

Version number: 1.32 Publication Date: 19/11/2020 Effective Date: 19/11/2020

LuxTrust S.A

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

Luxembourg | VAT LU 20976985 | RCS B112233

Business Number N°00135240/0

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





## **Document Information**

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

# **Version History**

Version	Who	Date	Reason of modification
1.0	MSC	29/08/2011	Initial Version DRAFT
1.01	MSC	27/10/2011	Added CRL validity period, revision
1.02	MSC	24/11/2011	Modified – Document OIDs for Cas
1.03	MSC	09/02/2012	Modified – Added LCP for integration purposes.
1.04	MSC	01/03/2012	Modified:
			<ul> <li>Added LCP for integration purposes for CSS</li> </ul>
			Table for OIDs
			Modification of the CRL issuance algorithm (SHA256 to SHA1)
1.05	MSC	19/03/2012	Modifications following review by Chris Quaresimin and Laurent Breuskin:              Removal of + Nestcape proprietary extension:             NetscapeCertificateType: sslClient, smime for non-SSL products             Display text for CSS integration product             Correct CRL and Ala for CSS integration product
1.06	MSC	26/03/2012	SSL Object certificate profile  Modifications for CSS certificates, signature will be performed using
1.06	IVISC	26/03/2012	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:
			Table for OIDs & LuxTrust CA Hierarchy
1.09.1	LBR	02/08/2012	Update of OID Page 22
1.09.2	MSC	07/08/2012	Added: Certificate profile for Extended Validation Certificates :
			EVCP – ETSI TS 102 042
			EVCP+ - ETSI TS 102 042
			Added: Certificate profile for Secure Online File Exchange (SOFiE)
1.10	YNU	23/08/2012	Review for validation of CP
1.10	CSPBoard	24/08/2012	Validation
1.11	CSPBoard	20/09/2012	Typo update
1.12	YNU	21/12/2012	Added CP SSL/TLS Certificate for Client Authentication
	TKO		Added CP non SSCD NCP+ Certificates supporting Advanced
			Electronic Signatures for Mass Signature Services
1.10	000	20/24/2042	Various syntactical and format corrections
1.13	CSP Board	23/04/2013	insertion of ILNAS logo including accreditation reference and technical standards reference
1.14	YNU	29/11/2013	Update specific requirements for CP under the SSL CA
1.15	YNU	18/01/2014	Clarification on Mozilla request
1.16	YNU	05/06/2014	Update Cp
			<ul> <li>for LuxTrust Global Root Renew</li> <li>QcS2 et QcS3</li> <li>Typo</li> <li>Add CP Seal Signature Services</li> </ul>
1.17	YNU	30/06/2014	Add certificate profile for eID
	_		CP eID QCP+
			CP eID NCP+
			Update CP Seal Signature Services OID
1.18	YNU	15/10/2014	Update AIA in SSL CA



4.40	N/NII I	44/44/0044	Library Ala is OB and so the OOL OA size a OOL OA O				
1.19	YNU	11/11/2014	Update AIA in CP under the SSL CA since SSL CA 2				
1.20	YNU	19/12/2014	Add Integration CP for eID Update eID CP with pseudonym Update Global Root CA CP with OID attribute				
			Update SSL CA profile since SSL CA 3 Update lifetime of SSL Server/Object/SSL Client auth to 24 months				
1.21	CSP Board	25/03/2015	Update LT CA - lifetime up to 20 years - AIA				
			Update Display text - EV SSL CP Update eID CP				
1.22	YNU	03/11/2015	Update ILNAS Logo Update Common Names in non SSL certificates				
			Remove NetscapeCertType extension from SSL and Object Signing Certificates Added: OCSP signing Certificate which contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560				
1.23	YNU	05/08/2016	Add Timestamping Profile under Global Qualified CA Update Signing Server LCP Certificate profil				
1.24	DEL	12/06/2017	Add:  • LuxTrust Qualified Timestamping Certificate profile with QC				
			<ul> <li>statements</li> <li>SPARE LuxTrust Signing Server LCP Certificate Profile</li> <li>Qualified/Advanced eSeal certificate profiles</li> </ul>				
			<ul> <li>eIDAS qualified certificate profiles</li> <li>Signing Server Signature and eSeal certificates and QWAC certificate and signing stick certificates</li> </ul>				
1.25	DEL	30/08/2017	Add Microsoft OIDs in SSL certificates profiles to ensure alignement with Microsoft Trusted Root certificate Program requirements ( <a href="https://technet.microsoft.com/en-us/library/cc751157.aspx">https://technet.microsoft.com/en-us/library/cc751157.aspx</a> ).				
1.26	NDE DEL	24/11/2017 15/12/2017	Increase CRL validity from 4h30min to 8h30min for SSL certificates     Increase CRL validity from 4h30min to 8h30min for SSL certificates				
	DEL	01/01/2018	<ul> <li>Update hash functions in accordance with normative requirements</li> <li>Add Advanced eSeal certificate profile</li> </ul>				
1.27	DEL	19/03/2018	<ul> <li>Add LuxTrust Corporate CA &amp; Corporate certificate profile</li> <li>Update SSL certificates profiles to support Certificate         Transparency     </li> </ul>				
1.28	DEL	29/06/2018	<ul> <li>Change O.I.D in SSL OV certificates</li> <li>Introduce O.I.D prefixed with 2.999</li> <li>Partitioned CRLS</li> </ul>				
1.29	DEL	19/03/2019	Long term Timestamping (In Test)     Setting an Issue Distribution point (IDP) in Partitioned CRL     New CRL creation				
1.30	DEL	21/10/2019	<ul> <li>Long term Timestamping (In production)</li> <li>LCP Certificate Profile Update</li> <li>Upgrading the public key length for the profiles with OID:         <ol> <li>1.3.171.1.1.10.3.5 &amp; OID: 1.3.171.1.1.10.3.20 from 2048 bit (RSA)</li> <li>to Public Key length from 2048 bit up to 4096bit (RSA)</li> </ol> </li> <li>Adding Wildcard - LCP certificates supporting Signature,         <ol> <li>Authentication &amp; Encryption</li> </ol> </li> </ul>				
1.31	YNU	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 1.3.171.1.1.10.3.32, o 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>				
			<ul><li>1.3.171.1.1.10.3.33,</li><li>1.3.171.1.1.10.3.21,</li></ul>				
			o 1.3.171.1.1.10.3.23, o 1.3.171.1.1.10.3.25				
1.32	CSP Board	16/11/2020	Update OI definition				



## **Table of content**

DOCUME	NT INFORMATION	2
VERSION	HISTORY	2
TABLE O	F CONTENT	4
INTELLEC	CTUAL PROPERTY RIGHTS	7
REFEREN	ICES	8
INTRODU	CTION	9
1.1	THE LUXTRUST PROJECT	9
1.2	GOAL OF THE LUXTRUST PKI	
1.3	LuxTrust PKI Hierarchy	
LUXTRUS	T CERTIFICATION AUTHORITIES	10
1.4	Two-level CA hierarchy	10
CERTIFIC	ATE AND CRL PROFILES	12
1.5	CERTIFICATE TYPES	12
1.6	LuxTrust Certification Authorities – Certificates profiles	23
1.7	LUXTRUST GLOBAL ROOT CA	23
1.8	LuxTrust Global Qualified CA	24
1.9	LuxTrust SSL CA	25
1.10	LUXTRUST TSA (TIMESTAMPING) CA	27
1.11	LUXTRUST CORPORATE CA	28
1.11.1	Certificate extensions	29
1.11.2	Algorithm object identifiers	29
1.11.3	Name forms	30
1.11.4	Name constraints	30
1.11.5	Certificate policy object identifier	30
1.11.6	Usage of Policy Constraints extension	30
1.11.7	Policy qualifiers syntax and semantics	30
1.12	LuxTrust End-entity – Certificates profiles	
1.12.1	Certificate profiles	30
1.12.2	Version number(s)	31
1.12.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	31
1.12.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	33
1.12.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	35
1.12.6	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	
1.12.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	
1.12.8	LuxTrust NCP+ Certificates supporting Mass Signature Services	
1.12.9	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures	
1.12.10	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption	
1.12.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration 46	n purposes
1.12.12	LuxTrust Smartcard LORA Certificates supporting Signature for LRAO purposes	48
1.12.13	LuxTrust Smartcard LORA Certificates supporting Authentication & Encryption for LRAO purposes	50
1 12 11	LuxTrust non SSCD Mass LPAO OCP Cartificates supporting Advanced Flectronic Signatures	51



1.12.15	Lux rust eld SSCD QCP+ Certificates supporting Qualified Signatures	54
1.12.16	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption	56
1.12.17	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures	57
1.12.18	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption	59
1.12.19	LuxTrust NCP+ Certificates supporting SEAL Signature Services	61
1.12.20	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & 63	Encryption
1.12.21	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Author	
1.12.22	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Author	
1.12.23	LuxTrust Object (or Code) Signing Certificates	74
1.12.24	LuxTrust SSL/TLS Certificate for Client Authentication	76
1.12.25	SSL/TLS QCP-w Extended Validation Server Certificates	78
1.12.26	Wildcard - LCP certificates supporting Signature, Authentication & Encryption	
1.12.27	LuxTrust SPARE Signing Server LCP Certificate Profile	
1.12.28	LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature	87
1.12.29	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	90
1.12.30	LuxTrust Advanced eSEAL - Certificate Profile supporting digital signature	91
1.12.31	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication	93
1.12.32	LuxTrust Advanced Automated eSEAL Certificate Profile supporting digital signature	96
1.12.33	LuxTrust Smart Card QCP-n-qscd Certificate Profile	98
1.12.34	LuxTrust Smart Card NCP+ Certificate Profile	100
1.12.35	LuxTrust Smart Card LORA NCP+ supporting Qualified Electronic Signature	102
1.12.36	LuxTrust Smart Card LORA NCP+-qscd supporting Authentication & Encryption for for LRAO Purposes	104
1.12.37	QCP-n-qscd supporting Qualified Electronic Signature for eID smart cards	105
1.12.38	NCP+ supporting Authentication & Encryption for eID smart cards	107
1.12.39	LuxTrust Signing Server QCP-n-qscd Certificate Profile	108
1.12.40	LuxTrust Signing Server QCP-I-qscd Certificate Profile	110
1.12.41	LuxTrust Signing Stick QCP-n-qscd certificate profile	112
1.12.42	LuxTrust Signing Stick NCP+ Certificate Profile	114
1.12.43	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	116
1.12.44	LuxTrust Corporate LCP Certificate Profile	119
1.13	TIMESTAMPING CERTIFICATE PROFILE	123
1.13.1	Normalized Certificate Policy for LuxTrust Qualified Timestamping	124
1.13.2	Qualified Timestamping Certificate Profile	126
1.13.3	TimeStamp Request and Response Format	127
1.14	CERTIFICATE EXTENSIONS	128
1.15	ALGORITHM OBJECT IDENTIFIERS	129
1.16	NAME FORMS	129
1.17	NAME CONSTRAINTS	129
1.18	CERTIFICATE POLICY OBJECT IDENTIFIER	129
1.19	Usage of Policy Constraints extension	129
1.20	POLICY QUALIFIERS SYNTAX AND SEMANTICS	129
1.21	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES	129
1.22	CRL PROFILE	129
1.22.1	Version number(s)	131
1.22.2	CRL entry extensions	131
1.23	OCSP PROFILE.	131





