 12
	AccessMethod accessLocation	✓ ✓			1	Id-ad-2
cRLDistribut		<b>V</b> ✓	False			http://ca.luxtrust.lu/LTSSLCAx1.crt
CIVEDISHIBUT	distributionPoint	<b>✓</b>	i aise		S	
	fullName	✓			†	http://crl.luxtrust.lu/LTSSLCAx1.crl
Subject						
Properties						
subjectAltNa	ime	✓	False			



	LuxTru	st SSL	Client L	CP Cert	ificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>*</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.5.5
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	✓				0.4.0.2042.1.3
Extended Ke	ey Usage	<b>√</b>	False			
·	serverAuth	✓			S	False
	clientAuth	✓			S	True
	emailProtection	✓			S	True

#### 1.11.25 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-v	v Extend	led Valid	dation S	erver	Certificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	r	✓	False			
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust <b>SSL</b> CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 12;24 Months
subject		✓	False			
	countryName (OID: 2.5.4.6)	<b>✓</b>		М	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)



	SSL/TLS QCP-w	Extende	ed Valid	lation S	erver (	Certificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	✓		М	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.
	stateOrProvinceName (OID: 2.5.4.8)	<b>√</b>		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	✓		0	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName (2.5.4.7)	✓		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>√</b>		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	✓		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	<b>√</b>		М	D	Depending on the Subject qualifications, this field contains one of the following String:  Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	<b>✓</b>		М	D	See EV Guidelines [13]:  For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.  For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	<b>√</b>		0	D	Postal code of the subject place of business.



	SSL/TLS QCP-v	v Extend	ed Valid	dation S	erver	Certificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	streetAddress			0	D	Number and Street of the physic
	(OID: 2.5.4.9)	<b>✓</b>				location of the subject
subjectPubli	cKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001)
Extensions						
Authority Properties						
authorityKey		<b>✓</b>	False			SHA-1 Hash of the LuxTrust SSL (
	keyldentifier					public key
authorityInfo		✓	False			
	AccessMethod	✓ ✓				Id-ad-1
	accessLocation	·				http://ssl.ocsp.luxtrust.lu 12
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx1.crt
RLDistribut		<b>√</b>	False			
	distributionPoint	✓	1		S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx1.crl
CTs		✓	False	М	D	Values returned by Log Servers
Subject Properties						
ubjectAltNa		✓	False			
	SubjectAltName-dNSName	<b>✓</b>		M		FQDN (Fully Qualified Domain Name) application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by a subject and to be associated with a Subject's server. Wildcard name allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by subject and to be associated with Subject's server. Wildcard name allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by subject and to be associated with Subject's server. Wildcard name allowed for EV SSL Certificates
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by subject and to be associated with Subject's server. Wildcard name allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>*</b>		0		FQDN (Fully Qualified Domain Name) application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by subject and to be associated with Subject's server. Wildcard name allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>*</b>		0		FQDN (Fully Qualified Domain Name) application/server – Exact DNS for a W Server or IP address or unique name server, owned or controlled by subject and to be associated with Subject's server. Wildcard name allowed for EV SSL Certificates.



	SSL/TLS QCP-v	v Extend	ed Valid	lation S	erver (	Certificates
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not
	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
	SubjectAltName-dNSName			0		Subject's server. Wildcard name not allowed for EV SSL Certificates.  FQDN (Fully Qualified Domain Name) of
	oubject-autume-unortaine	<b>✓</b>				application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>*</b>		O		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyld	entifier	<b>√</b>	False		F: .	71 17 11 27
	keyldentifier	·			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	digitalSignature	<b>√</b>	True		S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePol		<b>√</b>	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.5.6
	policyQualifierID	✓ ✓			S	Id-qt-1 (CPS)
	qualifier Policyldentifier	<b>*</b>			S	https://repository.luxtrust.lu 0.4.0.194112.1.4
	Policyldentifier	✓				0.4.0.2042.1.4
	Policyldentifier	<b>√</b>			S	2.23.140.1.1
Extended Ke		<b>V</b>	False			
	serverAuth	<b>√</b>			S	True
	clientAuth	<b>√</b>			S	True
QualifiedCert	emailProtection iificateStat	✓ ✓	False		S	False
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	✓		М	S	URL=https://www.luxtrust.com/repositor y
	QcType (0.4.0.1862.1.6)	<b>✓</b>		М	S	id-etsi-qct-web (0.4.0.1862.1.6.3)





# 1.11.26 Wildcard - LCP certificates supporting Signature, Authentication & Encryption

Wildcard SSL are certificates which can be used with multiple sub-domains of a specifi domain. Wildcard SSL are certificates have the following profile with <OID: 1.3.171.1.1.10.5.7> under LTSSLCA5.

	LuxTrust SSL S	erver	LCP Ce	ertifica	te Pro	file -Wildcard
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base						
Profile						
Version	T	✓	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	T	<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust SSL CA 5
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						<b>12;24</b> 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,
	organizationi valle			IVI	"	including the legal form (as specified in
		✓				the memorandum and articles of
						association or an equivalent document)
	organizationalUnitName1	<b>√</b>		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber



Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
	commonName	<b>√</b>		М	D	FQDN (Fully Qualified Domain Name) of application/server registered for LuxTrus S.A.
	serialNumber	<b>√</b>		0	D	Serial Number as provided by subscribe
subjectPublic	cKeyInfo	✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit up
	subjectPublicKey	<b>√</b>		М		4096 bits (RSA); public exponer Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	Identifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> C public key
authorityInfo	Access	✓	False			
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu[1]
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA5.crt
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCA5.crl
Subject Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
	SubjectAltName-dNSName	<b>✓</b>		М		FQDN (Fully Qualified Domain Name) application/server registered for LuxTru S.A.
subjectKeylo	dentifier	<b>√</b>	False			
	keyldentifier	<b>*</b>			Fixed	The Key Identifier comprises a four-befield with a 0100 value, followed by the least significant 60 bits of the SHA-1 has of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False



	LuxTrust SSL Server LCP Certificate Profile -Wildcard									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
	keyEncipherment	<b>√</b>			S	True				
	dataEncipherment	<b>√</b>			S	True				
certificatePo	licies	✓	False							
	Policyldentifier	✓			S	1.3.171.1.1.10.5.7				
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)				
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu				
	Policyldentifier	<b>√</b>				2.23.140.1.2.2				
	Policyldentifier	<b>✓</b>				0.4.0.2042.1.7				
Extended Ke	ey Usage	<b>✓</b>	False							
	serverAuth	✓			S	True				
	clientAuth	✓			S	True				
	emailProtection	✓			S	True				

## 1.11.27 LuxTrust SPARE Signing Server LCP Certificate Profile

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

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

The LuxTrust SPARE Signing Server LCP Certificate Profile include the corresponding SPARE Signing Server LCP Certificate, i.e., <1.3.171.1.10.3.20>.

	SPARE LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		<b>√</b>	False							
					S	Version 3 Value = "2"				
SerialNumber		<b>✓</b>	False							
					FDV	Validated on duplicates.				
signatureAlgo	rithm	<b>√</b>	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.				
signatureValue	e	<b>√</b>	False							
					D	Issuing CA Signature.				
Issuer	<b>'</b>	<b>√</b>	False		S					
	countryName	<b>√</b>			S	LU				
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>				



SPARE LuxTrust Signing Server LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value			
	organizationName	<b>√</b>			S	LuxTrust S.A.			
Validity		<b>√</b>	False						
	NotBefore	<b>✓</b>			D	Certificate generation process date/time.			
	NotAfter	<b>*</b>			D	Certificate generation process date/time 36 Months			
Subject		<b>√</b>	False						
	serialNumber	✓		М	D	Serial Number as constructed by LRAO			
	commonName	<b>√</b>		М	D	LGQCA XX CSS (XX a number selecter internally by LuxTrust) or Concatenation of given name(s) and surname(s) separated by a "Space" character.			
	givenName	<b>~</b>		М	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s) a on ID document			
	Surname	<b>✓</b>		М	D	CSS or Surname(s) as on ID docume without indication "épouse", "ép." or simile and the subsequent name(s)			
	countryName	<b>✓</b>		М	D	LU or Nationality of holder (ISO3166)			
	emailAddress	✓		0	D	N/A			
	Title	✓		М	D	Private Person			
subjectPubli	cKeyInfo	✓	False						
	Algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA) up 4096 bit (RSA); public exponent: Fermat-			
	subjectPublicKey	<b>√</b>		М	1	- (0x010001).			
Extensions									
Authority Properties									
authorityKey	Identifier	<b>~</b>	False						
	keyldentifier	<b>~</b>				SHA-1 Hash of the LuxTrust Globa Qualified CA public key			
authorityInfo	Access	<b>√</b>	False						
	AccessMethod	<b>√</b>				ld-ad-2			
	accessLocation	<b>✓</b>			†	http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt			
	AccessMethod	<b>√</b>				ld-ad-1			
	accessLocation	<b>✓</b>				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>			



	SPAR	E LuxTru	st Signin	g Server L	CP Certifi	icate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
cRLDistribution	cRLDistributionPoint		False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Subject Properties						
subjectAltNar	me	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeylde	subjectKeyldentifier		False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	•	<b>√</b>	True			
	digitalSignature	<b>√</b>			S	True
certificatePoli	icies	<b>√</b>	False			
	Policyldentifier	<b>~</b>				1.3.171.1.1.10.3.20
	policyQualifierID	<b>~</b>			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	Policyldentifier	<b>√</b>				0.4.0.2042.1.3

## 1.11.28 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] QCPI-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.110.3.21>. The following table provides the description of the fields for LuxTrust Qualified Certificates for digital signatue purpose.

	LuxTrust Qualified eSEAL Certificate Profile										
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	<b>O/M</b>	CO <sup>11</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumb	er	✓	False								
					FDV	Validated on duplicates.					
signatureAl	gorithm	✓	False			·					
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					



		Lux	Trust Qu	alified	eSEAL (	Certificate Profile
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	<b>O/M</b>	CO <sup>11</sup>	Value
signatureVa	l alue	· ✓	False	10		
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	<b>√</b>			S	LU
	commonName organizationName	<b>✓</b>			S S	LuxTrust Global Qualified CA x <sup>1</sup> LuxTrust S.A.
Validity	organizationivanie	<b>√</b>	False		3	Euxilust S.A.
ranary	NotBefore	<b>√</b>	1 4100		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject	T	✓	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)
	organisationIdentifi er (2.5.4.97)	<b>√</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by the legal entitiy or LU when the identifier is provided by LuxTrust.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnit Name	✓		0	D	Company/institution department or other information item
	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
subjectPub		<b>√</b>	False			Dublic Key Key less the 0040hh and 4000hh (700h)
	Algorithm subjectPublicKey	<b>✓</b>		М		Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (0x010001).
Extension	Junjecti uniteriey	,		IVI		public experient. I citiat + (0x010001).
S Authority Propertie						
S						
authorityKe		<b>√</b>	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf		<b>√</b>	False			
	AccessMethod	<b>✓</b>		<u> </u>		Id-ad-2
	accessLocation AccessMethod	<b>✓</b>		<del> </del>		http://ca.luxtrust.lu/LTGQCAx1.crt
	accessLocation	<b>∨</b>				ld-ad-1 http://qca.ocsp.luxtrust.lu/3
cRLDistribu		<b>√</b>	False			παρε/γοα.ουσρ.ιακτιαστ.ια/
	distributionPoint	<b>√</b>	. 4.00		S	
	fullName	✓		1		http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Propertie s						
subjectKey	Identifier	✓	False			



		Lux	Trust Qu	alified	eSEAL C	Certificate Profile
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	<b>O/M</b>	<b>CO</b> <sup>11</sup>	Value
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Propertie s						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP		✓	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
BasicConst	traints					
	CA	<b>√</b>			S	FALSE
	pathLenConstrain t	✓			S	0 (ZERO)
QualifiedCe	ertificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	✓		М	S	URL=https://www.luxtrust.com/repository
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