1.23.1	Version number(s)	131
1.23.2	OCSP extensions	131
1 24	INTEGRATION CERTIFICATES	132

VERSION 1.32



## **Intellectual Property Rights**

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



## References

- [1] The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [2] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
- [3] ETSLTS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- [4] ETSITS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- [5] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- [6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 1 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] elDAS regulation: Regulation (EU) No 910/2014



### INTRODUCTION

### 1.1The LuxTrust project

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

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

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

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

#### 1.2 Goal of the LuxTrust PKI

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

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

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

### 1.3 LuxTrust PKI Hierarchy

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

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

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



### **LuxTrust Certification Authorities**

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

### 1.4 Two-level CA hierarchy

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

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

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

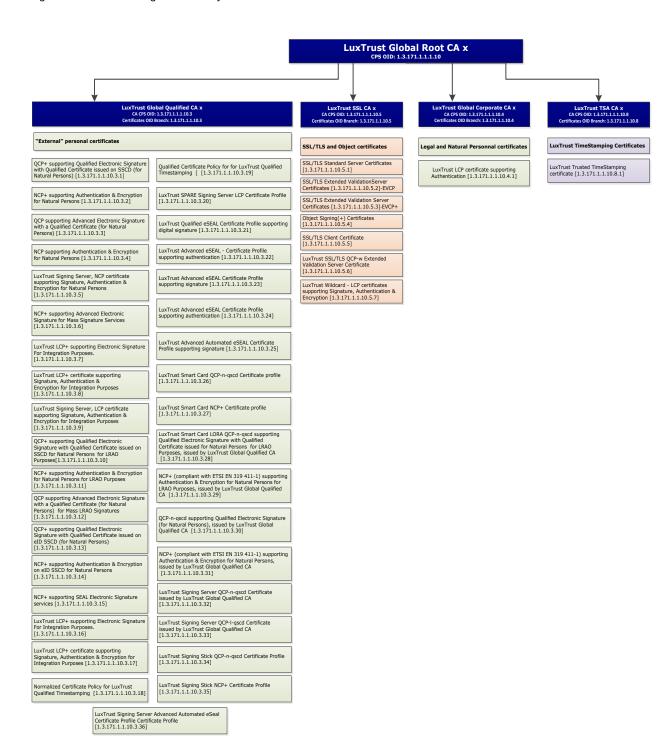
Subordinate CAs are operating within a grant of authority for issuing certificates under the LuxTrust CPS and the applicable CP. This grant has been provided by the "LuxTrust Global Root CA" (hereafter "LTGRCA") under the responsibility and authority of LuxTrust S.A. acting as CSP.

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

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



Figure 1- LuxTrust running CA Hierarchy





## **CERTIFICATE AND CRL PROFILES**

## 1.5 Certificate types

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

CP identification	CP OID	CPS OID	Short Description	Ref.		
LuxTrust Qualified 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	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption		
			Certification Service Providers.			
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		



CP identification	CP OID	CPS OID	Short Description	Ref.
NCP+ supporting Advanced Electronic Mass Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Mass Signature Services.	LuxTrust NCP+ Certificates supporting Mass Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.7	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.8	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 2048-bit key size and three (3) years, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+authentication and encryption certificates.	LuxTrust SSCD LCP+ Integration Certificates supporting Authentication & Encryption
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.9	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for INTEGRATION PURPOSES.	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integration purposes
QCP+ 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



CP identification	CP OID	CPS OID	Short Description	Ref.
QCP+ supporting Qualified Electronic Signature (for Natural Persons) issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.13	1.3.171.1.1.1.10.3	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	LuxTrust eID SSCD QCP+ Certificates supporting Qualified Signatures
NCP+ supporting Authentication & Encryption for Natural Persons issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.14	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature) and key & data encryption.	LuxTrust eID SSCD NCP+ Certificates supporting Authentication & Encryption
NCP+ Advanced Electronic Seal Signature Services issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.15	1.3.171.1.1.1.10.3	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Seal Signature Services.	LuxTrust NCP+ Certificates supporting SEAL Signature Services
LCP for INTEGRATION certificates LCP compliant certificates supporting integration Electronic Signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.16	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of electronic signature for INTEGRATION purposes of QCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Electronic Signatures
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	1.3.171.1.1.1.10.3	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by the CSP, 2048 bit key size and one (1) year validity, and with a key usage limited to the support of authentication (to the exclusion of electronic signature) and key & data encryption for INTEGRATION purposes of NCP+ signature certificates.	LuxTrust eID SSCD LCP+ Certificates supporting Authentication & Encryption
Normalized Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.18	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Normalized Certificate Policy for Qualified Timestamping
Qualified Certificate Policy for Qualified Timestamping issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.19	1.3.171.1.1.1.10.3	EN 319 421 compliant.	Qualified Certificate Policy for Qualified Timestamping
LuxTrust SPARE Signing Server LCP Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.20	1.3.171.1.1.1.10.3	LuxTrust SPARE Certificate not on SSCD compliant with ETSLTS 102 042 LCP cert.policy.	SPARE Signing Server LCP Certificate Profile
LuxTrust Qualified eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.21	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy.	Qualified eSEAL Certificate Profile supporting digital signature



CP identification	CP OID	CPS OID	Short Description	Ref.
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 Certificate Profile supporting authentication
LuxTrust Advanced eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.23	1.3.171.1.1.1.10.3	Advanced eSEAL.  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	1.3.171.1.1.10.3	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,



CP identification	CP OID	CPS OID	Short Description	Ref.		
QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.30	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 QCP-n-qscd certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and sixty-one (61) months validity, and with a key usage limited to the support of qualified electronic signature.	QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons),		
NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.31	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose.	NCP+ (compliant with ETSI EN 319 411-1) supporting Authentication & Encryption for Natural Persons,		
LuxTrust Signing Server QCP-n- qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.32	1.3.171.1.1.1.10.3	Signing Server certificate for qualified signature	LuxTrust Signing Server QCP-n-qscd Certificate profile		
LuxTrust Signing Server QCP-I- qscd Certificate issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.33	1.3.171.1.1.1.10.3	Signing Server certificate for qualified eSeal	LuxTrust Signing Server QCP-I-qscd Certificate profile		
LuxTrust Signing Stick QCP-n-qscd Certificate Profile	1.3.171.1.1.10.3.34	1.3.171.1.1.1.10.3	Signing Stick QCP-n-qscd Certificate Profile	Signing Stick QCP-n-qscd Certificate Profile		
LuxTrust Signing Stick NCP+ Certificate Profile	1.3.171.1.1.10.3.35	1.3.171.1.1.1.10.3	Signing Stick NCP+ Certificate Profile	Signing Stick NCP+ Certificate Profile		
LuxTrust Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	1.3.171.1.1.10.3.36	1.3.171.1.1.1.10.3	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile Certificate Profile		
	LuxTrust SSL Certification Authority					
SSL/TLS Standard Server Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	1.3.171.1.1.1.10.5	ETSI TS 102 042 <b>LCP</b> compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption		



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





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

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

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

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

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

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

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

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



VERSION 1.32

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

Domain	Document category	Document		Sub-document – description	LuxTrust Product	Version	Sub-version	Complete OID	ETSI OID
1 LuxTrust	LuxTrust Certif Statements	ication Practice							
PKI	1 CPS LuxTrust	1 CPS Summary GTE/Verizon Chain	О			x	у	1.3.171.1 <b>.1.1.0.x.y</b>	N/A
		<b>2</b> Not Used		Not Used		-	-	not used	N/A
		10 CPS LuxTrust		LuxTrust Global Root CA		-	-	1.3.171.1 <b>.1.1.10</b>	N/A
		Global Root Chain	3	LuxTrust Global Qualified CA		-	-	1.3.171.1 <b>.1.1.10.3</b>	N/A
			5	LuxTrust SSL CA		-	-	1.3.171.1. <b>1.1.10.5</b>	N/A
			8	LuxTrust Global Timestamping CA		-	-	1.3.171.1. <b>1.1.10.8</b>	N/A
1 LuxTrust	LuxTrust Certi	ficate Policies							
PKI	10 CP's LuxTrust Global Chain	LuxTrust LuxTrust Global	1	QCP+ supporting Advanced Electronic Signature with Qualified Certificate issued on SSCD (for Natural Persons)	SmartCard PRI/PRO Signature Certificate	-	-	1.3.171.1. <b>1.10.3.1</b>	0.4.0.1456.1.1
		Certificates	2	NCP+ supporting Authentication & Encryption for Natural Persons	SmartCard PRI/PRO Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.2</b>	0.4.0.2042.1.2
			3	QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons)	Signing Stick PRI/PRO Signature Certificate	-	-	1.3.171.1. <b>1.10.3.3</b>	0.4.0.1456.1.2
			4	NCP Authentication & Encryption	Signing Stick PRI/PRO Authentication Certificate	-	-	1.3.171.1. <b>1.10.3.4</b>	0.4.0.2042.1.1
			5	NCP Authentication, Encryption & Signature [LuxTrust Signing Server]	Signing Server Certificate	-	-	1.3.171.1 <b>.1.10.3.5</b>	0.4.0.2042.1.1
			6	NCP+ supporting AdES for Mass Signature Services	Mass Signature Service signature Certificate	-	-	1.3.171.1. <b>1.10.3.6</b>	0.4.0.2042.1.1



VERSION 1.32

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



VERSION 1.32

	23	LuxTrust Advanced eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1 <b>.1.10.3.23</b>	0.4.0.2042.1.2	
	24	LuxTrust Advanced eSEAL Certificate supporting authentication	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.24</b>	0.4.0.2042.1.2	
	25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.25</b>	0.4.0.2042.1.2	
	26	Lux Trust Coast Coast OCD a good Coatificate Dusfile	SmartCard PRI/PRO			1.3.171.1 <b>.1.10.3.26</b>	0.4.0.404440.4.0	
	20	LuxTrust Smart Card QCP-n-qscd Certificate Profile	Signature Certificate	]	-	1.3.171.1.1.10.3.26	0.4.0.194112.1.2	
	0.7	Las Taras Caras None Caras None Caras Par Cla	SmartCard PRI/PRO			4 0 474 4 4 40 0 07	0.4.0.0040.4.0	
	27	LuxTrust Smart Card NCP+ Certificate Profile	Authentication Certificate	-	-	1.3.171.1 <b>.1.10.3.27</b>	0.4.0.2042.1.2	
	28	LuxTrust Smart Card LORA NCP+ - Signature	SmartCard LORA			4 2 474 4 4 40 2 20		
	20	Certificate for LRAO Purposes	Signature Certificate	-	-	1.3.171.1 <b>.1.10.3.28</b>		
		LuxTrust Smart Card LORA NCP+ - authentication	SmartCard LORA					
	29	Certificate for LRAO Purposes	Authentication Certificate	-	-	1.3.171.1 <b>.1.10.3.29</b>	0.4.0.2042.1.2	
	30	LuxTrust elD Smart Card QCP-n-qscd Certificate	eID SmartCard			1.3.171.1 <b>.1.10.3.30</b>	0.4.0.194112.1.2	
	30	Luxitust eib Smart Card QCF-II-qscd Certificate	Signature Certificate	-	-	1.3.171.1.11.10.3.30	0.4.0.194112.1.2	
	-	Las Translat D. Ossarla and NOD. Ossillant	eID SmartCard			1.3.171.1. <b>1.10.3.31</b>	0.4.0.2042.4.2	
	31	LuxTrust eID Smart card NCP+ Certificate	Authentication Certificate	]-	-	1.3.171.1.1.10.3.31	0.4.0.2042.1.2	
	32	LuxTrust Signing Server QCP-n-qscd Certificate	Signing Server certificate for qualified signature	-	-	1.3.171.1. <b>1.10.3.32</b>	0.4.0.194112.1.2	
	33	LuxTrust Signing Server QCP-I-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1. <b>1.10.3.33</b>	0.4.0.194112.1.3	
	34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171. <b>1.1.10.3.34</b>	0.4.0.194112.1.2	
	35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171. <b>1.1.10.3.35</b>	0.4.0.2042.1.2	
	36	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile			1.3.171.1.1.10.3.36	0.4.0.2042.1.3	
5 LuxTrust SSL CA	1	SSL/TLS Standard Server Certificates	SSL/TLS Standard Server Certificates	-	-	1.3.171.1 <b>.1.10.5.1</b>	0.4.0.2042.1.3	
Certificates	2	SSL/TLS(+) Extended Validation Server Certificates – EVCP	SSL/TLS Extended Validation Server Certificates	-	-	1.3.171.1. <b>1.10.5.2</b>	0.4.0.2042.1.4	



	0		I = 1.3	
vrr		ルフハ	11.5	/

	3	SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	-	-	1.3.171.1. <b>1.10.5.3</b>	0.4.0.2042.1.5
	4	Object Signing(+) Certificates	Object Signing(+) Certificates	-	-	1.3.171.1. <b>1.10.5.4</b>	0.4.0.2042.1.3
	5	SSL/TLS Client Certificate	SSL/TLS Client Certificate	-	-	1.3.171.1. <b>1.10.5.5</b>	0.4.0.2042.1.3
	6	SSL/TLS QCP-w Extended Validation Server Certificates	SSL/TLS Qualified website authentication certificate	-	-	1.3.171.1. <b>1.10.5.6</b>	0.4.0.194112.1.4
,	7	LuxTrust SSL Server LCP Certificate Profile -Wildcard	SSL Server LCP Wildcard Certificate Profile			1.3.171.1. <b>1.10.5.7</b>	0.4.0.2042.1.7
8 LuxTrust Global Timestamping CA Certificates	1	LuxTrust Trusted TimeStamping certificate	LuxTrust Trusted TimeStamping certificate	-	-	1.3.171.1 <b>.1.10.8.1</b>	0.4.0.2042.1.3
4 LuxTrust Corporate CA	1	LuxTrust Corporate LCP Certificate Profile	LCP Corporate Certificate used for authentication purposes	-	-	1.3.171.1.1. <b>10.4.1</b>	0.4.0.2042.1.3



## 1.6LuxTrust Certification Authorities - Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

## 1.7LuxTrust Global Root CA

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



	Lu	xTrust Gl	obal Root	CA	
Base Profile	OID	Include d	Critical	Value	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyldentifie r	{id-ce 35}	Х	FALSE		
Keyldentifier		X		SHA-1 Hash	
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE⁴		
CA		Х		TRUE	Fixed
pathLenConstraint		Х		None	Fixed

## 1.8LuxTrust Global Qualified CA

	Lux	Trust Glob	al Qualifie	ed CA	
Base Profile	OID	Include d	Critical	Value	
Version		Х		V3	
SerialNumber		Х		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed
SignatureValue		Х		Issuing LTGRCA Signature	
Validity					
NotBefore		Х		Key Generation Process Date/Time	
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed
SubjectPublicKeyInf o		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).  20 years certificate requires a 4096 key length.	
Issuer					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Qualified CA x1	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	



	Lu	xTrust Glob	al Qualifie	ed CA	
Base Profile	OID	Include d	Critical	Value	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	Х	TRUE <sup>4</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyldentifie r	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		Х		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx1.crt	Fixed
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Subject public key	
cRLDistributionPoin ts	{id-ce 31}	Х	FALSE		
distributionPoint					
FullName		Х		http://crl.luxtrust.lu/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

		LuxTru	st SSL C	A	
Base Profile	Included	Critical	Value		
Version		X		V3	
SerialNumber		Х		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed
SignatureValue		Х		Issuing LTGRCA Signature	
Validity					
NotBefore		Х		Key Generation Process Date/Time	

 $<sup>^{3}</sup>$  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			
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed		
SubjectPublicKeyInfo		×		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).  20 years certificate requires a 4096 key length.			
Issuer							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	Х		LU	Fixed		
CommonName	{ id-at-3 }			LuxTrust SSL CA x <sup>1</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
CertificatePolicies	{id-ce 32}	Х	FALSE				
policyldentifier (1)		Х		1.3.171.1.1.1.10.5	Fixed		
policyQualifiers (1)				N/a			
policyQualifierId (1)	{ id-qt-1 }	Х		CPS	Fixed		
Qualifier (1)		Х		https://repository.luxtrust.lu	Fixed		
policyldentifier (2)	{ anyPolicy }	Х		2.5.29.32.0	Fixed		
policyQualifiers (2)				N/a			
policyQualifierId (2)							
Qualifier (2)							
KeyUsage	{id-ce 15}	Х	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> AccessMethod	{id-pe 1} {Id-ad-1}		False				
accessLocation		Х		http://ltgroot.ocsp.luxtrust.lu	Fixed		
AccessMethod accessLocation	{Id-ad-2}	x	False	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		

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



LuxTrust SSL CA								
Base Profile OID Included Critical Value								
BasicConstraints	{id-ce 19}	X	TRUE⁴	N/a				
CA		X		TRUE	Fixed			
pathLenConstraint		X		0 (Zero)	Fixed			

## 1.10 LuxTrust TSA (Timestamping) CA

LuxTrust Global Timestamping CA								
Base Profile	OID	Included	Critical	Value				
Version		Х		V3				
SerialNumber		Х		As provided by CA or by LuxTrust S.A.				
SignatureAlgorithm								
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed			
SignatureValue		Х		Issuing LTGRCA Signature				
Validity								
NotBefore		Х		Key Generation Process Date/Time				
NotAfter		Х		Key Generation Process Date/Time +up to 20 years	Fixed			
SubjectPublicKeyInfo		Х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). 20 years certificate requires a 4096 key length.				
Issuer								
CountryName	{ id-at-6 }	Х		LU	Fixed			
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x1	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
Subject								
CountryName	{ id-at-6 }	Х		LU	Fixed			
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA x <sup>1</sup>	Fixed			
organizationName		Х		LuxTrust S.A.	Fixed			
CertificatePolicies	{id-ce 32}	Х	FALSE					
policyldentifier		Х		1.3.171.1.1.10.8	Fixed			
policyQualifiers				N/a				
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed			
Qualifier		Х		https://repository.luxtrust.lu	Fixed			
KeyUsage	{id-ce 15}	Х	TRUE <sup>4</sup>					
keyCertSign				Set	Fixed			
crlSign				Set	Fixed			
authorityKeyldentifier	{id-ce 35}	Х	FALSE					



	LuxTru	st Global 1	imestamp	oing CA	
Base Profile	OID	Included	Critical	Value	
Keyldentifier		X		SHA-1 Hash of Authority public key	
authorityInfoAccess6	{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/LTGRCA1.crl	Fixed
Basic Constraints	{id-ce 19}	Х	TRUE⁴	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

## 1.11 LuxTrust Corporate CA

	LuxTrust Corporate CA									
Base Profile	OID	Included	Critical	Value						
Version		Х		V3						
SerialNumber		Х		Random CSN						
SignatureAlgorithm										
Algorithm	1.2.840.113549.1.1.11	Х		SHA256 with RSA Encryption	Fixed					
SignatureValue		х		Issuing LTGRCA2 Signature						
Validity										
NotBefore		Х		Key Generation Process Date/Time						
NotAfter		Х		Key Generation Process Date/Time +up	Fixed					
				to 20 years						
				Public Key: Key length: 2048 up to 4096						
Out to a Dutalla Kanda fa				bits (RSA); public exponent: Fermat-4						
SubjectPublicKeyInfo		X		(=010001).						
				20 years certificate requires a 4096 key						
				length.						
Issuer										
CountryName	{ id-at-6 }	Х		LU	Fixed					
CommonName	{ id-at-3 }	Х		LuxTrust Global Root 2	Fixed					

 $<sup>^{6}</sup>$  Since LuxTrust Global Timestamping CA 2



		LuxTrust Co	orporate	: CA	
Base Profile	OID	Included	Critical	Value	
organizationName		Х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	Х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Corporate CA x	Fixed
organizationName		Х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	Х	FALSE		
policyldentifier		х		1.3.171.1.1.1.10.4	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	Х		CPS	Fixed
Qualifier	CPSuri	Х		https://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	Х	TRUE⁴		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Authority public key	
authorityInfoAccess	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		х		http://ca.luxtrust.lu/LTGRCA2.crt	Fixed
subjectKeyldentifier	{id-ce 14}	Х	FALSE		
Keyldentifier		Х		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	Х	FALSE		
distributionPoint					
FullName		Х		http://crl.luxtrust.lu/LTGRCA2.crl	Fixed
BasicConstraints	{id-ce 19}	Х	TRUE	N/A	
CA		Х		TRUE	Fixed
pathLenConstraint		Х		0 (Zero)	Fixed

### 1.11.1 Certificate extensions

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

## 1.11.2 Algorithm object identifiers

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

VERSION 1.32



#### 1.11.3 Name forms

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

#### 1.11.4 Name constraints

Name constraints are supported as per RFC 5280.

#### 1.11.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

### 1.11.6 Usage of Policy Constraints extension

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

### 1.11.7 Policy qualifiers syntax and semantics

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

### 1.12 LuxTrust End-entity - Certificates profiles

#### 1.12.1 Certificate profiles

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

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

- LuxTrust SSCD Smartcards: These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP+<sup>7</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>8</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 1.3.171.1.10.3.26.
- LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.10.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1]
  (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP<sup>7</sup> Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.10.3.3, and
  - One LuxTrust NCP<sup>8</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>8</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 1.3.171.1.10.3.22

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

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

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:

\_

 $<sup>^{7}</sup>$  As defined by ETSI TS 101 456 (cf. [3]).

<sup>&</sup>lt;sup>8</sup> As defined in ETSI TS 102 042 (cf. [4]).





- 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 1.3.171.1.10.5.4.
- 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.

#### 1.12.2 Version number(s)

X.509 v3 is supported and used.

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

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

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

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

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

	LuxTrust SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg		✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	lue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>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	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.				

<sup>&</sup>lt;sup>9</sup> IN = Included: Attribute / field included within the certificate profile.

<sup>11</sup> O/M: O = Optional, M = Mandatory.

 $<sup>^{10}</sup>$  CE = Critical Extension.