#### 1.11.29 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>.



	LuxTru	ıst NC	P+ Certif	icate Profi	le for au	thentication
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Base	1 1010			O/III		Turac
Profile						
Version		✓	False			
		,			S	Version 3 Value = "2"
SerialNumbe	er T	✓	False		ED\/	M-Pdata dan dan Pastas
signatureAlg	varithm	<b>√</b>	Folso		FDV	Validated on duplicates.
SignatureAig	Algorithm	•	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	Aigorium				3	RSA Encryption.
signatureVal	lue	✓	False			TO CETOTY DUTIES
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x1
N. P. P.	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NetDefere	<b>√</b>	False			Contificate managetica are seen data him a
	NotBefore NotAfter	<b>∨</b>			D D	Certificate generation process date/time.  Certificate generation process date/time + 24
	MOLAILEI				0	Months
Subject		✓	False			
	aamman Narra	<b>√</b>		N 4	_	Shall contain the full registered name of the
	commonName	<b>V</b>	<u> </u>	M	D	subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person)
	Journal yradine		ļ	IVI		is established (ISO3166)
	organisationIdentifier (2.5.4.97)	<b>✓</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entitity when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.  Shall contain the full registered name of the
	organizationName	<b>✓</b>		M	D	shall contain the full registered name of the subject (legal person).  Company/institution department or other
	organizationalUnitName	✓ ✓		O M	D	information item
	serialNumber	, i		М	D	Serial Number as constructed by LRAO
subjectPubli		<b>√</b>	False			Bull's Keep Keep langer 100 (01 %)
	Algorithm	<b>✓</b>		N 4		Public Key: Key length: 2048bit up to 4096bit
Extensions	subjectPublicKey	V		M		(RSA); public exponent: Fermat-4 (0x010001).
Authority						
Properties						
authorityKey	/Identifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified
						CA public key
authorityInfo		✓	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓ ✓				Id-ad-1
cRLDistribut	accessLocation	<b>✓</b>	Folco			http://qca.ocsp.luxtrust.lu/3
CKLDISTIBUT	distributionPoint	<b>✓</b>	False		0	
	uistributionPoint		<u> </u>		S	<u>l</u>





	LuxTrust NCP+ Certificate Profile for authentication									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl				
Subject Properties										
subjectKeylo		✓	False							
	keyldentifier	<b>*</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	True				
	nonRepudiation	✓			S	False				
	keyEncipherment	✓			S	True				
	dataEncipherment	✓			S	False				
certificatePo		✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.22				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	Policyldentifier	✓				0.4.0.2042.1.2				

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

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

	LuxTrust Advanced eSEAL Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	r	✓	False							
					FDV	Validated on duplicates.				
signatureAlg		✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	signatureValue		False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x1				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
•	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	<b>~</b>			D	Certificate generation process date/time + 24 Months				
Subject		✓	False							
	commonName	<b>√</b>		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)				



	Lu	xTrust	Advance	d eSEAL (	Certificate	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
	organisationIdentifier (2.5.4.97)	✓		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust.  The country code is either the country code where the subject is registered as legal entitity when the identifier is provided by the legal entitity or LU when the identifier is provided by LuxTrust.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	✓		0	D	Company/institution department or other information item
aubia at Dubli	serialNumber	✓ ✓	Falsa	М	D	Serial Number as constructed by LRAO
subjectPubli	Algorithm	<b>V</b>	False			Public Key: Key length: 2048bit up to 4096bit
	subjectPublicKey	<b>√</b>		М		(RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKey	l Identifier	<b>√</b>	False			
	keyldentifier	<b>√</b>	. 4.00			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓ ✓				Id-ad-2
	accessLocation AccessMethod	<b>∨</b>				http://ca.luxtrust.lu/LTGQCAx1.crt Id-ad-1
	accessLocation	· ✓				http://qca.ocsp.luxtrust.lu/3
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
Subject	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Properties						
subjectKeyld		✓	False			
	keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			
,	digitalSignature	<b>√</b>			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment dataEncipherment	✓ ✓			S	False
certificatePo		<b>✓</b>	False		S	False
	Policyldentifier	<b>√</b>	1 0.00			1.3.171.1.1.10.3.23
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID PolicyIdentifier	✓ ✓			S	Id-qt-2 (User Notice) 0.4.0.2042.1.2
BasicConstra		ı ,	1		I	V.T.V.EVTE.1.E
	CA	✓			S	FALSE
	pathLenConstraint	✓			S	0 (ZERO)





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

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



	LuxTrust Advanced eSEAL Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value				
Base										
Profile		<b>√</b>	F-1							
Version	1	~	False		S	Version 3 Value = "2"				
SerialNumbe	er	<b>√</b>	False		3	Version 3 value – 2				
ochantambe			1 alsc		FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False			randatod on adprioatoo.				
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with				
						RSA Encryption.				
signatureVa	lue	✓	False							
Issuer		✓	False		D S	Issuing CA Signature.				
issuei	countryName	· /	raise		S	LU				
	commonName	·			S	LuxTrust Global Qualified CA x1				
	organizationName	<b>√</b>			S	LuxTrust S.A.				
Validity	<b>9</b>	✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	✓			D	Certificate generation process date/time + 24				
						Months				
Subject	1	✓	False			Chall contain the full newletters discuss of the				
	commonName	✓		M	D	Shall contain the full registered name of the subject (legal person).				
						the country in which the subject (legal person)				
	countryName	✓		M	D	is established (ISO3166)				
	organisationIdentifier (2.5.4.97)	Ý		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by the legal entitity or LU when the identifier is provided by LuxTrust.				
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).				
	organizationalUnitName	<b>✓</b>		0	D	Company/institution department or other information item				
	serialNumber	<b>✓</b>		М	D	Serial Number as constructed by LRAO				
subjectPubli	icKeyInfo	✓	False							
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit				
_	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (0x010001).				
Extensions										
Authority Properties										





authorityKeyldentifier	✓	False		
keyldentifier	<b>~</b>			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfoAccess	✓	False		
AccessMethod	✓			ld-ad-2
accessLocation	✓			http://ca.luxtrust.lu/LTGQCAx1.crt
AccessMethod	✓			ld-ad-1
accessLocation	✓			http://qca.ocsp.luxtrust.lu/3
cRLDistributionPoint	✓	False		
distributionPoint	✓		S	
fullName	✓			http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties				
subjectKeyldentifier	✓	False		
keyldentifier	<b>√</b>		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties				
keyUsage	✓	True		
digitalSignature	✓		S	True
nonRepudiation	✓		S	False
keyEncipherment	✓		S	True
dataEncipherment	✓		S	False
certificatePolicies	✓	False		
Policyldentifier	✓			1.3.171.1.1.10.3.24
policyQualifierID	✓		S	Id-qt-1 (CPS)
qualifier	✓		S	https://repository.luxtrust.lu
policyQualifierID	✓		S	Id-qt-2 (User Notice)
Policyldentifier	✓			0.4.0.2042.1.2

#### 1.11.32 LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature

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

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

	LuxTrust Advanced Automated eSEAL Certificate Profile								
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
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 x1			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 24 Months			
Subject		✓	False						



	LuxTrust	Advano	ed Autor	nated eSE	AL Certi	ficate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Attribute	commonName	√ ×	OL.	M	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		M	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	<b>√</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust.  The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.
	organizationName	<b>~</b>		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	<b>~</b>		0	D	Company/institution department or other information item
subjectPubli		<b>✓</b>	False			
	Algorithm	<b>√</b>				Public Key: Key length: 2048bit up to 4096bit
Extensions	subjectPublicKey	· ·		М		(RSA); public exponent: Fermat-4 (0x010001).
Authority						
Properties						
authorityKey	dentifier	✓	False			
	keyldentifier	<b>~</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			, ,
-	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	<b>✓</b>				Id-ad-1
cRLDistribut	accessLocation	✓ ✓	False			http://qca.ocsp.luxtrust.lu/3
CKLDISTIBUT	distributionPoint	<b>V</b> ✓	False		S	
	fullName	· /				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties						7.00.00
subjectKeylo	lentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	<b>√</b>			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment dataEncipherment	<b>✓</b>			S S	False
certificatePo		<b>V</b>	False		3	i aist
201111104101	Policyldentifier	· ✓	1 4/30			1.3.171.1.1.10.3.25
	policyQualifierID	<b>✓</b>			S	
	policywaaimeriD		L		ა	Id-qt-1 (CPS)





	LuxTrust Advanced Automated eSEAL Certificate Profile									
Attribute	Attribute Field IN <sup>8</sup> CE <sup>9</sup> O/M <sup>10</sup> CO <sup>11</sup> Value									
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	Policyldentifier	✓				0.4.0.2042.1.2				
BasicConstr	aints									
	CA	✓			S	FALSE				
	pathLenConstraint	✓			S	0 (ZERO)				

## 1.11.33 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									
Attribut e	Field	IN 13	CE <sup>14</sup>	O/M <sup>15</sup>	CO 16	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNum	nber	✓	False		ED) (	A P L d L L P d				
-:	A I	<b>√</b>	Гајаа		FDV	Validated on duplicates.				
signature	Algorithm	•	False		S	OID = "1,2,840,113549,1,1,11" - SHA256 with RSA				
	,				8	OID = 1.2.840.113549.1.1.11 - SHA256 WITH RSA Encryption.				
signature	Value	✓	False							
		<b>√</b>	F-1		D	Issuing CA Signature.				
Issuer	a a um t m Alarra	<b>✓</b>	False		S	LU				
	countryName commonName	<b>∨</b>			S					
					_	LuxTrust Global Qualified CA x <sup>1</sup>				
M-11:-11:	organizationName	✓			S	LuxTrust S.A.				
Validity	NetDefere	<b>✓</b>	False			One Control of the Co				
	NotBefore NotAfter	<b>∨</b>			D D	Certificate generation process date/time.  Certificate generation process date/time + 36 Months				
Subject	NOTAITEI	<b>√</b>	False			Certificate generation process date/time + 36 Months				
Cubject	serialNumber	✓	1 disc	М	D	Serial Number as constructed by LRAO				
	commonName	<b>✓</b>		М	D	<b>PRO and PRIVATE products</b> : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.				
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card				
	surname	<b>✓</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)				
	countryName	✓		М	D	Nationality of holder (ISO3166)				
	emailAddress	✓		0	D	Subject's email address				
						PRIVATE products:				
						Fixed value: "Private Person"				
	title	✓		M	D	PRO products:				
						"Professional Person" (default) or "Professional Administrator"				
						(Other titles possible for special purpose certificates)				



	Lux <sup>-</sup>	Trust	Smart	Card Q	CP-n-c	qscd Certificate Profile
Attribut e	Field	IN 13	CE <sup>14</sup>	O/M <sup>15</sup>	CO 16	Value
						PRO products only:
	organizationName	<b>✓</b>		М	D	Name of company/institution as in articles of
	organization tanto			141		association or equivalent documents, including the
						legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of
	i o o antyriamo			141		HQ (as in articles of association)
				M for		PRO products:
				PRO		Company/Institution VAT number (or if no VAT number
	organizationalUnit			prod., condi-	_	available, other unique national company/institution
	Name 1	✓		tional	D	identifier)
				(O) for		PRIVATE products:
				PRIV prod.)		If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
				prod.)		,
	organizationalUnit	<b>✓</b>		0	D	PRO products only:
	Name 2					Company/institution department or other information item
subjectPu	iblicKeyInfo	✓	False			
	Algorithm	✓ ✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
Extensi	subjectPublicKey	<b>V</b>		M		public exponent: Fermat-4 (0x010001).
ons						
Authorit						
Properti						
es	(a.d.lantifian		Гаја			
autnority	Keyldentifier keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualified CA
	Regidentine	-				public key
authorityl	nfoAccess	<b>√</b>	False			
	AccessMethod accessLocation	✓ ✓				ld-ad-2 http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistri	butionPoint	✓	False		_	
	distributionPoint fullName	✓ ✓			S	http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Subject	Tullitallic	•				nttp://cri.iuxtrust.iu/L1GQCAxcri
Properti						
es	(Al annua	<b>√</b>	E-I			
subjectAl	Rfc822Name	<b>∨</b>	False	0	D	Certificate Holder's email address
subjectKe	yldentifier	✓	False			
	keyldentifier	✓			Fixe d	The Key Identifier comprises a four-bit field with a 0100
					u	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-
Policy						string bits).
Properti						
es		,	_			
keyUsage	digitalSignature	✓ ✓	True		S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	<b>V</b>			S	False
certificate	dataEncipherment	✓ ✓	False		S	False
Certificate	Policyldentifier	<b>✓</b>	1 0150			1.3.171.1.1.10.3.26
	policyQualifierI	<b>√</b>			S	Id-qt-1 (CPS)
	D qualifier	<b>✓</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
0. 11.11	Policyldentifier	<b>√</b>	F			0.4.0.194112.1.2
Qualified	CertificateStat	✓	False			