 $<sup>^{12}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	Lux1	Trust SS	CD QC	P+ Cert	ificate	Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	givenName	<b>√</b>		M	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	<b>~</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		М	D	PRO products only: Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	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
subjectPubli		✓	False			
	Algorithm	✓ ✓				Public Key: Key length: 2048bit (RSA); public
Extensions	subjectPublicKey	<b>V</b>		M		exponent: Fermat-4 (=010001).
Authority						
Properties	1.1					
authorityKey	ldentifier keyldentifier	√ √	False			SHA-1 Hash of the LuxTrust Global
authoritulet-	Acces	<b>√</b>	Eoloo			Qualified CA public key
authorityInfo	AccessMethod	<b>✓</b>	False			Id-ad-2
	accessLocation	<i>√</i>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistribut		<b>√</b>	False			
	distributionPoint fullName	✓ ✓			S	http://crl.luxtrust.lu/LTGQCAx.crl
Subject	TUITIVATTIE	<b>V</b>				http://ch.iuxtrust.iu/ΕΤΘQCAX.CH
Properties						
subjectAltNa		<b>√</b>	False			
auhicat/ard	Rfc822Name	✓ ✓	Folse	0	D	Certificate Holder's email address
subjectKeylo	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 or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).

<sup>13</sup> SINCE LTGQCA3



	LuxTrust SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	False				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.1				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>~</b>				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Support of Qualified Electronic Signature.				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCer	tificateStat									
	QcCompliance	✓		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]				
	QcSSCD	✓		М	D	0.4.0.1862.1.4				

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

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

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

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

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

	LuxTrust SSCD NCP+ Certificate Profile								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	gorithm	✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVa	lue	✓	False						
					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x			
	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			



	Lux	Trust S	SSCD N	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>9</sup>	<b>CE</b> <sup>10</sup>	O/M <sup>11</sup>	<b>CO</b> <sup>12</sup>	Value
	commonName	<b>~</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	<b>~</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>~</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>√</b>		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnitName 1	<b>√</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à:" & (Date of birth + 18 years).
	organizationalUnitName 2	<b>√</b>		0	D	PRO products only: Company/institution department or other information item
subjectPubli		<b>√</b>	False			Public Koya Koyalongth: 2040 hit /DCA); and I'm
	algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	dentifier	✓	False			
	keyldentifier	✓				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.crt
	AccessMethod	✓				ld-ad-1
*DI D! - (-!)	accessLocation	<b>√</b>	F-!			http://qca.ocsp.luxtrust.lu/13
cRLDistribut	ionPoint distributionPoint	✓ ✓	False		S	
	fullName	✓			j	http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltNa	me Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False		_ U	Gerundate Fiologi S erriali dudress
					•	



	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field				
						with a 0100 value, followed by the least				
						significant 60 bits of the SHA-1 hash of the				
						value or subjectPublicKey bit string (tag, not				
						including the length and number of unused				
Policy						bit-string bits).				
Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	True				
	nonRepudiation				S	False				
	keyEncipherment	✓			S	True				
	dataEncipherment	✓			S	True				
certificatePo		✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.2				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	✓				LuxTrust Certificate on SSCD compliant with				
						ETSITS 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				
	Policyldentifier	•				0.4.0.2042.1.2				

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

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

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

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

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

LuxTrust non SSCD QCP Certificate Profile								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</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	✓			S	LuxTrust Global Qualified CA x		
	organizationName	✓			S	LuxTrust S.A.		



LuxTrust non SSCD QCP Certificate Profile								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value		
Validity		✓	False					
	NotBefore	✓			D	Certificate generation process date/time.		
	NotAfter	✓			D	Certificate generation process date/time + 36 Months		
Subject		✓	False					
	serialNumber	✓		М	D	Serial Number as constructed by LRAO		
	commonName	<b>√</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character		
	givenName	>		М	D	<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	<b>✓</b>		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	✓		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.		
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)		
	organizationalUnitName 1	<b>√</b>		M for PRO prod., conditional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)  PRIVATE products:  If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).		
	organizationalUnitName 2	<b>✓</b>		0	D	PRO products only:  Company/institution department or other information item		
subjectPublicKeyInfo		✓	False					
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public		
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).		
Extensions								
Authority Properties								
authorityKeyldentifier		<b>✓</b>	False					
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key		
authorityInfoAccess		<b>✓</b>	False					
	AccessMethod	<b>√</b>				ld-ad-2		
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt		



A contract						cate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistrib	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Pro	operties					
subjectAltI	Name	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	/Identifier	✓	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value of 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
certificateF	Policies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.3
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	<b>✓</b>				LuxTrust Qualified Certificate not on SSCI compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert
	Policyldentifier	<b>√</b>				0.4.0.1456.1.2
QualifiedC	ertificateStat					
	QcCompliance	✓		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance wit [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance wit [3]
	QcSSCD	✓				NOT SET

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

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

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

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





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

	LuxTrus	t non	SSCDN	ICP Cert	ificate	Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base						
Profile						
Version	T	✓	False		_	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
SerialNumbe	l ar	<b>√</b>	False		S	Version 3 Value = "2"
Serialivullibe	ਸ਼ 	•	i aise		FDV	Validated on duplicates.
signatureAlg	orithm	✓	False		151	validated on adplicates.
<b>J</b>	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVal	lue	✓	False			
icour		<b>√</b>	Folso		D S	Issuing CA Signature.
issuer	countryName	<b>∨</b>	False		S	LU
	commonName	· /			S	LuxTrust Global Qualified CA x
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
		,	-			36 Months
subject	T	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>✓</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>✓</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<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
subjectPubli	ckeyInto	✓	False			



Extensions   Authority   Properties   Authority   Properties   Authority   Properties   Authority   Properties   Authority   Properties   Authority   Access   Authority   Access   A		LuxTr	ust non S			tificate	Profile
Extensions	Attribute		IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Extensions		algorithm	✓				Public Key: Key length: 2048 bit (RSA);
Extensions   Authority   Properties   authorityKeyldentifier			✓		М		
Authority   Properties   authorityKeyldentifier	Extensions						, ,
authorityKeyldentifier							
authorityKeyldentifier	Properties						
Reyldentifier	authorityKey	dentifier	✓	False			
authorityInfoAccess			✓				SHA-1 Hash of the LuxTrust Qualified CA
AccessMethod   V							public key
AccessMethod   V	authorityInfo	Access	✓	False			
AccessMethod			✓				ld-ad-2
AccessMethod		accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt
CRLDistributionPoint		AccessMethod	<b>√</b>				
CRLDistributionPoint		accessLocation	✓				http://gca.ocen.luxtrust.lu/13
distributionPoint	cPI Dietribut			False			πιφ.// γοα. ο ο ο ρ. ια λτι α ο τ. ια/
Subject   Subj	CVEDISHIBIN			1 alse		9	
Subject Properties SubjectAltName    Rfc822Name						3	http://orl.luxtrust.lu/LTGQCAx.orl
Properties   SubjectAitName   V   False   Rfc822Name   V   False   Rfc822Name   V   False   SubjectKeyldentifier   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   ReyUsage   V   True   S   True	Subject	lulinalile	<b>V</b>				http://ch.iuxtrust.iu/LTGQCAX.ch
SubjectAltName							
Rfc822Name		l mo		Folco			
SubjectKeyIdentifier   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   V   True	SubjectAlliva			i aise	0		Cartificate Holder's email address
Reyldentifier   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	subject/out			Foloo	0	U	Certificate Holder's erriali address
Policy   P	Subjectkeyid			raise		Fived	The Key Identifier commisses a four hit
Policy   Properties		,					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
digitalSignature							¥ /
digitalSignature			✓	True			
ReyEncipherment   V		digitalSignature	<b>√</b>			S	True
CertificatePolicies   V False     1.3.171.1.1.10.3.4		nonRepudiation				S	False
CertificatePolicies   ✓ False		keyEncipherment	<b>~</b>			S	True
PolicyIdentifier		dataEncipherment	<b>√</b>			S	True
PolicyIdentifier	certificatePo	licies	✓	False			
policyQualifierID ✓ S Id-qt-1 (CPS) qualifier ✓ S https://repository.luxtrust.lu policyQualifierID ✓ S Id-qt-2 (User Notice) noticeNumbers  DisplayText ✓ LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity Authentication and Data Encryption.			✓				1.3.171.1.1.10.3.4
qualifier     ✓     S     https://repository.luxtrust.lu       policyQualifierID     ✓     S     Id-qt-2 (User Notice)       noticeNumbers     LuxTrust     Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP.       Sole Authorised Usage: Data or Entity Authentication and Data Encryption.			✓			S	
policyQualifierID ✓ S Id-qt-2 (User Notice) noticeNumbers  DisplayText ✓ LuxTrust Certificate not on SSCD compliant with ETSL TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity Authentication and Data Encryption.			✓				https://repository.luxtrust.lu
noticeNumbers  DisplayText  ✓  LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity Authentication and Data Encryption.			✓				
DisplayText  ✓  LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity Authentication and Data Encryption.							
Policyldentifier ✓		DisplayText					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.
0.7.0.Z07Z.1.1		Policyldentifier	✓				0.4.0.2042.1.1

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

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

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

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

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



	LuxTrust S	igning	Serve	r NCP C	ertifica	te Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base						
Profile						
Version	I	✓	False		S	Version 3 Value = "2"
SerialNumbe	er er	<b>✓</b>	False		5	Version 3 value = 2
Ochamanibe			1 alsc		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
						OID = 1.2.840.113549.11.11
signatureVal	lue	✓	False			OTIAZOO WIIT NOA ETICIYEUOTI.
					D	Issuing CA Signature.
Issuer	T	✓	False		S	
	countryName	<b>√</b>			S	LU
	commonName organizationName	✓ ✓			S	LuxTrust Global Qualified CA x LuxTrust S.A.
Validity	organizationname	<b>▼</b>	False		3	Lux Trust S.A.
validity	NotBefore	<b>√</b>	1 0.00		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time +
						36 Months
subject		✓	False			
	serialNumber	✓	<u>L</u>	М	D	Serial Number as constructed by LRAO
						PRO and PRIVATE products:
	commonName	<b>✓</b>		М	D	Concatenation of given name(s) and
	Commonwante	•		IVI	D	surname(s) as on ID card separated by a
						"Space" character
	niven Name	<b>✓</b>			2	PRO and PRIVATE products: Given
	givenName	•		М	D	name(s) as on ID card
						PRO and PRIVATE products:
		<b>✓</b>		N4	_	Surname(s) as on ID card without
	surname	•		М	D	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
						•
						PRIVATE products:
						Fixed value: "Private Person"
	41410	<b>✓</b>			_	PRO products:
	title	•		М	D	"Professional Person" (default) or
						"Professional Administrator"
						(Other titles possible for special purpose
			<u> </u>			certificates)
						PRO products only:
	organizationName	✓		М	D	Name of company/institution as in articles
						of association or equivalent documents,
						including the legal form.
					_	PRO products only: Company/institution
	localityName	✓		M	D	country of HQ (as in articles of association)
			<u> </u>			assuciation)
				M for		PRO products:
				PRO		Company/Institution VAT number (or if no
				prod., condi-		VAT number available, other unique
	organizationalUnitName 1	<b>✓</b>		tional	D	national company/institution identifier)
				(O) for		PRIVATE products:
				PRIV		If the holder is underage: "Mineur jusqu'à
				prod.)		: " & (Date of birth + 18 years).
						PRO products only:
					-	1
	organizationalUnitName 2	✓		0	D	Company/institution department or other
	organizationalUnitName 2	<b>✓</b>		0	D	Company/institution department or other information item
subjectPubli		✓ ✓ ✓	False	O	D	



	LuxTrus	st Signing	y Serve	r NCP C	ertifica	te Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	subjectPublicKey	✓		М		Public Key: Key length: 2048 bit (RSA) up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey		✓	False			
	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/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/13
cRLDistribut	ionPoint	✓	False			
J. 122 1011 1041	distributionPoint	· ·	7 4.00		S	
	fullName	<b>/</b>				http://crl.luxtrust.lu/LTGQCA.crl
Subject	Tumtume					TREP.//OFFICIAL GOLIGIE FOR GOVERN
Properties						
subjectAltNa	ime	<b>√</b>	False			
oubjoot, and	Rfc822Name	<b>-</b>	1 0.00	0	D	Certificate Holder's email address
subjectKeylo		✓	False			
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation				S	True
	keyEncipherment	<b>~</b>			S	True
	dataEncipherment	<b>√</b>			S	True
certificatePo	licies	✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.5
	policyQualifierID	<b>✓</b>			S	Id-qt-1 (CPS)
	qualifier	<b>✓</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	noticeNumbers	1			† Ť	- 1 - (
	DisplayText	<b>√</b>				LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Signature, Data or Entity Authentication and Data
						Encryption.