	LuxTrust Smart Card QCP-n-qscd Certificate Profile										
Attribut e	Field	IN 13	CE <sup>14</sup>	O/M <sup>15</sup>	CO 16	Value					
	QcCompliance (0.4.0.1862.1.1)	<b>✓</b>		М	S	True					
	QcSSCD (0.4.0.1862.1.4)			М	S	True					
	QcPDS (0.4.0.1862.1.5)	✓		М	S	URL=https://www.luxtrust.com/repository					
	QcType (0.4.0.1862.1.6)	<b>✓</b>		М	S	id-etsi-qct-esign					

#### 1.11.34 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>.

		LuxT	rust Sm	art Card	NCP+ Cei	rtificate Profile
Attribut e	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base Profile						
Version		✓	False			
	_	,			S	Version 3 Value = "2"
SerialNum	nber	✓	False		ED) /	N. F. L. C. L. B. C.
signature	Algorithm	<b>√</b>	False		FDV	Validated on duplicates.
Signature	Algorithm		raise		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature\	Value	✓	False			
					D	Issuing CA Signature.
Issuer	T	✓	False		S	
	countryName	✓			S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	LNIS	<b>√</b>	False			
	NotBefore NotAfter	✓ ✓			D	Certificate generation process date/time.
Cubinet	NotAfter	<b>V</b>	False		D	Certificate generation process date/time + 36 Months
Subject	T		Faise		_	
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	<b>PRO and PRIVATE products</b> : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		OOCSP	D	Subject's email address
	title	<b>*</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.



	LuxTrust Smart Card NCP+ Certificate Profile											
Attribut e	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value						
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)						
	organizationalUnit Name 1	<b>~</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à: " & (Date of birth + 18 years).						
	organizationalUnit Name 2	<b>✓</b>		0	D	PRO products only: Company/institution department or other information item						
subjectPu	blicKeyInfo	✓	False									
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit						
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (0x010001).						
Extensi ons												
Authorit y Properti es												
authorityK	eyldentifier	✓	False									
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key						
authoritylr	nfoAccess	✓	False			passe noy						
	AccessMethod	✓				ld-ad-2						
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt						
	AccessMethod	✓				ld-ad-1						
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3						
cRLDistrib	outionPoint	✓	False									
	distributionPoint	✓			S							
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl						
Subject Properti es						·						
subjectAlt		<b>√</b>	False	_								
aubicati/-	Rfc822Name	<b>✓</b>	Fal	0	D	Certificate Holder's email address						
subjectKe	keyldentifier	<b>▼</b>	False		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value o subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).						
Policy Properti es			_									
keyUsage	digitalSignature	<b>✓</b>	True		c	Truo						
	nonRepudiation	<b>✓</b>	-		S S	True False						
	keyEncipherment	<b>✓</b>	-		S	True						
	dataEncipherment	<b>√</b>			S	False						
certificate		✓	False									
	Policyldentifier	✓				1.3.171.1.1.10.3.27						
	policyQualifierID	✓			S	Id-qt-1 (CPS)						
	qualifier	✓			S	https://repository.luxtrust.lu						
	policyQualifierID	✓	1	<u></u>	S	Id-qt-2 (User Notice)						
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2						

## 1.11.35 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>.

	LuxTrust Sn	nart C	ard LOF	RA NCP	- Sign	ature Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base						
Profile Version		<b>✓</b>	False			
version		•	raise		S	Version 3 Value = "2"
SerialNumb	per	<b>✓</b>	False			Verdien e value
					FDV	Validated on duplicates.
signatureAl		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	<b>√</b>	False			Encryption.
			1 3.100		D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓ ✓			S	LU
	commonName				S	LuxTrust Global Qualified CA x <sup>1</sup>
Validity	organizationName	✓ ✓	False		S	LuxTrust S.A.
Validity	NotBefore	· /	raise		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			,
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						Connection of given name(a) and autrama(a) as
	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(s) as on ID card without indication
	Surname	✓		M	D	"épouse", "ép." or similar and the subsequen
						name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	<b>√</b>		0	D	Subject's email address
					_	
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		M	D	Constructed by LuxTrust
	le celitudiom e	<b>√</b>		N.4	D	Country of DA
	localityName	•		М	U	Country of RA
	organizationalUnitNa	<b>✓</b>		М	D	RA code Constructed by LuxTrust
	me 1			IVI		THA COUC GONSTRUCTED by Eux Trust
	organizationalUnitNa	<b>✓</b>			6	DAO and Comptunated by LawTweet
	me 2	~		М	D	RAO code Constructed by LuxTrust
subjectPub		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA)
Futanaian	subjectPublicKey	✓		М		public exponent: Fermat-4 (0x010001).
Extension s						
Authority						
Propertie						
S			E-I			
authorityKe	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualified CA
	Regidentifie					public key
authorityInf	foAccess	✓	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	<b>√</b>	1			Id-ad-1
DI D' : '	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribu		<b>√</b>	False		S	
	distributionPoint fullName	✓ ✓			٥	http://orl.leastreet.lea/LTCCCAl
Subject	Tullituilie					http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Propertie						
S						
subjectAltN		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address



	LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
subjectKey	dentifier	✓	False							
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy Propertie s										
keyUsage		✓	True							
	digitalSignature	✓			S	False				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificateP	olicies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.28				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	Policyldentifier	✓				0.4.0.2042.1.2				

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

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

	LuxTrust Smart Card LORA NCP+ - authentication Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	er	✓	False							
					FDV	Validated on duplicates.				
signatureAl	<del>-</del>	✓	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 <sup>1</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity	-	✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	✓			D	Certificate generation process date/time + 36 Months				
Subject		✓	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.				
	givenName	✓		М	D	Given name(s) as on ID card				
	Surname	<b>✓</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)				
	countryName	✓		М	D	Nationality of holder (ISO3166)				
	emailAddress	✓		0	D	Subject's email address				
	Title	✓		М	D	"LuxTrust RA Officer"				
	organizationName	✓		М	D	Constructed by LuxTrust				



	LuxTrust Sma	rt Cai	d LOR	A NCP+	- authen	tication Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Attribute	ricia		OL	O/III	- 00	Value
	localityName	~		М	D	Country of RA
	organizationalUnitNa me 1	<b>√</b>		М	D	RA code Constructed by LuxTrust
	organizationalUnitNa me 2	<b>✓</b>		М	D	RAO code Constructed by LuxTrust
subjectPub	licKevInfo	<b>✓</b>	False			
	Algorithm	<b>/</b>	. 4.00			Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	<b>/</b>		М		public exponent: Fermat-4 (0x010001).
Extension s						
Authority Propertie s						
authorityKe	yldentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf	oAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribu	utionPoint	<b>✓</b>	False			
	distributionPoint	<b>✓</b>			S	
	fullName	<b>✓</b>			_	http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Propertie s						
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	Identifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
_	keyEncipherment	✓			S	True
	dataEncipherment	<b>√</b>	L		S	False
certificateP		<b>√</b>	False			
	Policyldentifier	<b>√</b>		ļ		1.3.171.1.1.10.3.29
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)
	Policyldentifier	✓		<u> </u>		0.4.0.2042.1.2

## 1.11.37 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 Smart Card QCP-n-qscd Certificate Profile								
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M 10	CO <sup>11</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			



	LuxTrus	t eID S	Smart C	ard Q0	CP-n-qs	cd Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M 10	CO <sup>11</sup>	Value
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
-:	1	✓	E-I			Encryption.
signatureVa	lue	•	False		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	issuing CA Signature.
100001	countryName	<b>√</b>	1 4100		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity	organizationi vario	<b>√</b>	False			Edit 1 dot 6.74.
	NotBefore	<b>✓</b>			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			1 CEOBOITINI COllinoate
Cusjour	serialNumber	✓	Taioo	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	<b>✓</b>		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	<b>✓</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	Subject's email address
	Title	<b>√</b>		М	D	"Private Person"
	organizationalUnitName	<b>√</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of
	1					birth + 18 years).
subjectPubl	icKeyInfo	<b>√</b>	False			
	Algorithm	<b>√</b>		М		Public Key: Key length: 2048bit up to 4096bit (RSA); public exponent: Fermat-4 (0x010001).
Extension	subjectPublicKey	V		IVI		public exponent. Fernat-4 (0x010001).
s Authority						
Properties						
authorityKe		<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfo	OAccess AccessMethod	<b>√</b>	False			ld ad 2
		<b>✓</b>	-			Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>	1	1		Id-ad-1
D: 5: ::	accessLocation					http://qca.ocsp.luxtrust.lu/Error! Bookmark not defined.
cRLDistribu		<b>√</b>	False		-	
	distributionPoint fullName	<b>✓</b>			S	http://ord.loude.cet.lou/J.TOOOA.cl
Culpinat	Tullivarrie	•				http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
Subject Properties						
subjectAltN	ame	<b>√</b>	False			
JudjeotAitiN	Rfc822Name	· ✓	1 4130	0	D	Subject email address
subjectKeyl		✓	False		_	,
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	<b>√</b>			S	False



	LuxTrust eID Smart Card QCP-n-qscd Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M 10	CO <sup>11</sup>	Value				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificateP		✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.30				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2				
QualifiedCe	ertificateStat	✓	False							
	QcCompliance (0.4.0.1862.1.1)	<b>✓</b>		М	S	True				
	QcSSCD (0.4.0.1862.1.4)	<b>✓</b>		М	S	True				
	QcPDS (0.4.0.1862.1.5)	<b>~</b>		М	S	URL=https://www.luxtrust.com/repository				
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign				

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

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

	LuxTrust eID Smart card NCP+ Certificate Profile										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumb	er	✓	False								
					FDV	Validated on duplicates.					
signatureAl		✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	alue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>					
	organizationName	<b>✓</b>			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	<b>√</b>			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate					
Subject		✓	False								
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) separated by the space character					
	givenName	✓		М	D	Given name(s) as on ID card or as provided by the RNCID					
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID					
	countryName	✓		М	D	LU					
	emailAddress	✓		0	D	Subject's email address					



	LuxTru	st eID	Smart	card N	CP+ Ce	rtificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
	Title	✓		М	D	"Private Person"
	organizationalUnitNa me 1	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPub		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).
Extension s						
Authority Properties						
authorityKe		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x <sup>1</sup> public key
authorityInf	foAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/3
cRLDistribu	utionPoint	<b>√</b>	False			
	distributionPoint	<b>✓</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properties						
subjectAltN	lame	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	Subject email address
subjectKey	Identifier	✓	False			,
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓	ļ		S	False
	keyEncipherment	✓			S	True
	dataEncipherment	<b>✓</b>			S	False
certificateP		<b>√</b>	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.31
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>	<u> </u>		S	https://repository.luxtrust.lu
	policyQualifierID	✓ ✓			S	Id-qt-2 (User Notice)
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

	LuxTrust Signing Server QCP-n-qscd Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	per	✓	False							
					FDV	Validated on duplicates.				
signatureA	lgorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.				
signatureV	alue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					