## 1.12.8 LuxTrust NCP+ Certificates supporting Mass Signature Services

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

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

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

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>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False		_	
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
g	algorithm		. 4.00		S	OID = "1.2.840.113549.1.1.11" -
	a.go					SHA256 with RSA Encryption
signatureValue		✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	recurring of Congruence
100001	countryName	<b>✓</b>	1 0100		S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity	organization value	✓ ·	False			Edititude C.7 t.
validity	NotBefore	<b>V</b>	1 0100		D	Certificate generation process
	NotBelore					date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process
		'				date/time + 36 Months
subject	1	<b>✓</b>	False			date/time i dd iviontiis
Junject			1 0135			
	commonName	✓		М	D	Name commonly used by the subject to represent itself as stated in ETSI TS 119 412-3, the name should not be domain-shaped
	countryName	<b>✓</b>		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	✓		0	D	As provided by Subscriber
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
<b>Authority Properties</b>						
authorityKeyldentifier		✓	False			
	keyldentifier	<b>V</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/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistributionPoint	1	<b>✓</b>	False			
JALDION DUNON ONL	distributionPoint	· /	1 4130		S	
	fullName	· /				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties	Tullituille					mip.//GIT.iuxtruət.iu/ETGQGAX.GI
subject AltName		<b>√</b>	False			
SubjectAllivallie	Dfc922Nome	V /	i aise	0	D	Cartificate Holder's amail address
	Rfc822Name		]	U	L	Certificate Holder's email address



LuxTrust r	on SSCD NCP+ Publi	c Cert	ificate	Profile	for Ma	ass Signature Services
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
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	<b>√</b>			S	False
	nonRepudiation				S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>√</b>				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Advanced electronic massive signature services.
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

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

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.

The following to	le following table provides the description of the fields for Eux trust 55CD ECP Certificates.										
	LuxTrust Integration Certificate Profile										
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value					
Base Profile											
Version		<b>√</b>	False								
					S	Version 3 Value = "2"					
SerialNumbe	er	✓	False								
					FDV	Validated on duplicates.					
signatureAlg	jorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVal	ue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Global Qualified CA x					
	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								



	Lux	Trus	t Integ	ration	Certifi	cate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s)
	givenName	<b>✓</b>		М	D	TEST ONLY + " " + As provided by Subscriber
	surname	✓		М	D	As provided by Subscriber
	countryName	✓		М	D	LU
	emailAddress	✓		0	D	As provided by Subscriber
	Title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator"
	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>		M	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
subjectPubli		✓	False			
	Algorithm subjectPublicKey	<b>√</b>		M		Public Key: Key length: 2048bit (RSA); public
Extensions	SubjectFublicKey	•		IVI		exponent: Fermat-4 (=010001).
Authority						
Properties authorityKey	Idontifior	<b>√</b>	False			
aumontykey	keyldentifier	<b>√</b>	raise			SHA-1 Hash of the LuxTrust Global Qualified CA
authorityInfo	Access	<b>✓</b>	False			public key
	AccessMethod	<b>✓</b>	1 4.00			ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod accessLocation	<b>✓</b>				Id-ad-1
cRLDistribut		<b>▼</b>	False			http://qca.ocsp.luxtrust.lu/13
CIVEDISHIBUT	distributionPoint	<b>✓</b>	i aist		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeylo	lentifier 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						



	LuxTrust Integration Certificate Profile										
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value					
keyUsage		✓	True								
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificatePo	licies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.7					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	Policyldentifier	✓				0.4.0.2042.1.3					

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

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

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

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

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

	LuxTrust SSCD LCP+ Integration Certificate Profile										
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumb	er	✓	False								
-:A1			F-I		FDV	Validated on duplicates.					
signatureAl	gorithm	✓	False			OID = "4 0 040 440540 4 4 44" CLIA050 with					
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	alue	✓	False								
		1			D	Issuing CA Signature.					
Issuer		<b>✓</b>	False		S						
	countryName	<b>V</b>			S	LU					
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x					
Validity	organizationName	<b>✓</b>	False		5	LuxTrust S.A.					
validity	NotBefore	\ \ \ \	Faise		D	Certificate generation process date/time.					
	NotAfter	· ·			D	Certificate generation process date/time + 36 Months					
Subject		<b>✓</b>	False			Widhtis					
	serialNumber	✓	. 0.00	М	D	Serial Number as constructed by LRAO					
	commonName	<b>√</b>		М	D	LGQCA XX SC PRI V3 (XX a number selected internally by LuxTrust)					
	givenName	<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					
subjectPub	licKeyInfo	✓	False								
-	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public					
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).					



	LuxTrust SSCD LCP+ Integration Certificate Profile										
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value					
Extensions											
Authority Properties											
authorityKey	Identifier	✓	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/LTGQCAx.crt					
	AccessMethod	<b>√</b>				ld-ad-1					
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/13					
cRLDistribut	ionPoint	✓	False								
	distributionPoint	✓			S						
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl					
Subject Properties											
subjectAltNa	ıme	✓	False								
	Rfc822Name	✓		0	D	N/A					
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 bitstring bits).					
Policy Properties											
keyUsage		✓	True								
	digitalSignature	✓			S	True					
	nonRepudiation				S	False					
	keyEncipherment	✓			S	True					
	dataEncipherment	<b>√</b>			S	True					
certificatePo		<b>√</b>	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.8					
	policyQualifierID	✓ ✓			S	Id-qt-1 (CPS)					
	Qualifier				S	https://repository.luxtrust.lu					
	policyQualifierID DisplayText	√ ✓			S	Id-qt-2 (User Notice)  LuxTrust INTEGRATION CERTIFICATE on SSCD compliant with ETSI TS 102 042 LCP+certificate policy. Key Generation by CSP. Sole Authorised Usage: Authentication and Encryption for Integration Purposes.					
	Policyldentifier	✓				0.4.0.2042.1.3					

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

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

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

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

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



	LuxTrus	st Signing	g Serve	r LCP C	ertifica	te Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.5" – if SHA with RSA Encryption. OID = "1.2.840.113549.1.1.11" – SHA256 with RSA Encryption.
signatureVal	ue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time <b>36</b> Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	LGQCA XX CSS (XX a number selecte internally by LuxTrust) concatenation of given name(s) and surname(s) separated by a "Space character."
	givenName	<b>✓</b>		М	D	LGQCA XX (XX a number selecte internally by LuxTrust) or Give name(s) as on ID document
	Surname	<b>✓</b>		М	D	CSS or Surname(s) as on ID document without indication "épouse", "ép." of similar 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	cKevinfo	<b>✓</b>	False			
,	Algorithm	<b>✓</b>				Public Key: Key length: 2048 bit (RSA
	subjectPublicKey	<b>√</b>		М		public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties authorityKey	Identifier	<b>✓</b>	False			
aumontyney	keyldentifier	<b>✓</b>	i alse			SHA-1 Hash of the LuxTrust <b>Glob Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓	1			http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓			İ	http://qca.ocsp.luxtrust.lu/ <sup>13</sup>
cRLDistribut	ionPoint	<b>√</b>	False			TREAT GOLDOOP TO ALT USE LIVE
J. LEDISHIBUL	distributionPoint	<b>→</b>	1 4130		S	
	fullName	· ·	1		<del>                                     </del>	http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties	Turnium C					TREP # OH HUNCH GOLDEN ET GOODALOTT
subjectAltNa	ime	✓	False			
, , , , , , , , , , , , , , , , , , , ,	Rfc822Name	✓	1	0	D	N/A
subjectKeyld		<b>✓</b>	False			



	LuxTrus	t Signin	g Serve	r LCP C	ertifica	te Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</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	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.9
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					, , ,
	DisplayText	<b>V</b>				INTEGRATION Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Signature, Data or Entity Auth. and Data Enc. for integration purposes
	Policyldentifier	✓				0.4.0.2042.1.3

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

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

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

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

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

	LuxTr	ust SSCD	LORA	QCP+ (	Certific	ate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			·
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	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			



	LuxTrus	st SSCD	LORA	QCP+ (	Certific	ate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	✓		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		М	D	Constructed by LuxTrust
	localityName	✓		М	D	Country of RA
	organizationalUnitName 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	✓		М	D	RAO code Constructed by LuxTrust
subjectPubli		✓	False			
	Algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	SubjectFublickey	<u> </u>		IVI		exponent. 1 enhat-4 (=010001).
Authority						
Properties	d do náitic n	<b>✓</b>	Falsa			
authorityKey	keyldentifier	<u> </u>	False			SHA-1 Hash of the LuxTrust Global
and a wife deaf						Qualified CA public key
authorityInfo	AccessMethod	✓ ✓	False			Id-ad-2
	accessLocation	<u>√</u>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/13
cRLDistribut	tionPoint distributionPoint	<u>√</u>	False		S	
	fullName	<u> </u>			3	http://crl.luxtrust.lu/LTGQCAx.crl
Subject						THE PROPERTY OF THE PROPERTY O
Properties						
subjectAltNa	me Rfc822Name	<u>√</u>	False	0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False			Continuate Floride & Critain 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		<b>√</b>	True			
	digitalSignature nonRepudiation	✓ ✓	<del>                                     </del>		S	False True
	keyEncipherment	<u> </u>	-		S	False
	dataEncipherment	✓			S	False
certificatePo		<b>√</b>	False			10474440040
	PolicyIdentifier policyQualifierID	✓ ✓	-		S	1.3.171.1.1.10.3.10 Id-qt-1 (CPS)
	Qualifier	<u> </u>	-		S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers	•				



	LuxTrus	st SSCD	LORA	QCP+ (	Certific	ate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	DisplayText	<b>~</b>				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Support of Qualified Electronic Signature for LRAO purposes
	Policyldentifier	✓				0.4.0.1456.1.1
QualifiedCer	tificateStat					
	QcCompliance	✓		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]
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }

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

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

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

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

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

	LuxTr	ust SSC	D LOR	A NCP+	Certific	cate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			S	LuxTrust S.A.
Validity	1	<b>√</b>	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address



	LuxTrus	st SSC		A NCP+		cate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		М	D	Constructed by LuxTrust
	- <b>J</b>					
	localityName	✓		М	D	Country of RA
	, <b>,</b>					
	organizationalUnitName	,				DA
	1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName				_	
	2	✓		М	D	RAO code Constructed by LuxTrust
subjectPubli	cKeyInfo	✓	False			
-	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); publi
	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Globa
authorityInfo	Access	<b>√</b>	False			Qualified CA public key
authoritymic	AccessMethod	<b>✓</b>	raise			Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	<b>\</b>				http://qca.ocsp.luxtrust.lu/13
cRLDistribut		✓	False			
	distributionPoint	<b>√</b>			S	
Subject	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylo	dentifier keyldentifier	<b>√</b>	False		Fixed	The Key Identifier comprises a four hit field
	keyidentiner	·			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 th
						value or subjectPublicKey bit string (tag, no
						including the length and number of unuse
Policy						bit-string bits).
Properties						
keyUsage	1	✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	-	<b>√</b>			S	
	keyEncipherment					True
	dataEncipherment	✓			S	True
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.10.3.11
	policyQualifierID Qualifier	<b>√</b>			S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)
	noticeNumbers					·
	DisplayText	✓				LuxTrust Certificate on SSCD compliant wit
						ETSITS 102 042 NCP+ certificate policy. Ke
						Generation by CSP.  Sole Authorised Usage: Data or Entit
						Authentication and Data Encryption for LRAG
					<u> </u>	purposes.
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2

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

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





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

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

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

	LuxTrust non SS	CD Q	CP Mas	s LRAO	Signat	tures Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile	•					
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	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	<b>✓</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA officer – LRS"
	organizationName	<b>✓</b>		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA
	localityName	<b>✓</b>		M	D	Country of RA (as in articles of association)
	organizationalUnitName 1	✓		М	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	<b>✓</b>		0	D	RAO code Constructed by LuxTrust
sub	jectPublicKeyInfo	✓	False			
	Algorithm	✓				



	LuxTrust non S	SCD Q	CP Mas	s LRAO	Signat	tures Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	subjectPublicKey	<b>✓</b>		М		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority P	roperties					
authorityKe	eyldentifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the <b>LuxTrust Global Qualified</b> CA public key
authorityInf	foAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistrib	utionPoint	✓	False			
	distributionPoint	<b>✓</b>			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	✓				1.3.171.1.1.10.3.12
	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]



	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile						
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value	
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]	
	QcSSCD	✓				NOT SET	

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

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

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

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

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

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

The certificate re-key is not allowed.

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

	Lux	Trust eID S	SSCD Q	CP+ Ce	rtifica	te Profile
Attribute	Field	IN <sup>14</sup>	CE <sup>15</sup>	O/M <sup>16</sup>	CO <sup>17</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVal	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>18</sup>
	organizationName	✓			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

 $<sup>^{14}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certificate profile.

<sup>&</sup>lt;sup>15</sup> CE = Critical Extension.

 $<sup>^{16}</sup>$  O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>17</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

 $<sup>^{18}</sup>$  X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



	LuxII	ust eID S	SCD Q	CP+ Ce	rtifica	te Profile
Attribute	Field	IN <sup>14</sup>	CE <sup>15</sup>	O/M <sup>16</sup>	CO <sup>17</sup>	Value
	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
ļ	countryName	✓		М	D	LU
ļ	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"Private Person"
	organizationalUnitName 1	<b>✓</b>		0	D	If the holder is underage: "Mineur jusqu'à : " (Date of birth + 18 years).
subjectPubli		✓	False			
	Algorithm	<b>√</b>				Public Key: Key length: 2048bit up to 4096b
Extensions	subjectPublicKey	<b>V</b>		M		(RSA); public exponent: Fermat-4 (=010001)
Authority						
Properties						
authorityKey		<b>√</b>	False			SHA-1 Hash of the LuxTrust <b>Global Qualifie</b>
	keyldentifier	<b>Y</b>				CA x public key
authorityInfo		✓	False			,
	AccessMethod	✓				ld-ad-2
	accessLocation	✓ ✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod accessLocation	<b>✓</b>				Id-ad-1
aDI Diatrikus			Falsa			http://qca.ocsp.luxtrust.lu/13
cRLDistribut	distributionPoint	✓ ✓	False		S	
	fullName	<b>V</b> ✓			3	http://crl.luxtrust.lu/LTGQCAx.crl
Subject	rumvame					Tittp://ornidxtrast.la/E10Q0/A.ori
Properties						
subjectAltNa		✓	False			
subjectKeylo	Rfc822Name	✓ ✓	False	0	D	Subject email address
oubjeen to jie	keyldentifier	<b>√</b>	T dioo		Fixed	The Key Identifier comprises a four-bit fiel with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of th value or subjectPublicKey bit string (tag, not including the length and number of unused bit string bits).
						ettinig zite).
Policy						
Properties		<b>√</b>	True			
	digitalSignature	✓ ✓	True		S	
Properties	digitalSignature nonRepudiation		True		S	False True
Properties	nonRepudiation keyEncipherment	✓ ✓ ✓	True		S S	False True False
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment	✓ ✓ ✓			S	False True
Properties	nonRepudiation keyEncipherment dataEncipherment dicies	✓ ✓ ✓ ✓	True		S S	False True False False
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier	√ √ √ √ √			\$ \$ \$	False True False False 1.3.171.1.1.10.3.13
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier policyQualifierID	✓ ✓ ✓ ✓			<i>S S S</i>	False True False False False I.3.171.1.10.3.13 Id-qt-1 (CPS)
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier policyQualifierID Qualifier	√ √ √ √ √			S S S S	False True False False 1.3.171.1.1.10.3.13
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier policyQualifierID	\frac{\sqrt{\chi}}{\sqrt{\chi}}			<i>S S S</i>	False True False False False 1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment llicies PolicyIdentifier policyQualifierID Qualifier policyQualifierID noticeNumbers DisplayText	\frac{\sqrt{\chi}}{\sqrt{\chi}}			S S S S	False True False False  1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu Id-qt-2 (User Notice)  LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP.  Sole Authorised Usage: Support of Qualifie Electronic Signature.
Properties keyUsage certificatePo	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier policyQualifierID Qualifier policyQualifierID noticeNumbers DisplayText  PolicyIdentifier	\frac{\sqrt{\chi}}{\sqrt{\chi}}			S S S S	False True False False False  1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu Id-qt-2 (User Notice)  LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualifie
Properties keyUsage	nonRepudiation keyEncipherment dataEncipherment dicies PolicyIdentifier policyQualifierID Qualifier policyQualifierID noticeNumbers DisplayText  PolicyIdentifier tificateStat	V V V V V V V V V V V V V V V V V V V		NA NA	\$ \$ \$ \$ \$	False True False False  1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu Id-qt-2 (User Notice)  LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualifie Electronic Signature. 0.4.0.1456.1.1
Properties keyUsage certificatePo	nonRepudiation keyEncipherment dataEncipherment licies PolicyIdentifier policyQualifierID Qualifier policyQualifierID noticeNumbers DisplayText  PolicyIdentifier	\frac{\sqrt{\chi}}{\sqrt{\chi}}		M	S S S S	False True False False False  1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu Id-qt-2 (User Notice)  LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualifie Electronic Signature. 0.4.0.1456.1.1
Properties keyUsage certificatePo	nonRepudiation keyEncipherment dataEncipherment dicies PolicyIdentifier policyQualifierID Qualifier policyQualifierID noticeNumbers DisplayText  PolicyIdentifier tificateStat QcCompliance	V V V V V V V V V V V V V V V V V V V			\$ \$ \$ \$ \$	False True False False  1.3.171.1.1.10.3.13 Id-qt-1 (CPS) https://repository.luxtrust.lu Id-qt-2 (User Notice)  LuxTrust Qualified Certificate on SSCI compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Support of Qualifie Electronic Signature. 0.4.0.1456.1.1





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

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

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

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

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

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

The certificate re-key is not allowed.

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

	Lux	Trust	SSCD N	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version		✓	False			
<b>-</b>					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAl		✓	False			OID "4.0.040.440540.4.44", OILA050, W
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
signatureVa	luo.	<b>√</b>	False			RSA Encryption.
Signatureva	lue	•	i aise		D	Issuing CA Signature.
issuer		<b>√</b>	False		S	issuing OA Oighature.
100001	countryName	<b>√</b>	7 0100		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	✓			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	<b>✓</b>		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	<b>√</b>		М	D	Given name(s) as on ID card or as provided by the RNCID
	surname	<b>√</b>		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	✓		М	D	LU
	emailAddress	<b>√</b>		0	D	Subject's email address
	title	✓		М	D	"Private Person"
	organizationalUnitName 1	<b>√</b>		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubl	icKeyInfo	✓	False			
	algorithm	✓		_		Public Key: Key length: 2048 bit up to 4096bit
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (=010001).



	Lux	cTrust :	SSCD N	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Extensions						
Authority Properties						
	authorityKeyldentifier		False			
authorityitey	keyldentifier	✓ ✓	i aise			SHA-1 Hash of the LuxTrust Global Qualified
	noyluonimo.					CA x public key
authorityInfo	Access	✓	False			
,	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/13
cRLDistribut	ionPoint	✓	False			
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						·
Properties subjectAltNa	-	<b>√</b>	False			
SubjectAitNa	Rfc822Name	<b>✓</b>	Faise	0	D	Subject email address
subjectKeylo		<b>V</b> ✓	False	<u> </u>	U	Subject email address
Subjectivelying	keyldentifier	· ·	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).
Policy Properties						
keyUsage		<b>√</b>	True			
,	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo		✓	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	1			1	
	DisplayText	<b>*</b>				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP.  Sole Authorised Usage: Data or Entity Authentication and Data Encryption.
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

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

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

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 SS	SCD LCP	Integra	tion Sig	gnatur	e Certificate Profile
Attribute	Field	IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>	CO <sup>22</sup>	Value
Base			<u> </u>	· · · · · · · · · · · · · · · · · · ·		
Profile						
Version	1	✓	False		_	
CarialNivesh		<b>√</b>	E-I		S	Version 3 Value = "2"
SerialNumbe	er 	<b>V</b>	False		FDV	Validated on duplicates.
signatureAlg	porithm	<b>√</b>	False		TDV	validated on duplicates.
orginatar or ag	Algorithm		1 4100		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
						RSA Encryption.
signatureVa	lue	✓	False			
		,			D	Issuing CA Signature.
Issuer	accumtate them a	<b>√</b>	False		S	111
	countryName commonName	<b>✓</b>			S	LU
		· ✓			S	LuxTrust Global Qualified CA x <sup>1</sup> LuxTrust S.A.
Validity	organizationName	<b>√</b>	False		3	Luxtrust S.A.
validity	NotBefore	<u> </u>	i aise		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	1	✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
						Concatenation of given name(s) and
	commonName	✓		М	D	surname(s) separated by the space character
					_	
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x as provided by the RNCID
	countryName	✓		М	D	LU
		,		•		specimen-x Subject's email address as
	emailAddress	✓		0	D	provided by the RNCID
	title	✓		М	D	"Private Person"
	organizationalUnitName					If the holder is underage: "Mineur jusqu'à : " &
	1	✓		0	D	(Date of birth + 18 years).
subjectPubli	icKeyInfo	<b>√</b>	False			(2 and or arms 1 to years).
Subjecti ubii	Algorithm	<u> </u>	1 also			Public Key: Key length: 2048bit up to 4096bit
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions	,					
Authority						
Properties		_				
authorityKey		<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified
authorityInfo	Λοτρες	<b>√</b>	False			CA x public key
authorityniic	AccessMethod	<u> </u>	1 0130			ld-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓			İ	http://qca.ocsp.luxtrust.lu/ <sup>13</sup>
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						
Properties		,				
subjectAltNa		<b>√</b>	False	0	_	anasiman y Cubiastia amail addu
	Rfc822Name	<b>v</b>		0	D	specimen-x Subject's email address as provided by the RNCID