	LuxTrust	Signin	ig Serv	er QCP	-n-qsc	d Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	I w an a	✓	False		-	
	NotBefore NotAfter	✓ ✓			D	Certificate generation process date/time.  Certificate generation process date/time + 36
	NotArter	*			D	Months
subject		<b>✓</b>	False			Widhuis
0 0.00 10 0 0	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
	Serialivallibei	•		IVI		•
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
						PRO products:
	title	✓		М	D	"Professional Person" (default) or "Professional Administrator"
						(Other titles possible for special purpose certificates)
						PRO products only:
	organizationName	<b>✓</b>		М	D	Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>✓</b>		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnitNa me 1	<b>√</b>		M for PRO prod., condi - tional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitNa me 2	✓		0	D	PRO products only:  Company/institution department or other information item
subjectPub	licKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA);
-,	subjectPublicKey	✓		М		public exponent: Fermat-4 (0x010001).
Extension s						
Authority Propertie s						
authorityKe		✓	False			
<u>-</u>	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
	Î.	-	<del> </del>	1		passio noj
authorityInf	foAccess	✓	False			
authorityInf	foAccess AccessMethod	✓ ✓	False			Id-ad-2
authorityInt			False			Id-ad-2 http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt



	LuxTrust	Signin	g Serv	er QCP	-n-qscc	d Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3
cRLDistribu	ıtionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx-yy.crl
Subject Propertie s						
subjectAltN		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey		✓	False			
	keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation				S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.32
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	5 " 11 ""					0.40.40.440.40
0	Policyldentifier	<b>√</b>	F-1-			0.4.0.194112.1.2
QualifiedCe	ertificateStat	<b>√</b>	False			-
	QcCompliance (0.4.0.1862.1.1)	·		М	S	True
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	URL=https://www.luxtrust.com/repository
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)

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

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

	LuxTrus	t Sign	ing Ser	ver QCF	P-I-qscd	l Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber	İ	✓	False			
					FDV	Validated on duplicates.
signatureAlgo	orithm	✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValu	ie	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 12, 24, 60 Months
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO



A stuile est a	Luxirust	Sign	_	ver QCI	I-qsco	l Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	commonName	<b>~</b>		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)
	organisationIdentifi er (2.5.4.97)	<b>~</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust)
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitN ame 1	<b>√</b>		0	D	Company/institution department or other information item
	organizationalUnitN ame 2	<b>~</b>		0	D	Company/institution department or other information item
subjectPublic		✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).
Authority Properties						
authorityKey	Identifier	<b>√</b>	False			
•	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	A BA - 41: I	✓				
	AccessMethod					Id-ad-1
	accessLocation	✓				Id-ad-1 <a href="http://qca.ocsp.luxtrust.lu/">http://qca.ocsp.luxtrust.lu/</a>
cRLDistributi	accessLocation ionPoint	✓ ✓	False			
cRLDistributi	accessLocation ionPoint distributionPoint	✓ ✓ ✓	False		S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
	accessLocation ionPoint	✓ ✓	False		S	
Subject	accessLocation ionPoint distributionPoint	✓ ✓ ✓	False		S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
	accessLocation ionPoint distributionPoint fullName	✓ ✓ ✓	False False		S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
Subject Properties	accessLocation ionPoint distributionPoint fullName	✓ ✓ ✓			S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  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
Subject Properties subjectKeyld	accessLocation ionPoint distributionPoint fullName entifier	✓ ✓ ✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits
Subject Properties subjectKeyld Policy Properties	accessLocation ionPoint distributionPoint fullName entifier	V V V V	False			http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  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
Subject Properties subjectKeyld	accessLocation ionPoint distributionPoint fullName entifier keyldentifier	✓ ✓ ✓			Fixed	http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  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).
Subject Properties subjectKeyld Policy Properties	accessLocation ionPoint distributionPoint fullName entifier keyldentifier digitalSignature	V V V V	False		Fixed	http://crl.luxtrust.lu/LTGQCAx-yy.crl  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).
Subject Properties subjectKeyld Policy Properties	accessLocation ionPoint distributionPoint fullName entifier keyldentifier digitalSignature nonRepudiation	V V V V	False		Fixed S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  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).
Subject Properties subjectKeyld Policy Properties keyUsage	accessLocation ionPoint distributionPoint fullName entifier keyldentifier  digitalSignature nonRepudiation keyEncipherment dataEncipherment	V V V V V V V V V V V V V V V V V V V	False		Fixed	http://crl.luxtrust.lu/LTGQCAx-yy.crl  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).  True  False
Subject Properties subjectKeyld Policy Properties	accessLocation ionPoint distributionPoint fullName entifier keyldentifier  digitalSignature nonRepudiation keyEncipherment dataEncipherment	V V V V V V	False		Fixed S S S	http://qca.ocsp.luxtrust.lu/ <sup>3</sup> http://crl.luxtrust.lu/LTGQCAx-yy.crl  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).  True  False False False



	LuxTrust Signing Server QCP-I-qscd Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	qualifier	✓			S	https://repository.luxtrust.lu				
	Policyldentifier	<b>√</b>				0.4.0.194112.1.3				
BasicConstr	aints									
	CA	✓			S	FALSE				
	pathLenConstraint	✓			S	0 (ZERO)				
QualifiedCer	tificateStat	✓	False			`				
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True				
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		М	S	True				
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	URL=https://www.luxtrust.com/repository				
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)				

## 1.11.41 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>.

	LuxTr	ust S	igning	Stick C	QCP-n-c	qscd Certificate Profile
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	O/M <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	False		==>:/	
	L	<b>/</b>	F-1		FDV	Validated on duplicates.
signatureA		V	False		_	OID = "4 0 040 440 40 4 444" CLIA 050 with DC/
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	False			
1		,	F-'		D	Issuing CA Signature.
Issuer	a a un tru Alama	<b>✓</b>	False		S	LU
	countryName commonName	<b>✓</b>			S	
						LuxTrust Global Qualified CA x <sup>1</sup>
17 P P	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NetDefens	<b>✓</b>	False		_	Ocalificate manager floor manager data // acc
	NotBefore NotAfter	V /			D D	Certificate generation process date/time.  Certificate generation process date/time + 36 Months
Subject	Notallel	<b>✓</b>	False		_ D	Certificate generation process date/time + 36 Months
Oubject	serialNumber	✓	1 alse	М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on IL card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
						PRIVATE products:
						Fixed value: "Private Person"
	4:41.					PRO products:
	title			M	D	"Professional Person" (default) or "Professional Administrator"
						(Other titles possible for special purpose certificates)



	LuxTr	ust S	Signing	Stick C	QCP-n-c	qscd Certificate Profile
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
						PRO products only:
	organizationName	<b>✓</b>		М	D	Name of company/institution as in articles of associati
	J. gamzanomiame	_		IVI	5	or equivalent documents, including the legal form.
						5. Squivalone assuments, molaumy the legal form.
	localityName	<b>✓</b>		М	D	PRO products only: Company/institution country of I
						(as in articles of association)
				M for		PRO products:
				PRO		Company/Institution VAT number (or if no VAT number
	organizationalUnit			prod., condi-		available, other unique national company/institut
	Name 1	✓		tional	D	identifier)
				(O) for		PRIVATE products:
				PŔIV		If the holder is underage: "Mineur jusqu'à : " & (Date
				prod.)		birth + 18 years).
	organizationalUnit					PRO products only:
	Name 2	✓		0	D	Company/institution department or other informat
						item
subjectPub		<b>V</b>	False			
	Algorithm subjectPublicKey	<b>√</b>		M		Public Key: Key length: 2048bit (RSA); public expone Fermat-4 (0x010001).
Extension	SubjectrubilCNey	v		IVI		i Gillat-4 (UNU 10001).
3						
Authority						
Propertie S						
authorityKe		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA pul
authorityInf	in Access	<b>✓</b>	False			key
addionityiili	AccessMethod	<b>✓</b>	i aist			Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>✓</b>	<b>†</b>			Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribu		✓	False			
	distributionPoint	<b>√</b>			S	
DI. !	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Propertie s						
subjectAltN		<b>V</b>	False			
subjectKey	Rfc822Name	✓ ✓	Eoloo	0	D	Certificate Holder's email address
subjectkey	keyldentifier	✓ ✓	False		Fixed	The Key Identifier comprises a four-bit field with a 01
	,					value, followed by the least significant 60 bits of
						SHA-1 hash of the value or subjectPublicKey bit str
						(tag, not including the length and number of unused
Policy						string bits).
Propertie						
s keyUsage		<b>✓</b>	True			
,	digitalSignature	<b>√</b>			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	<b>√</b>			S	False
noutificate P	dataEncipherment	<b>√</b>	False		S	False
certificateP	olicies Policyldentifier	<b>√</b>	False			1.3.171.1.1.10.3.34
	policyQualifierI	✓ ✓			S	Id-qt-1 (CPS)
	D					1 ( )
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	<b>√</b>	ļ		S	Id-qt-2 (User Notice)
Onalificaco	Policyldentifier ertificateStat	✓ ✓	False			0.4.0.194112.1.2
wuaiiiieaCe	QcCompliance	<b>✓</b>	raise	М	S	True
	(0.4.0.1862.1.1)	1	1	171		1100



	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribute	Field	<b>IN</b> 8	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value					
	QcSSCD (0.4.0.1862.1.4)			М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	URL=https://www.luxtrust.com/repository					
	QcType (0.4.0.1862.1.6)	<b>√</b>		M	S	id-etsi-qct-esign					

#### 1.11.42 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>.

	L	uxTr	ust Sigi	ning Stick	NCP+ C	ertificate Profile
Attribut e	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNun	nber	✓	False			
					FDV	Validated on duplicates.
signature	Algorithm	✓	False			OID
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature	Value	✓	False			
					D	Issuing CA Signature.
Issuer	T 4 N1	<b>√</b>	False		S	1
	countryName commonName	✓ ✓			S S	LU
						LuxTrust Global Qualified CA x <sup>1</sup>
Validity	organizationName	✓ ✓	Folso		S	LuxTrust S.A.
Validity	NotBefore	V /	False		D	Certificate generation process date/time.
	NotAfter	<i>'</i>			D	Certificate generation process date/time + 3 Months
Subject		<b>√</b>	False			IVIOLITIS
<del>- Cubject</del>	serialNumber	<b>✓</b>	1 4100	М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation given name(s) and surname(s) as on ID call separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) a on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as a ID card without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) (Professional Administrator" (Other titles possible for special purposite certificates)
	organizationName	<b>✓</b>		М	D	PRO products only:  Name of company/institution as in articles association or equivalent documents, includir the legal form.