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

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

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

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



	LuxTrust eID S	SCD LCP	Integra	ation Si	gnatur	e Certificate Profile
Attribute	Field	IN <sup>19</sup>	<b>CE</b> <sup>20</sup>	<b>O/M</b> <sup>21</sup>	CO <sup>22</sup>	Value
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	<b>✓</b>			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.16
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>V</b>				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Electronic signature for Integration Purposes.
	Policyldentifier	✓				0.4.0.1456.1.1
QualifiedCer	rtificateStat					
	QcCompliance	✓		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]

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

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

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

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

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:

- 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>9</sup> CE <sup>10</sup> O/M <sup>11</sup> CO <sup>12</sup> Value								
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	SerialNumber								
					FDV	Validated on duplicates.			



	LuxTrust elD	SSCE	LCP li	ntegratio	n AE Ce	ertificate Profile
Attribute	Field	IN <sup>9</sup>	<b>CE</b> <sup>10</sup>	<b>O/M</b> <sup>11</sup>	CO <sup>12</sup>	Value
signatureAlg		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with
signatureVal	lua	<b>√</b>	False			RSA Encryption.
Signatureval	lue	•	raise		D	Issuing CA Signature.
issuer		✓	False		S	rooming of Orgitatoro.
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NetDefere	<b>√</b>	False		_	Contificate managetics are also details
	NotBefore NotAfter	<b>✓</b>			D D	Certificate generation process date/time.  Certificate generation process date/time + 12
	Notatei	·				Months; Certificate generation process date/time + 1
subject		<b>√</b>	False			day for PSEUDONYM Certificate
Subject	a and a IB Is seed to an		i aise		_	Operial Number and a second mode of the LDAO
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	✓		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x provided by the RNCID
		<b>√</b>				
	countryName	<b>V</b>		М	D	LU
	emailAddress	✓		0	D	specimen-x Subject's email address as provided by the RNCID
	title	✓		М	D	"Private Person"
	organizationalUnitName 1	✓		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit
Extensions	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (=010001).
Authority Properties						
authorityKey		✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInfo		<b>√</b>	False			14 - 4 0
	AccessMethod	<b>✓</b>				ld-ad-2
	accessLocation AccessMethod	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt Id-ad-1
	accessLocation	<b>√</b>				http://qca.ocsp.luxtrust.lu/ <sup>13</sup>
cRLDistribut		<b>√</b>	False			nttp://qca.ocsp.iuxtrust.iu/
OKEDISKIDA	distributionPoint	<b>√</b>	1 4100		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltNa		<b>√</b>	False			
aubicat/art	Rfc822Name	<b>√</b>	<b>F</b> =!	0	D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo		<b>✓</b>	False		Eivad	The Key Identifier comprises a faur his field
	keyldentifier	V			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties		<b>√</b>	True			
			Hue		+	
keyUsage	digitalSignature	1			0	I Truo
	digitalSignature	✓			S	True
	digitalSignature nonRepudiation keyEncipherment	✓			S S	True False True



	LuxTrust elD SSCD LCP Integration AE Certificate Profile									
Attribute	Field	IN <sup>9</sup>	<b>CE</b> <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
	dataEncipherment	✓			S	True				
certificatePo	licies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.3.17				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	<b>√</b>				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Authentication and Encryption for Integration Purposes				
	Policyldentifier	✓				0.4.0.2042.1.2				

#### 1.12.19 LuxTrust NCP+ Certificates supporting SEAL Signature Services

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

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

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

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

Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile	11010		<u> </u>	O/		Talac
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	✓			S	LuxTrust Global Qualified CA x
	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			
	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)



Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	ass Signature Services  Value
Attribute	stateOrProvinceName		CL	0	D	Value
	StateOrProvinceName	_ <u> </u>		_	D	
	emailAddress	✓		0	D	Subject's email address if available
	organizationName	~		М	D	Names as in articles of associatio including the legal form (as specified the memorandum and articles association or an equivale document)
	localityName	~		М	D	Location in which the organization registered office is established (a specified in the memorandum articles of association or an equivale 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	<b>✓</b>	ļ		ļ	Public Key: Key length: 2048 bit (RSA
Extensions	subjectPublicKey	V		M		public exponent: Fermat-4 (=010001
Authority Properties						
authorityKeyldentifier		<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Glob
		<b>✓</b>	Гаја			Qualified CA public key
authorityInfoAccess	AccessMethod	<b>V</b> ✓	False			ld-ad-2
	accessLocation	· /				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	<b>✓</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
0.11.45	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties subjectAltName		<b>✓</b>	False			
SubjectAllivanie	Rfc822Name	· /	i aise	0	D	Certificate Holder's email address
subjectKeyldentifier	THE SECTION OF THE SE	✓	False			Continuate Florage & Citian address
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-field with a 0100 value, followed by the least significant 60 bits of the SHA hash of the value or subjectPublicKebit string (tag, not including the leng and number of unused bit-string bits)
Policy Properties			_			
keyUsage	digitalSignature	<b>✓</b>	True		S	True
	nonRepudiation	<u> </u>			S	True
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	<b>✓</b>			S	False
certificatePolicies	l	<b>√</b>	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.15
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID DisplayText	<u> </u>			S	Id-qt-2 (User Notice)  LuxTrust Certificate on Secure Us Device compliant with ETSI TS 10 042 NCP+ certificate policy. K Generation by CSP.  Sole Authorised Usage: Advance
						electronic seal signature services.



LuxTrust n	LuxTrust non SSCD NCP+ Public Certificate Profile for Mass Signature Services								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
	Policyldentifier	✓				0.4.0.2042.1.2			

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

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

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

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

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

	LuxTrus	t SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			N. W. L. L. W. L.
-!AI		<b>✓</b>	F-1		FDV	Validated on duplicates.
signatureAl	algorithm	•	False		S	OID = "1.2.840.113549.1.1.11" -
			<u> </u>		3	SHA256 with RSA Encryption.
signatureVa	ilue	<b>√</b>	False			Landar OA Circatona
issuer		<b>✓</b>	False		D S	Issuing CA Signature.
issuer	countryName	<b>V</b> ✓	raise		S	LU
	commonName	· /			S	LuxTrust <b>SSL</b> CA x
	organizationName	· ✓			S	LuxTrust S.A.
Validity		✓	False			23777437 377
, , , , , , , , , , , , , , , , , , ,	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 12;24;36 Months
subject	1	✓	False			, ,
	countryName	<b>✓</b>		M	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	1		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName1	✓		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber
	commonName	~		М	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or IP address or unique name of server.
	serialNumber	✓		0	D	Serial Number as provided by subscriber



	LuxTrust	SSL S	erver LC	P Certif	icate P	rofile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	emailAddress	,		0	D	Subject's email address
		<b>✓</b>				
subjectPublic		✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA)
Extensions	subjectPublicKey	<b>✓</b>		M		public exponent: Fermat-4 (=010001).
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA
authorityInfo	Access	<b>√</b>	False			public key
daniontyllilo	AccessMethod	√ ·	1 disc			Id-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu <sup>23</sup>
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx.crt
cRLDistributi		<b>√</b>	False			
	distributionPoint fullName	✓ ✓			S	http://and.bustmint.bu/LTCCLCAss.ord
	fullname	•				http://crl.luxtrust.lu/LTSSLCAx.crl
CCT-		<b>✓</b>	E-I			Value and the Lan Orange
SCTs Subject		· ·	False	М	D	Values returned by Log Servers
Properties						
subjectAltNa	me	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
-	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name)
	•	<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)
	oubject/attivame-divolvame					of application/server – Exact DNS for a
		<b>✓</b>				Web Server or IP address or unique
	Outlie of Alfahama a dhighlama					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.
ļ	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		1	0		FQDN (Fully Qualified Domain Name
	<b>,</b>	<b>✓</b>				of application/server – Exact DNS for a
		•				Web Server or IP address or unique
	SubjectAltName-dNSName	-	1	0	1	name of server.  FQDN (Fully Qualified Domain Name
	ounjeurniname-unomaine					of application/server – Exact DNS for a
		<b>✓</b>				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
			i	1	1	
						name of server.
	SubjectAltName-dNSName			0		
	SubjectAltName-dNSName	<b>✓</b>		0		name of server.  FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique

 $<sup>^{23}</sup>$  Since SSL CA 2



	LuxTrust	OOLO	erver LC	r cerui	icate i	rofile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</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.
	SubjectAltName-URL	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server — Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server — Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
aubia at Vaudu	SubjectAltName-URL	<b>√</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
subjectKeylo		<b>V</b>	False			
D. U.	keyldentifier	v			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
operties			_			
keyUsage		✓	True			
	digitalSignature	<b>√</b>	True		S	True
	nonRepudiation	✓ ✓	True		S	False
	nonRepudiation keyEncipherment	✓ ✓	True		S	False True
keyÜsage	nonRepudiation  keyEncipherment  dataEncipherment	✓ ✓ ✓			S	False
	nonRepudiation keyEncipherment dataEncipherment	· · · · · · · · · · · · · · · · · · ·	True False		S	False True True
keyÜsage	nonRepudiation  keyEncipherment  dataEncipherment  blicies  PolicyIdentifier	\rightarrow			S	True True 1.3.171.1.1.10.5.1
keyÜsage	nonRepudiation  keyEncipherment  dataEncipherment  blicies  PolicyIdentifier  policyQualifierID	· · · · · · · · · · · · · · · · · · ·			S	True  True  1.3.171.1.1.10.5.1  Id-qt-1 (CPS)
keyÜsage	nonRepudiation  keyEncipherment  dataEncipherment  blicies  PolicyIdentifier  policyQualifierID  qualifier  PolicyIdentifier	\rightarrow			S S S	True True 1.3.171.1.1.10.5.1
keyÜsage	nonRepudiation  keyEncipherment  dataEncipherment  blicies  PolicyIdentifier  policyQualifierID  qualifier	\rightarrow			S S S	False  True  True  1.3.171.1.1.10.5.1  Id-qt-1 (CPS)  https://repository.luxtrust.lu



LuxTrust SSL Server LCP Certificate Profile									
Attribute	Attribute Field IN <sup>9</sup> CE <sup>10</sup> O/M <sup>11</sup> CO <sup>12</sup> Value								
	serverAuth	✓			S	True			
	clientAuth	✓			S	True			
	emailProtection	✓			S	True			

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

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

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

#### **Prohibited Certificate uses:**

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>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	r	✓	False						
		,			FDV	Validated on duplicates.			
signatureAlg		✓	False			015 "4 0 040 440540 4 4 44" 014050			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	ue	✓	False		_	Landa a OA Cina atom			
issuer		<b>√</b>	False		D S	Issuing CA Signature.			
issuer	countryName	<b>✓</b>	raise		S	LU			
	commonName	<b>√</b>			S	LuxTrust <b>SSL</b> CA x			
	organizationName	<b>√</b>			S	LuxTrust S.A.			
Validity	organizationivanie	<b>√</b>	False		3	Luxitust S.A.			
Validity	NotBefore	<i>✓</i>	1 4130		D	Certificate generation process date/time.			
	NotAfter	<b>√</b>			D	Certificate generation process date/time			
	HotAitei					+ 12;24 Months			
subject		✓	False						
	countryName			М	D	Country in which the company's or			
	(OID: 2.5.4.6)	✓		IVI		institution's registered office is established (as specified in the memorandum and articles of			
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)			M	D	association). (ISO3166)  Contains the country information specified using the applicable ISO			
		<b>√</b>				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)	✓		M	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 or Registration Agency at the state or 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'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.			