	Lı	uxTru	ust Sigr	ning Stick	NCP+ Ce	ertificate Profile
Attribut e	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
	localityName	<b>~</b>		М	D	PRO products only: Company/institution countr of HQ (as in articles of association)
	organizationalUnit Name 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VA number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à: " of (Date of birth + 18 years).
	organizationalUnit Name 2	<b>√</b>		0	D	PRO products only: Company/institution department or other information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); publi
	subjectPublicKey	✓		М		exponent: Fermat-4 (0x010001).
Extensi ons						
Authorit y Properti es						
authorityK	Keyldentifier	✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> C public key
authorityli	nfoAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRI Distrik	outionPoint	<b>√</b>	False			тири, чостоорнали соста
UI LE IOLI IL	distributionPoint	<b>√</b>	1 4.00		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx1.crl
Subject Properti es						
subjectAlt		<b>√</b>	False		_	
oubicati/-	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKe	keyldentifier	<b>▼</b>	False		Fixed	The Key Identifier comprises a four-bit field with 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 Properti es						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment	<b>✓</b>			S	True
certificate	dataEncipherment	<b>✓</b>	Folco		S	False
cermicate	Policyldentifier	<b>∨</b>	False			1.3.171.1.1.10.3.35
	policyQualifierID	<b>√</b>			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	· ✓			S	Id-qt-2 (User Notice)
	Policyldentifier	· ✓				0.4.0.2042.1.2

# 1.11.43 LuxTrust Signing Server Advanced Automated eSeal Certificate Profile

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



Advanced eSeal - LCP Certificate Profile						
Attribute	Field	IN8	CE9	O/M <sup>10</sup>	CO <sup>11</sup>	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" – if SHA256 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x1
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 12, 24 Months
subject		<b>√</b>	False			
	serialNumber	<b>✓</b>		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	<b>√</b>		М	D	the country in which the subject (legal person) is established (ISO3166)



	Adva	ince	d eSea	I - LCP	Certif	icate Profile
Attribute	Field	IN8	CE9	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Attribute	organisationIdentifier (2.5.4.97)	<b>→</b>	51	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. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entity when the identifier is provided by the legal entitiy or LU when LuxTrust provides the identifier.
	organizationName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitNam e 1	✓		0	D	Company/institution department or other information item
	organizationalUnitNam e 2	✓		0	D	Company/institution department or other information item
subjectPubl	icKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	<b>√</b>		М		public exponent: Fermat-4 (0x010001).
Extension s						
Authority Properties						
authorityKe	yldentifier	<b>√</b>	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	<b>√</b>	False			
	AccessMethod	<b>✓</b>				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt



	Advanced eSeal - LCP Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE9	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	AccessMethod	<b>√</b>				Id-ad-1				
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/3				
cRLDistribu	tionPoint	<b>√</b>	False							
	distributionPoint	✓			S					
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGQCAx1.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	True				
	nonRepudiation	✓			S	False				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificatePo	olicies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.36				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	Policyldentifier	✓				0.4.0.2042.1.3				

# 1.11.44 LuxT LuxTrust Signing Server QCP-I Certificate Profile

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

	LuxTrust Signing Server QCP-I Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	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" – if SHA256 with RSA Encryption.				
signatureValue	,	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x1				
	organizationNam e	<b>√</b>			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				



	LuxTr	ust Si	igning S	erver Q	CP-I C	ertificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 24, 36 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)
	organisationIdent ifier (2.5.4.97)	<b>√</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - Identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by LuxTrust)
	organizationNam e	✓		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUni tName 1	✓		0	D	Company/institution department or other information item
	organizationalUni tName 2	✓		0	D	Company/institution department or other information item
subjectPublicK		<b>√</b>	False			
	algorithm	<b>√</b>				Public Key: Key length: 3072 up to 4096 bit (RSA);
Fotomalous	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).
Authority Properties						
authorityKeyld	entifier	<b>√</b>	False			
authoritykeylo	keyldentifier	<b>√</b>	raise			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfoAd		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocatio n	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
	AccessMethod	<b>√</b>	<u> </u>	<u> </u>		Id-ad-1
	accessLocatio n	<b>v</b>				http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribution		✓	False			
J. 122.511 10 41101	distributionPoint	✓	1 4.00		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx-yy.crl
Subject Properties						
subjectKeylder	ntifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy						
Properties		<b>√</b>	Ture			
keyUsage	digitalSignature	<u>√</u>	True		S	True
	nonRepudiation	•			S	False
	keyEncipherment				S	False
	,		1	1		1



	LuxTrust Signing Server QCP-I Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
	dataEnciphermen t				S	False				
certificatePolic	ies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.37				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	Policyldentifier	<b>√</b>				0.4.0.194112.1.1				
BasicConstrair	nts									
	CA	✓			S	FALSE				
	pathLenConstraint	✓			S	0 (ZERO)				
QualifiedCertifi	cateStat	✓	False			,				
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True				
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	URL=https://www.luxtrust.com/repository				
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)				

# 1.11.45 LuxTrust Signing Server eID BE delegated Sign QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by LuxTrust, from 3072-bit key size and with a key usage that supports qualified electronic signature. This profile is only associated with identification performed with a notified eID BE and notified foreign eID BE.

Lu	LuxTrust Signing Server elD BE delegated Sign QCP-n-qscd Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
		,		M	S	Version 3 Value = "2"				
SerialNumbe	er I	✓	False		ED\/	MaPilata dan dan Pastas				
olamoturo Ala	a vith m	<b>/</b>	Folos	M	FDV	Validated on duplicates.				
signatureAlg	algorithm	V	False	M	S	OID = "1.2.840.113549.1.1.11" – if SHA256 with				
	J			IVI	3	RSA Encryption.				
signatureVal	ue	✓	False		_					
				M	D	Issuing CA Signature.				
Issuer	a a compton Allama a	<b>√</b>	False	N 4	S S					
	countryName commonName	V /		M M	S	LU				
		· ·				LuxTrust Global Qualified CA x <sup>1</sup>				
Validit.	organizationName	✓ ✓	F-1	M	S	LuxTrust S.A.				
Validity	NotBefore	V /	False	M	D	Cartificate garagetian process data/time				
	NotAfter	\ \ \ \		M	D	Certificate generation process date/time.  Certificate generation process date/time + 1				
	Notatiei	·		IVI	, D	Month				
subject	1	✓	False							
	serialNumber	✓		М	D	As provided by the eID product				
	commonName	✓		М	D	As provided by the eID product				
	givenName	✓		М	D	As provided by the eID product				
	surname	✓		М	D	As provided by the eID product				
	countryName	✓		М	D	As provided by the eID product				
subjectPubli		✓	False							
	algorithm	✓		М		Public Key: Key length: from 3072 bits (RSA);				
	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).				
Extensions										
Authority										
Properties										



Lu	ıxTrust Signing Se	rver ell	D BE d	elegate	d Sign	QCP-n-qscd Certificate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
authorityKey	authorityKeyldentifier		False			
	keyldentifier	✓		M		SHA-1 Hash of the LuxTrust Global Qualified CA
						x <sup>1</sup> public key
authorityInfo	Access	✓	False			, ,
	AccessMethod	✓				Id-ad-2
	accessLocation	✓		М		http://ca.luxtrust.lu/LTGQCAx1.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>		М		http://qca.ocsp.luxtrust.lu/ <sup>3</sup>
cRLDistribut		<b>✓</b>	False			TREP IT QUELOUS PROVIDENCE IN THE PROVIDENCE IN
CIVEDISHIBUL	distributionPoint	· ·	1 0136		S	
	fullName	<b>✓</b>		М		http://crl.luxtrust.lu/LTGQCAx-yy.crl
Subject	Tumvame			101		TREP.//OTHER REGISTRE PER CONTROL STREET
Properties						
subjectKeyld	lentifier	✓	False			
	keyldentifier	✓		М	Fixed	SHA-1 Hash of the LuxTrust Global Qualified CA
						x <sup>1</sup> public key
Policy Properties						,
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation			М	S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	✓		М		1.3.171.1.1.10.3.38
	policyQualifierID	✓		M	S	Id-qt-1 (CPS)
	qualifier	✓		M	S	https://repository.luxtrust.com
	Policyldentifier	✓		M		0.4.0.194112.1.2
QualifiedCer		✓	False			
	QcCompliance	✓		M	S	True
	(0.4.0.1862.1.1)	<u> </u>				
	QcSSCD	✓		M	S	True
	(0.4.0.1862.1.4)			L		
	QcPDS	✓		M	S	https://repository.luxtrust.com
	(0.4.0.1862.1.5)	<b>/</b>		L		
	QcType	<b>'</b>		M	S	id-etsi-qct-esign
	(0.4.0.1862.1.6)					(0.4.0.1862.1.6.1)

# 1.11.46 LuxTrust Signing Server LuxTrust PRI/PRO delegated Sign QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by LuxTrust, from 3072-bit key size and with a key usage that supports qualified electronic signature. This profile is only associated with identification performed with a qualified LuxTrust PRI/PRO certificate.

Attribute	Field	IN	CE	O/M	CO	Value
Base Profil	e					
Version		✓	False			
				M	S	Version 3 Value = "2"
SerialNuml	ber	✓	False			
				М	FDV	Validated on duplicates.
signatureA	lgorithm	✓	False			·
	algorithm			М	S	OID = "1.2.840.113549.1.1.11" - if SHA25
						with RSA Encryption.
signatureV	alue	✓	False			
				М	D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓		М	S	LU
	commonName	✓		М	S	LuxTrust Global Qualified CA x
	organizationName	✓		М	S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓		М	D	Certificate generation process date/time.
	NotAfter	✓		М	D	Certificate generation process date/time +
						Month



						n QCP-n-qscd Certificate Profile
Attribute	Field	IN	CE	O/M	СО	Value
subject		<b>√</b>	False			
<b>,</b>	serialNumber	<b>✓</b>		М	D	As provided by the LuxTrust product
		<b>√</b>				As provided by the LuxTrust product
	commonName			М	D	, ,
	givenName	✓		М	D	As provided by the LuxTrust product
	surname	✓		М	D	As provided by the LuxTrust product
	countryName	✓		М	D	As provided by the LuxTrust product
	emailAddress	<b>✓</b>		0	D	As provided by the LuxTrust product
	title	<b>✓</b>		М	D	As provided by the LuxTrust product
						As provided by the LuxTrust product
	organizationName	✓		M for PRO, O for PRIV	D	As provided by the Edithust product
	localityName	✓		M for PRO, O for PRIV	D	As provided by the LuxTrust product
	organizationalUnitName 17	<b>✓</b>		M for PRO, O for PRIV	D	As provided by the LuxTrust product
	organizationalUnitName	<b>✓</b>		0	D	As provided by the LuxTrust product
subjectPub	olicKeyInfo	<b>√</b>	False			
	algorithm subjectPublicKey	✓ ✓		M M		Public Key: Key length: from 3072 bits up 4096 bits (RSA); public exponent: Ferma
	SubjectPublickey	*		IVI		(0x010001).
Extensions						(
Authority F						
authorityKe	eyldentifier	✓	False			
	keyldentifier	✓		М		SHA-1 Hash of the LuxTrust Glo  Qualified CA x public key
authorityln	foAccess	<b>√</b>	False			Qualified CA x public key
<u>autinorityiii</u>	AccessMethod	<b>√</b>	i disc			ld-ad-2
	accessLocation	✓		М		http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	<b>✓</b>				Id-ad-1
	accessLocation	<b>√</b>		М		http://gca.ocsp.luxtrust.lu/
RI Distrib	l utionPoint	<b>✓</b>	False			nttp://qca.ocsp.ndxtrdst.nd/
INEDISTIB	distributionPoint	· /	i aise		S	
	fullName	✓		М		http://crl.luxtrust.lu/LTGQCAx-yy.crl
Subject Pro	nerties					interior in a second control of the second c
subjectKey		<b>√</b>	False			
	keyldentifier	<b>✓</b>		М	Fixe	SHA-1 Hash of the LuxTrust Glo
	1				d	Qualified CA x public key
Policy Prop	perties	<b>✓</b>	Truc	1		
keyUsage	digitalSignature	✓ ✓	True		S	False
	nonRepudiation			M	S	True
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificateF		<b>√</b>	False	B 4		4 2 474 4 4 40 2 20
	PolicyIdentifier	✓ ✓	-	M	-	1.3.171.1.1.10.3.39
	policyQualifierID qualifier	✓ ✓		M M	S	Id-qt-1 (CPS) https://repository.luxtrust.com
	Policyldentifier	<b>∨</b>	-	M	- 3	0.4.0.194112.1.2
QualifiedCo	ertificateStat	<b>√</b>	False	IVI		0.7.0.107112.1.2
	QcCompliance	·	. 4.50	М	S	True
	(0.4.0.1862.1.1)					
	QcSSCD (0.4.0.1862.1.4)	✓		М	S	True

 $<sup>^{\</sup>rm 17}$  Two occurrences of this field are supported in this profile



LuxTru	LuxTrust Signing Server LuxTrust PRI/PRO delegated Sign QCP-n-qscd Certificate Profile									
Attribute	Field	IN	CE	O/M	CO	Value				
	QcPDS	✓		M	S	https://repository.luxtrust.com				
	(0.4.0.1862.1.5)									
	QcType (0.4.0.1862.1.6)	✓		M	S	id-etsi-qct-esign				
						(0.4.0.1862.1.6.1)				

# 1.11.47 LuxTrust Signing Server elD LU delegated Sign QCP-n-qscd Certificate Profile

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by LuxTrust, from 3072-bit key size and with a key usage that supports qualified electronic signature. This profile is only associated with identification performed with a notified eID LU.

L	uxTrust Signing Se	rver el	D LU d	elegate	ed Sign	QCP-n-qscd Certificate Profile
Attribute	Field	IN	CE	O/M	СО	Value
Base Profile						
Version		<b>✓</b>	False			
				М	S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
				M	FDV	Validated on duplicates.
signatureAlo		✓	False			
	algorithm			М	S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
		L		M	D	Issuing CA Signature.
Issuer	T 4 N	<b>√</b>	False		S	
	countryName	<b>√</b>		M	S	LU
	commonName	✓ ✓		M	S	LuxTrust Global Qualified CA x
Validity	organizationName	<b>✓</b>	False	M	S	LuxTrust S.A.
validity	NotBefore	<b>V</b> ✓	raise	М	D	Certificate generation process date/time.
	NotAfter	<b>√</b>		M	D	Certificate generation process date/time.  Certificate generation process date/time + 1 Month
subject	NOLAILEI	<b>√</b>	False	IVI		Certificate generation process date/time + 1 Month
Subject	serialNumber	✓ ·	1 4150	М	D	As provided by the eID LU product
				IVI		As provided by the eID LU product
	commonName	✓		М	D	
	givenName	✓		М	D	As provided by the eID LU product
	Surname	✓		М	D	As provided by the eID LU product
	countryName	✓		М	D	As provided by the eID LU product
	emailAddress	✓		0	D	As provided by the eID LU product
	Title	✓		М	D	As provided by the eID LU product
	organizationalUnitNa me	✓		0	D	As provided by the eID LU product
subjectPubl	icKeyInfo	✓	False			
-	algorithm	✓		М		Public Key: Key length: from 3072 bits up to 4096
	subjectPublicKey	✓		М		bits (RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Pr	operties					
authorityKey		<b>√</b>	False			
	keyldentifier	<b>✓</b>		М		SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInfo		✓	False	_		
	AccessMethod	✓				ld-ad-2
	accessLocation	<b>√</b>		M		http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓		М		http://qca.ocsp.luxtrust.lu/
cRLDistribu		<b>√</b>	False			
	distributionPoint	✓			S	



Lu	LuxTrust Signing Server eID LU delegated Sign QCP-n-qscd Certificate Profile										
Attribute	Field	IN	CE	O/M	CO	Value					
	fullName	<b>✓</b>		М		http://crl.luxtrust.lu/LTGQCAx-yy.crl					
Subject Prop	erties										
subjectKeylo	lentifier	✓	False								
	keyldentifier	<b>✓</b>		М	Fixed	SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key					
Policy Prope	rties										
keyUsage		✓	True								
	digitalSignature	<b>✓</b>			S	False					
	nonRepudiation			М	S	True					
	keyEncipherment	<b>√</b>			S	False					
	dataEncipherment	✓			S	False					
certificatePo	licies	✓	False								
	Policyldentifier	✓		М		1.3.171.1.1.10.3.40					
	policyQualifierID	✓		М	S	Id-qt-1 (CPS)					
	qualifier	✓		М	S	https://repository.luxtrust.com					
	Policyldentifier	✓		М		0.4.0.194112.1.2					
QualifiedCer		✓	False								
	QcCompliance (0.4.0.1862.1.1)	<b>✓</b>		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	<b>√</b>		М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>✓</b>		М	S	https://repository.luxtrust.com					
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)					

# 1.11.48 LuxTrust Corporate LCP Certificate Profile

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

	LuxTr	ust Corp	orate LCF	Certifica C	te Profile	e – Corporate CA
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Base Profile						
Version		<b>~</b>	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Sequential CSN
signatureAlgo	rithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with RSA Encryption.
signatureValue	signatureValue		False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Corporate CA x1
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 36 Months
Subject	•	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card



Attributo	LuxTr	ust Corp	Orate LCF CE <sup>9</sup>	O/M <sup>10</sup>	te Profile CO <sup>11</sup>	- Corporate CA Value
Attribute	Field	IN° ✓	CE	O/MI10	CO	PRO and PRIVATE products: Surname(s) as
	Surname	v		М	D	on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	<b>*</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		M for PRO	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form
	localityName	<b>√</b>		M for PRO	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUni tName 1	<b>√</b>		M for PRO prod., condi- tional (O) for PRIV prod	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUni tName 2	<b>√</b>		0	D	PRO products only: Company/institution department or other information item
subjectPublick		✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit up to 4096
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (0x010001).
Extensions						
Authority Properties						
authorityKeyld	keyldentifier	<b>√</b>	False			SHA-1 Hash of the LuxTrust Corporate CA public key
authorityInfoA	ccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTCCAx2.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://cca.ocsp.luxtrust.lu/
cRLDistributio	nPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTCCAx1.crl
Subject Properties						
subjectAltNam	e	✓	False			
	Rfc822Name	✓		0	D	N/A
subjectKeylde	ntifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	I 11 14 161	✓	True			-
	digitalSignature	<b>√</b>			S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment dataEnciphermen	<b>√</b>			S	False False
certificatePolic	l L	<b>√</b>	False			
	463		raise			



	LuxTrust Corporate LCP Certificate Profile – Corporate CA										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value					
	Policyldentifier	✓				1.3.171.1.1.10.4.1					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	Policyldentifier	✓				0.4.0.2042.1.3					

## 1.11.49 LuxTrust Corporate eSeal LCP Certificate Profile

LuxTrust Certificates for Advanced 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

	LuxTr	ust Adv	anced L	CP eSEAL	Certifica	ate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Base	i ieid		OL.	O/IVI	- 00	Value
Profile						
Version		<b>✓</b>	False			
10.0.0.			i aloc		S	Version 3 Value = "2"
SerialNumbe	er .	<b>✓</b>	False			Voloion o Valdo – E
Contantanto	Ī		1 0100		FDV	Validated on duplicates.
signatureAlg	orithm	<b>✓</b>	False		150	Validated on adplicated.
orginatar or ag	Algorithm		1 0100		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	Algorium					RSA Encryption.
signatureVal	ue	<b>√</b>	False			Ttert Eneryption.
<b>.</b>					D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	iodanig of Cognatare.
	countryName	<b>√</b>			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x1
	organizationName	√ ·			S	LuxTrust S.A.
Validity	- gammadom (amo	<i>'</i>	False			Edit ruot O.A.
, and ty	NotBefore	· /	1 4130		D	Certificate generation process date/time.
	NotAfter	· /			D	Certificate generation process date/time + 24
	Notate					Months
Subject		<b>✓</b>	False			Worths
Oubject			i alsc			Shall contain the full registered name of the
	commonName	✓		M	D	subject (legal person).
						the country in which the subject (legal person)
	countryName	✓		М	D	is established (ISO3166)
	organisationIdentifier (2.5.4.97)	<b>*</b>		M	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  3) "LT." for identification based on the value provided by the legal entity or by LuxTrust.  The country code is either the country code where the subject is registered as legal entitiy when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.
	organizationName organizationalUnitName	✓		M O	D D	Shall contain the full registered name of the subject (legal person).  Company/institution department or other information item
oubjectDuk!!	o Kovinto	./	Fo!			
subjectPubli		✓ ✓	False			Public Key: Key length: 2048bit up to 4096bit
	Algorithm			N 4	-	
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (0x010001).



	Lux	Trust Adv	anced L	CP eSEAL	Certifica	ate Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Extensions						
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTCCAx2.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://cca.ocsp.luxtrust.lu/
cRLDistribut	ionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTCCAx1.crl
Subject Properties						
subjectKeylo	lentifier	✓	False			
	keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy						-
Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificatePo		<b>√</b>	False			10.171.1.10.10
	Policyldentifier	✓				1.3.171.1.1.10.4.2
	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
BasicConstra	aints					
	CA	✓			S	FALSE
	pathLenConstraint	✓			S	0 (ZERO)

# 1.11.50 LuxTrust Corporate AATL Certificate Profile

LuxTrust Certificate Policy compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, This is a remote certificate issued for a short period of validity and for a single use. This certificate can only be used for a single signature process (for example, to digitally sign a set of documents/contracts). Thanks to its short validity period, this type of certificate does not need to be revoked or suspended. This Certificate include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.4.3>.

	LuxTrust Corporate NCP+ Certificate Profile – Corporate CA										
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value					
Base Profile											
Version	•	<b>√</b>	False								
					S	Version 3 Value = "2"					
SerialNumber		✓	False								
					FDV	Random CSN - Validated on duplicates.					
signatureAlgo	signatureAlgorithm		False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with RSA Encryption.					
signatureValu	е	✓	False								
					D	Issuing CA Signature.					
Issuer	Issuer		False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Corporate CA x1					
	organizationName	✓			S	LuxTrust S.A.					



						e – Corporate CA
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	CO <sup>11</sup>	Value
Validity	NetDefens	<b>√</b>	False		-	Out if and a second in a second state if an
	NotBefore	<b>✓</b>			D D	Certificate generation process date/time.
	NotAfter	<b>V</b>			ט	Certificate generation process date/time + 15 Minutes
Subject		<b>√</b>	False			Williutes
Cabjeot	serialNumber	√	1 alsc	М	D	Serial Number as constructed by LRAO
	Scriditaliber	<b>√</b>		IVI		Concatenation of given name(s) and
	commonName			М	D	surname(s) as on ID card separated by a
						"Space" character
	givenName	✓		М	D	Given name(s) as on ID card
		✓				Surname(s) as on ID card without indication
	Surname			M	D	"épouse", "ép." or similar and the subsequent
						name(s)
		✓			_	Country of the organisation requesting the
	countryName			М	D	certificate
		<b>√</b>				=> LU
	armonization Name	<b>V</b>		М	D	Provided by the organisation requesting the certificate
	organizationName			IVI		=> LuxTrust S.A.
		<b>√</b>	+	1	1	Optional - identifier of the certificate holder
	organizationalUni	]		0	D	within the organisation requesting the
	tName 1			~		certificate
subjectPublic	Kevinfo	✓	False			
,	Algorithm	✓	1			RSA - 1.2.840.113549.1.1.1, 3072 bit up to
	subjectPublicKey	✓		М	1	4096 bit.
						Based on ETSI TS 119 312, the public
						exponent e shall be an odd positive integer
						such that 2^16 < e < 2^256."
Extensions						
Authority						
Properties	1 416	<b>√</b>				
authorityKeylo		<b>✓</b>	False			CITY 4 Heats of the LiviTrust Company CA
	keyldentifier	•				SHA-1 Hash of the LuxTrust Corporate CA public key
authorityInfoA	Arrass	<b>√</b>	False			public key
addiontyllion	AccessMethod	· ✓	i aise			Id-ad-2
	accessLocation	<b>√</b>				1 11
						http://ca.luxtrust.lu/LTCCAx.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://cca.ocsp.luxtrust.lu
cRLDistributio		<b>√</b>	False			
	distributionPoint				S	1 // 11
Ond to a	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTCCAx-Y.crl
Subject Properties						
subjectAltNan	20	<b>√</b>	Folco			
SubjectAitNan	Rfc822Name	<b>√</b>	False	0	D	N/A
subjectKeylde		<b>√</b>	False	U	10	IWA
Subjective Aide	keyldentifier	<b>√</b>	i aist		Fixed	SHA-1 Hash of Subject public key – Use of 160
	regidentine	•			I IXEU	bits
Policy						
Properties						
keyUsage		✓	True			
	digitalSignature	<b>√</b>			S	False
	nonRepudiation	✓	1		S	True
	keyEncipherment	✓	1		S	False
	dataEnciphermen	✓			S	False
	t		<u> </u>	<u> </u>		
certificatePoli		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.4.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.com
	Policyldentifier	<b>√</b>	+		1	0.4.0.2042.1.2
id-etei-valaee	ured-ST-certificate	<b>√</b>	False			U.T.U.ZUTZ.1.Z
iu-cisi-vaia55l	0.4.0.194121.2.1	<b>√</b>	i alse			
BasicConstrai		<b>√</b>	False			
240.0001101141	CA	· ✓	False			
			. 4.50		1	1



## 1.11.51 BNPPF Corporate AATL Certificate Profile

BNPPF Certificate Policy compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, This is a remote certificate issued for a short period of validity and for a single and **exclusive** use in applications managed by BNPPF (FORTIS). This certificate can only be used for a single signature process (for example, to digitally sign a set of documents/contracts). Revocation is not applicable Thanks to the short validity period of this type of certificate. This Certificate include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.4.5>.

A44 !!						- Corporate CA
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M	CO <sup>11</sup>	Value
Base Profile						
Version		<b>√</b>	False			
Version		•	i aise			
	1				S	Version 3 Value = "2"
SerialNumbe	r	<b>√</b>	False		-	version 5 value – 2
- Contain turning			1 0.00		FDV	Random CSN - Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with
						RSA Encryption.
signatureVal	ue	✓	False		_	
		<b>√</b>	F-1		D	Issuing CA Signature.
Issuer	- countryNome	<b>∨</b>	False		S	LU
	countryName commonName	<b>√</b>		<del> </del>	S	LuxTrust Corporate CA x <sup>1</sup>
	organizationName	·			S	LuxTrust S.A.
Validity	organization tante	<b>√</b>	False		J	Eux Tust G.A.
	NotBefore	<b>√</b>	. 4.00		D	Certificate generation process date/time.
	NotAfter	✓	1	1	D	Certificate generation process date/time + 15
						Minutes
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Provided by BNPPF (FORTIS)
	givenName	<b>√</b>		M	D	Provided by BNPPF (FORTIS)
	Surname	<b>✓</b>		М	D	Provided by BNPPF (FORTIS)  Country of the organisation requesting the
	countryName	*		М	D	certificate
	Journal yrunne			'''		⇒ BE
	organizationName	✓		N/	D	'BNPPF Customer' as Provided by BNPPF
	organizationivanie			М	D	(FORTIS)
		✓				Provided by BNPPF (FORTIS): identifier of the
	organizationalUnitName 1			0	D	certificate holder within the organisation and (optionally) of the certificate request type
subjectPubli	- Kevinfo	<b>✓</b>	False			(optionally) of the certificate request type
Subjecti ubii	Algorithm	·	1 alsc			RSA - 1.2.840.113549.1.1.1, 3072 bit up to
	subjectPublicKey	✓		М		4096 bit.
	, , , , , , , , , , , , , , , , , , , ,					Based on ETSI TS 119 312, the public
						exponent e shall be an odd positive integer
Extensions						such that 2^16 < e < 2^256."
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Corporate CA
	<u> </u>	,	L	1		public key
authorityInfo		<b>√</b>	False			
	AccessMethod	<b>√</b>	<del> </del>	<del> </del>	ļ	Id-ad-2
	accessLocation	<u> </u>				http://ca.luxtrust.lu/LTCCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://cca.ocsp.luxtrust.lu
cRLDistribut		<b>√</b>	False			
	distributionPoint	<b>√</b>		<del> </del>	S	hua // add by day at by // TOO A
Cubicat	fullName	✓				http://crl.luxtrust.lu/LTCCAx-Y.crl
Subject Properties						
subjectAltNa	me	<b>√</b>	False			
JubjectAitila		·	1 0130	0	D	N/A
	Rfc822Name					



	LuxTrust Corporate NCP+ Certificate Profile – Corporate CA									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M	CO <sup>11</sup>	Value				
	keyldentifier	<b>√</b>			Fixe d	SHA-1 Hash of Subject public key – Use of 160 bits				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	False				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificatePo	icies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.4.5				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.com				
	Policyldentifier	✓				0.4.0.2042.1.2				
id-etsi-valass	sured-ST-certificate	✓	False							
	0.4.0.194121.2.1	✓								
BasicConstra	aints	✓	False							
	CA	✓	False							

# 1.12 Timestamping Certificate Profile

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

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

	LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	per	✓	False							
					FDV	Validated on duplicates.				
signatureA		✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureV	alue	✓	False		_					
			L		D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	<b>√</b>			S	LU				
	commonName	1			S	LuxTrust Global Timestamping CA x <sup>1</sup>				
	organizationName	<b>√</b>			S	LuxTrust S.A.				
Validity		<b>√</b>	False							
	NotBefore	<b>√</b>			D	Certificate generation process date/time.				
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 60 Months				
subject		✓	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				
subjectPub	licKeyInfo	✓	False							
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);				
	subjectPublicKey	✓		М		public exponent: Fermat-4 (0x010001).				



	LuxTru	st Time	estampi	ng Cert	ificate I	Profile
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	Value
Extensions						
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust
						Timestamping CA public key
authorityInfo		<b>√</b>	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGTSACAx1.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTGTSACAx1.crl
Subject						
Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓		0	D	info@luxtrust.lu
subjectKeylo		✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit
						field with a 0100 value, followed by the
						least significant 60 bits of the SHA-1 hash
						of the value or subjectPublicKey bit string
						(tag, not including the length and number of unused bit-string bits).
Policy						or unused bit-string bits).
Properties						
keyUsage			True			
Reyosage	digitalSignature	· ·	Tiuc		S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
Extended Ke		✓	False		Ŭ	- caree
	TimeStamping	<b>√</b>	. 4.00		S	Set
	(1.3.6.1.5.5.7.3.8)				_	
Private Key l	Jsage Period	✓	False			
	Usage period (2.5.29.16)	✓		М	D	Certificate generation process date/time +
	,		<u> </u>			12 Months
certificatePo		✓	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 with
						ETSI TS 102 042. Sole authorised usage:
						Signature of LuxTrust Trusted Time
						Stamp tokens generated by LuxTrust
	Dalland Jan (16 au			ļ		time-stamping authority.
	Policyldentifier	✓	1		l	0.4.0.2042.1.3

# 1.12.1 Normalized (NCP+) 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 12 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.



Attribute   Field   IN®   CE®   O/M®   CO®   Value		Normalized (NCI	2+) Ce	rtificate	Policy fo	r LuxTri	ust Qualified Timestamping
Base   Profile   Version   V   False   S   Version 3 Value = "2"	Attribute		IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	CO <sup>11</sup>	
Version	Base						
SerialNumber							
SerialNumber	Version		✓	False		_	
Signature   Algorithm			,			S	Version 3 Value = "2"
SignatureAlgorithm   SignatureAlgorithm   SignatureValue   SignatureValu	SerialNumbe	<u>:r</u>	<b>✓</b>	False		ED\/	Validated an displicated
algorithm   S   OID = "12.840.113549.1.1.11" - SHA256 will signatureValue   V   False   D   Issuing CA Signature.	cianoturo Ala	Jorithm	-/	Folso		FDV	Validated on duplicates.
signatureValue	signatureAig		· ·	raise			OID = "1 2 840 113549 1 1 11" - SHΔ256 with
issuer    CountryName		algorithm				S	
Sissuer	signatureVal	ue	✓	False			The state of the s
CountryName						D	Issuing CA Signature.
CommonName   V   S   LuxTrust Global Qualified CA x   Validity	issuer		✓	False			
NotBefore   V   False   D   Certificate generation process date/time.							_
NotBefore			✓				
NotBefore   V		organizationName				S	LuxTrust S.A.
NotAfter	Validity			False		_	
subject    OrganisationIdentifier (2.5.4.97)		NotBefore	✓			D	
subject    OrganisationIdentifier (2.5.4.97)		NotAfter	✓			D	
OrganisationIdentifier (2.5.4.97)	subject		1	Falso			INDITION OF THE PROPERTY OF TH
CommonName	Jabjoot	organisationIdentifier		1 0130			
CommonName   V   M   D   LuxTrust Qualified Timestamping organizationName   V   M   D   LuxTrust S.A.			<b>✓</b>		M	D	VAILU-20976985
SubjectPublicKeyInfo	ļ		✓		М	D	
SubjectPublicKeyInfo					M	D	
algorithm					М	D	LU
SubjectPublicKey   V	<u>subjectPubli</u>			False			
Extensions   Authority   Properties   authorityKeyIdentifier							
Authority Properties authoritykeyldentifier   keyldentifier	Evtonolono	subjectPublickey	· ·		IVI		public exponent: Fermat-4 (0x010001).
Properties authorityKeyldentifier    keyldentifier							
authorityKeyldentifier							
Reyldentifier   V		Identifier	<b>√</b>	False			
AccessMethod   AccessLocation   AccessMethod   AccessMethod   AccessMethod   AccessLocation   AccessMethod   AccessLocation		keyldentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA
accessLocation	authorityInfo		✓	False			
AccessMethod   accessLocation   distributionPoint   distribution		AccessMethod	✓				1 11
accessLocation		accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx1.crt
cRLDistributionPoint       ✓       False         distributionPoint       ✓       S         fullName       ✓       http://crl.luxtrust.lu/LTGQCAx.vy.crl         Subject Properties       SubjectAltName       ✓       False         Rfc822Name       ✓       False         subjectKeyldentifier       ✓       False         keyldentifier       ✓       False         Fixed       The Key Identifier comprises a four-bit field volume, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).         Policy Properties       Properties         keyUsage       ✓       True         digitalSignature nonRepudiation       ✓       S       True         nonRepudiation keyEncipherment       ✓       S       False							
distributionPoint   fullName   /							http://qca.ocsp.luxtrust.lu/
Subject   Properties	cRLDistributi		_	False			
Subject Properties subjectAltName  Rfc822Name SubjectKeyldentifier  Rfc822Name Fixed  Reyldentifier  Fixed  Reyldentifier comprises a four-bit field on 0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).  Reylsage  Rey	-					S	hus Wed by drove the // TOOO Assessed
Properties subjectAltName  ✓ False  Rfc822Name ✓ False  SubjectKeyldentifier  ✓ False  The Key Identifier comprises a four-bit field of 0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).  Policy Properties  keyUsage  ✓ True  digitalSignature nonRepudiation ✓ S False  keyEncipherment ✓ False  The Key Identifier comprises a four-bit field of 0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).  For info@luxtrust.lu  The Key Identifier comprises a four-bit field of 0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).  For info@luxtrust.lu  S False  Fixed  S False  S False	Cubicot	tuliname	<b>V</b>				http://cri.luxtrust.lu/LTGQCAx.yy.cri
Rfc822Name   V   False   SubjectKeyldentifier   V   False   The Key Identifier comprises a four-bit field of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).    Policy Properties   KeyUsage   V   True   S   True							
Rfc822Name		me	<b>√</b>	False			
SubjectKeyldentifier   V   False   The Key Identifier comprises a four-bit field of 0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).    Policy Properties   Properti			<b>✓</b>		0	D	info@luxtrust.lu
keyldentifier       ✓       Fixed       0100 value, followed by the least significant of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including length and number of unused bit-string bits).         Policy Properties       ✓       True         keyUsage       ✓       True         digitalSignature nonRepudiation       ✓       S       False         keyEncipherment       ✓       S       False	subjectKeyld		✓	False			
keyUsage         ✓         True           digitalSignature         ✓         S         True           nonRepudiation         ✓         S         False           keyEncipherment         ✓         S         False		keyldentifier	<b>✓</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
keyUsage         ✓         True           digitalSignature         ✓         S         True           nonRepudiation         ✓         S         False           keyEncipherment         ✓         S         False							
digitalSignature			1	Truo			
nonRepudiation     ✓     S     False       keyEncipherment     ✓     S     False	reyusaye	digitalSignature		rrue		S	True
keyEncipherment ✓ S False	-			<u> </u>			
	ļ		<b>√</b>				
dataEncipherment ✓ S False		dataEncipherment					
Extended Key Usage ✓ True	Extended Ke	y Usage	✓	True			
TimeStamping S Set			✓	<u> </u>		S	Set
(1.3.6.1.5.5.7.3.8)	Delegate 17			F			
Private Key Usage Period	Private Key L		<b>✓</b>	False			Contiliante generation process detailment of
Usage period (2.5.29.16)  M  D  Certificate generation process date/time + 24 Months			✓		M	D	Certificate generation process date/time + 24
certificatePolicies    False	certificatePo		<b>✓</b>	Falso			MOTULO
Policyldentifier   ✓   1.3.171.1.1.10.3.18	Jor IIII Jater O		1	1 0130			1.3.171.1.1.10.3.18
policyQualifierID ✓ S Id-qt-1 (CPS)	-					S	
qualifier ✓ S https://repository.luxtrust.lu	ŀ		<b>√</b>	1			
policyQualifierID   S Id-qt-2 (User Notice)	I		1 /	l			
Policyldentifier   0.4.0.2042.1.2	}		✓	<u></u>		3	id-qt-2 (Oser Notice)



#### 1.12.2 Qualified Timestamping Certificate Profile

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

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 3161 and RFC5816. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties. This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [21] and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles [22].

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

	Qualified Cer	rtificat	e Policy	for for L	uxTrust	Qualified Timestamping
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	O/M <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value
Base			02	O/III		
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	r	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
-!						Encryption.
signatureVal	ue T	✓	False			Lagrica OA Cinnatura
laguar		<b>√</b>	Folos		D	Issuing CA Signature.
issuer	countryNamo	<b>✓</b>	False		S	LU
	countryName commonName	V /			S	1
		<b>V</b> ✓				LuxTrust Global Qualified CA x <sup>1</sup>
Volidite	organizationName	✓ ✓	Folse		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Cartificate generation process data/time
	NotBefore	V /			D	Certificate generation process date/time.  Certificate generation process date/time + 60
	Notatier	•			ן ט	Months
subject		<b>√</b>	False			Worturs
Subject	organisationIdentifier		1 0100		_	=
	(2.5.4.97)	✓		М	D	VATLU-20976985
		_			_	LuxTrust Qualified Timestamping
	commonName	✓		М	D	
	organizationName	✓		М	D	LuxTrust S.A.
	countryName	✓		M	D	LU
subjectPubli		✓	False			
	algorithm	✓				Public Key: Key length: up to 3072 bit (RSA)
	subjectPublicKey	✓		M		public exponent: Fermat-4 (0x010001).
Extensions						
Authority						
Properties	I de la Ciffe de					
authorityKey		<b>✓</b>	False			CLIA 4 hope of the Low-Tweet Clabel Qualified CA
authorityInfo	keyldentifier	<b>∨</b>	False			SHA-1 hash of the LuxTrust Global Qualified CA
authorityiiiio	AccessMethod	<b>✓</b>	raise			ld-ad-2
	accessLocation	<b>V</b> ✓	<del>                                     </del>		<del>                                     </del>	http://ca.luxtrust.lu/LTGQCAx <sup>1</sup> .crt
		<b>V</b> ✓			-	•
	AccessMethod accessLocation	✓ ✓			-	Id-ad-1
	accessLocation	*				http://qca.ocsp.luxtrust.lu/
cRLDistribut	ionPoint	<b>/</b>	False			
J. C. Distribut	distributionPoint	· ·	1 4136		S	
	fullName	· /			<del>                                     </del>	http://crl.luxtrust.lu/LTGQCAx <sup>1</sup> .crl
						http://oii.iuxtiust.iu/ETGQCAX .CII
Subject						
Properties						
subjectAltNa	me	<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	info@luxtrust.lu
subjectKeyld		✓	False			
, j.u						



Qualified Certificate Policy for for LuxTrust Qualified Timestamping							
Attribute	Field	IN <sup>8</sup>	CE <sup>9</sup>	<b>O/M</b> <sup>10</sup>	<b>CO</b> <sup>11</sup>	Value	
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).	
Policy Properties							
keyUsage		✓	True				
	digitalSignature	✓			S	True	
	nonRepudiation	✓			S	False	
	keyEncipherment	✓			S	False	
	dataEncipherment	✓			S	False	
Extended Ke		✓	True				
	TimeStamping (1.3.6.1.5.5.7.3.8)	<b>√</b>			S	Set	
Private Key l	Jsage Period	✓	False				
	Usage period (2.5.29.16)	<b>√</b>		М	D	Certificate generation process date/time + 12 Months	
certificatePo	licies	✓	False				
	Policyldentifier	✓				1.3.171.1.1.10.3.19	
	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	licies	✓					
	QcType (0.4.0.1862.1.6)	<b>✓</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)	
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True	
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	URL=https://www.luxtrust.com/repository	

# 1.12.3 TimeStamp Request and Response Format

# 1.12.3.1 TimeStamp Request Format

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

LuxTrust Time Stamp Request								
Field	Value / comment							
Document Hash	Hash of the document on which the TimeStamp must be computed							
Hash OID	(SHA-256/SHA-512)  Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.							
Policy OID	1.3.171.1.1.10.3.18.1  The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.							
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.							
Should TSA Certificate be included?	TRUE/FALSE							
Request Extensions	Value *							
None	None							





\*no extension is required to be supported

# 1.12.3.2 TimeStamp Response Format

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

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

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

## 1.12.4 Certificate extensions

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

#### 1.12.5 Algorithm object identifiers

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

#### 1.12.6 Name forms

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

## 1.12.7 Name constraints

Name constraints are supported as per RFC 5280.

## 1.12.8 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

## 1.12.9 Usage of Policy Constraints extension

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

## 1.12.10 Policy qualifiers syntax and semantics

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

## 1.12.11 Processing semantics for the critical Certificate Policies

Not applicable.





# 1.13 CRL profile

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

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

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

LuxTrust CRL Profile								
Field	Comments							
Version	v2							
Signature	Same signature algorithm as related CA							
Issuer	<subjectca></subjectca>							
thisUpdate	<creation time=""></creation>							
nextUpdate	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" qualified="" subordinate="" time=""></creation></creation></pre>							
	<creation (8="" +="" 30="" 8,5="" and="" for="" hours="" minutes)="" p="" subordinate<="" time=""></creation>							
	SSL CAs>							
	<pre><creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></pre>							
revokedCertificates								
userCertificate	<certificate number="" serial=""></certificate>							
revocationDate	<revocation time=""></revocation>							
crlEntryExtensions								
reasonCode	<insert code="" list="" of="" reason="" revocation="" used=""></insert>							
crlExtensions								
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>							
authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>							

To avoid performance degradation that results from a big CRL size, LuxTrust uses partitioned CRL for LTGQCAx OCSP certificates. The CRLs can be downloaded from http://crl.luxtrust.lu/LTGQCAx-OCSP.crl. To prevent this CRL from treating the status of any certificate not listed on this CRL, we include in the CRL format the issuing distribution point extension as specified in RFC 5280. Please find below the format of this CRL:

LuxTrust CRL Profile							
Field	Comments						
Version	v2						
Signature	Same signature algorithm as related CA						
Issuer	<subjectca></subjectca>						
thisUpdate	<pre><creation time=""></creation></pre>						
nextUpdate	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" qualified="" subordinate="" time=""></creation></creation></pre>						
	<pre><creation (8="" +="" 30="" 8,5="" and="" for="" hours="" minutes)="" pre="" subordinate<="" time=""></creation></pre>						
	SSL CAs>						
	<pre><creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></pre>						
revokedCertificates							
userCertificate	<pre><certificate number="" serial=""></certificate></pre>						
revocationDate	<revocation time=""></revocation>						
crlEntryExtensions							
reasonCode	<pre></pre> <pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre></pre>						
crlExtensions							
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>						
authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>						
IssuingDistributionPoint	<pre><distributionpoint> http://crl.luxtrust.lu/LTGQCAx-OCSP.crl</distributionpoint></pre>						

To comply with the following ETSI requirement:

[ETSI EN 319411-2] clause 6.3.10a Certificate Status Services Revocation status information is not available beyond the validity period of the certificate.

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





We have created a complete CRL for our LTGQCA's which contains expired certificates and revoked certificates. To avoid performance degradation that results from a big CRL size, this new CRL is not referenced in any certificate. This CRL has a validity of 48 hours and will be generated every 24 hours.

Please find below the format of this CRL:

LuxTrust Complete CRL Profile							
Field	Comments						
Version	v2						
Signature	Same signature algorithm as related CA						
Issuer	<subjectca></subjectca>						
thisUpdate	<creation time=""></creation>						
nextUpdate	<creation +="" 48="" cas="" for="" hours="" other="" qualified="" subordinate="" time=""></creation>						
revokedCertificates							
userCertificate	<pre><certificate number="" serial=""></certificate></pre>						
revocationDate	<revocation time=""></revocation>						
crlEntryExtensions							
reasonCode	<insert code="" list="" of="" reason="" revocation="" used=""></insert>						
crlExtensions							
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>						
authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>						

#### 1.13.1 Version number(s)

See section 3.4.

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

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

## 1.13.2 CRL entry extensions

See section 3.4.

## 1.14 OCSP profile

The OCSP profile follows IETF PKIX RFC 6960 OCSP v1 and v2. The LuxTrust CAs support signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA.

## 1.14.1 Version number(s)

See section 3.5.

#### 1.14.2 OCSP extensions

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

LuxTrust OCSP Certificate Profile							
Attribute	Field	IN	CE	O/M	CO	Value	
Base Profile							
Version		✓	False				
					S	Version 3 Value = "2"	
SerialNumbe	SerialNumber		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 LTGRCA Signature	
issuer	issuer		False		S		
	countryName	✓			S	LU	
	commonName	✓			S	LuxTrust Global Root x	



LuxTrust OCSP Certificate Profile							
Attribute	Field	IN	CE	O/M	CO	Value	
	organizationName	✓			S	LuxTrust S.A.	
Validity		✓	False				
	NotBefore	✓			D	Certificate generation process date/time.	
	NotAfter	✓			D	Certificate generation process date/time +	
						maximum 12 Months	
subject		✓	False				
	countryName	✓		М	D	LU	
	organizationName	✓		М	D	LuxTrust S.A.	
	organizationalUnitName 1	✓		0	D	Pki entity	
	commonName	✓		М	D	LuxTrust S.A. OCSP Server 2	
subjectPubli		✓	False				
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);	
	subjectPublicKey	✓		М		public exponent: Fermat-4 (0x010001).	
Extensions							
Authority							
Properties							
authorityKey		<b>√</b>	False				
	keyldentifier	✓				SHA-1 Hash of the LuxTrust LTGR x CA	
id-ocsp-noch	nook	<b>✓</b>	False			public key	
iu-ocsp-noci	leck	<b>√</b>	raise		S	NULL	
Subject		T V			3	NULL	
Properties							
subjectKeylo	lentifier	<b>√</b>	False				
Subjectivelyie	keyldentifier	1	1 4150		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						or unused bit string bits).	
Properties							
keyUsage		✓	True				
	digitalSignature	<b>√</b>			S	True	
	nonRepudiation	<b>√</b>			S	False	
	keyEncipherment	<b>√</b>			S	False	
	dataEncipherment	<b>√</b>			S	False	
certificatePo	licies	<b>√</b>	False				
,			1 2.00				
		1	1	i e			
	qualifier	<b>√</b>	1	i e	S	https://repository.luxtrust.lu	
	policyQualifierID	<b>√</b>	1	1	S	Id-qt-2 (User Notice)	
	noticeNumbers	1					
	DisplayText	<b>√</b>				LuxTrust S.A. Online Certificate Status Server. IETF PKIX RFC 6960 OCSP v1 and v2. No OCSP extensions are	
	Deli end de máléi	+	1		-	supported.	
Futon de dat	Policyldentifier	✓	Fals :			0.4.0.2042.1.3	
Extended Key Usage		<b>√</b>	False			Total	
	OCSPSigning	✓			S	True	

# 1.15 Integration certificates

LuxTrust Integration certificates delivered in the context of test activities are identified by same O.I.D as real certificates but prefixed with 2.999 {joint-iso-itu-t(2) example(999)}.