	SSL/TLS Ex	tended \	/alidatio	on Serv	er Cert	ificates
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	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)	✓		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
subjectPublic	ı cKevinfo	✓	False			
	algorithm	<b>√</b>	. 4.00			Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfo		<b>√</b>	False			
	AccessMethod	<b>√</b>			<b>_</b>	Id-ad-1
	accessLocation	<b>√</b>			ļ	http://ssl.ocsp.luxtrust.lu 23
	AccessMethod	✓ ✓			-	ld-ad-2 http://ca.luxtrust.lu/LTSSLCAx.crt
cRLDistribut	accessLocation ionPoint	<b>✓</b>	False			nttp://ca.iuxtruSt.iu/Ε1ΘΘΕCAX.CΠ
UNEDISTIBUT	distributionPoint	<b>→</b>	1 4130		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCAx.crl
SCTs		<b>√</b>	False	М	D	Values returned by Log Servers
Subject						
Properties subjectAltNa	me	<b>√</b>	False			
OUDJOURNING	SubjectAltName-dNSName	✓	, aide	М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.



	SSL/TLS Ext	tended \	/alidatio	on Serv	er Cert	ificates
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
711111111111111111111111111111111111111	SubjectAltName-dNSName		<u> </u>	0		FQDN (Fully Qualified Domain Name) of
	,					application/server – Exact DNS for a Web
						Server or IP address or unique name of
		✓				server, owned or controlled by the
						subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
		<b>√</b>				Server or IP address or unique name of server, owned or controlled by the
		•				subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
	,					application/server – Exact DNS for a Web
						Server or IP address or unique name of
		✓				server, owned or controlled by the
						subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
		<b>√</b>				Server or IP address or unique name of server, owned or controlled by the
		•				subject and to be associated with the
						Subject and to be associated with the Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
						Server or IP address or unique name of
		✓				server, owned or controlled by the
						subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
		<b>√</b>				Server or IP address or unique name of
		•				server, owned or controlled by the subject and to be associated with the
						Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
						Server or IP address or unique name of
		✓				server, owned or controlled by the
						subject and to be associated with the
						Subject's server. Wildcard name not
		1				allowed for EV SSL Certificates.
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
						application/server – Exact DNS for a Web
		<b>√</b>			]	Server or IP address or unique name of server, owned or controlled by the
		*			]	subject and to be associated with the
					]	Subject's server. Wildcard name not
						allowed for EV SSL Certificates.
	SubjectAltName-dNSName	1		0		FQDN (Fully Qualified Domain Name) of
				_		application/server – Exact DNS for a 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
authing of the						allowed for EV SSL Certificates.
subjectKeyld		<b>✓</b>	False		Fixed	The Key Identifier comprises a few hit
	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						



	SSL/TLS Extended Validation Server Certificates								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
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	✓				1.3.171.1.1.10.5.2			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	Policyldentifier	✓				0.4.0.2042.1.4			
	Policyldentifier	✓				2.23.140.1.1			
Extended Ke	Extended Key Usage		False						
	serverAuth	✓			S	True			
	clientAuth	✓			S	True			
	emailProtection	✓			S	False			

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

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

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

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

#### Prohibited Certificate uses:

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

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

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

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

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





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

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

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

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

	SSL/TLS Extended Validation	on Serv	er Certi	ficates	on Sec	cure User Device
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</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	ılue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust <b>SSL</b> CA x
	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 of association). (ISO3166)
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	<b>~</b>		M	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)



	SSL/TLS Extended Validation	Serve	er Certif	icates	on Sec	cure User Device
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	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 or Registration Agency at the state or 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'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>		M	D	Depending on the Subject qualifications, this field contains one of the following String:  Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	✓		М	D	See EV Guidelines [13]:  For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.  For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	<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		✓	False			
	Algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						,



	SSL/TLS Extended Validation	n Serv	er Certi	ficates	on Sec	cure User Device
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Authority						
Properties authorityKey	/Identifier	<b>√</b>	False			
authorityrte	keyldentifier	· /	i aise			SHA-1 Hash of the LuxTrust SSL
						CA public key
authorityInfo		✓	False			
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>✓</b>				http://ssl.ocsp.luxtrust.lu 23
	AccessMethod	✓ ✓				Id-ad-2
cRLDistribu	accessLocation	<b>✓</b>	False			http://ca.luxtrust.lu/LTSSLCAx.crt
CKEDISHIDU	distributionPoint	<del> </del>	raise		S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTSSLCAx.crl
Subject						•
Properties						
subjectAltNa		✓	False			50011 (5.11 0.115)
	SubjectAltName-dNSName	<b>✓</b>		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>√</b>		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 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>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	SubjectAltName-dNSName	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	<b>~</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
subjectKeylo		<b>√</b>	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			
Reyosage	digitalSignature	<b>√</b>	Truc		S	True
	nonRepudiation	<b>✓</b>			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo		✓	False			
	Policyldentifier	✓			_	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 y Usage	✓ ✓	False			0.4.0.2042.1.5
	serverAuth	<b>✓</b>			S	True
	clientAuth	<b>✓</b>			S	True
	emailProtection	<b>✓</b>			S	False
	omani rotootion		1	1		1 4100

## 1.12.23 LuxTrust Object (or Code) Signing Certificates

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

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





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

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

	LuxTrust LCP Code Signing Certificate Profile										
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value					
Base Prof	ile										
Version		<b>✓</b>	False								
					S	Version 3 Value = "2"					
SerialNum	ber	<b>✓</b>	False								
					FDV	Validated on duplicates.					
signature	Algorithm	<b>✓</b>	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					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	✓			D	Certificate generation process date/time + 12; 24; 36 months					
Subject		✓	False								
	countryName	✓		М	D	Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)					
	stateOrProvinceName	✓		0	D						
	localityName	<b>√</b>		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)					
	organizationName	<b>√</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)					
	organizationalUnitName1	✓		0	D	As provided by Subscriber					
	organizationalUnitName2	<b>√</b>		0	D	As provided by Subscriber					
	commonName	<b>√</b>		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)					
	serialNumber	✓		0	D	NA or Serial Number as provided by subscriber					
	emailAddress	✓		0	D	Subject's email address if available					
subjectPu	blicKeyInfo	✓	False								
	Algorithm	✓				Public Key: Key length: 2048 (RSA); public					
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).					



LuxTrust LCP Code Signing Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
Extension	s								
Authority	Properties								
authorityK	<b>Keyldentifier</b>	✓	False						
	keyldentifier	<b>✓</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key			
authorityli	nfoAccess	✓	False						
	AccessMethod	✓				Id-ad-1			
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu 23			
	AccessMethod	✓				ld-ad-2			
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx.crt			
CRLDistril	butionPoint	✓	False						
	distributionPoint	✓			S				
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx.crl			
Subject Pr	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			

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

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





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

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

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

	LuxTrus	4 661	Client	CP Cor	tificato	Drofile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base						
Profile Version		<b>✓</b>	False			
Version		•	raise		S	Version 3 Value = "2"
SerialNumbe	er	<b>√</b>	False			version 5 value – 2
oon an tannot			1 dioc		FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
						with RSA Encryption.
signatureVa	lue	✓	False			
		,	<u> </u>		D	Issuing CA Signature.
Issuer	1	<b>√</b>	False		S	
	countryName	<b>√</b>			S	LU
	commonName organizationName	✓ ✓			S	LuxTrust <b>SSL</b> CA LuxTrust S.A.
Validity	organizationName	<b>V</b> ✓	False		3	Luxtrust S.A.
Validity	NotBefore	· ·	i aise		D	Certificate generation process date/time.
	NotAfter	· /	†		D	Certificate generation process date/time +
						12; 24; 36 Months
Subject		✓	False			
	countryName			М	D	Country in which the company's or
	oounii yraanie			141		institution's registered office is established
		✓				(as specified in the memorandum and
						articles of association). (ISO3166)
	stateOrProvinceName	<b>✓</b>		0	D	
	StateOrProvinceName	· ·		0	D	
	localityName			М	D	Location in which the company's
		✓				registered office is established (as
						specified in the memorandum and articles
						of association or an equivalent document)
	organizationName			М	D	Names as in articles of association,
		✓				including the legal form (as specified in
		•				the memorandum and articles of
						association or an equivalent document)
	organizationalUnitName 1			0	D	As provided by Subscriber
	organizational on the table of	✓				7.6 provided by Gubsonber
	organizationalUnitName 2	✓		0	D	As provided by Subscriber
	commonName	✓		М	D	As provided by Subscriber
	serialNumber	<b>✓</b>		0	D	Serial Number as provided by subscriber
			1			
	emailAddress	<b>✓</b>		0	D	Subject's email address
		•				
subjectPubli	icKovinto	<b>√</b>	Folos			
Subject ubil	Algorithm	V /	False			Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	· /	†	М	1	public exponent: Fermat-4 (=010001).
Extensions						1
Authority						
Properties						
authorityKey		<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA
auth auth du f	A0000	<b>√</b>	Folce			public key
authorityInfo	AccessMethod	<b>✓</b>	False			ld ad 1
	accessLocation	V /	+		1	Id-ad-1
			1		1	http://ssl.ocsp.luxtrust.lu <sup>23</sup>
	AccessMethod	✓				Id-ad-2



	LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCAx.crt				
cRLDistribut	ionPoint	✓	False							
	distributionPoint	✓			S					
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx.crl				
Subject Properties										
subjectAltNa	ime	✓	False							
	Rfc822Name	✓		0	D	Certificate Holder's email address				
subjectKeylo		✓	False							
	keyldentifier	<b>\</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy										
Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	True				
	nonRepudiation	<b>√</b>			S	False				
	keyEncipherment	<b>√</b>			S	True				
	dataEncipherment	<b>✓</b>			S	True				
certificatePo		✓	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							
<u> </u>	serverAuth	✓			S	False				
	clientAuth	✓			S	True				
	emailProtection	✓			S	True				

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

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

	SSL/TLS QCP-w Extended Validation Server Certificates								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	jorithm	✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	lue	✓	False						
,					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust SSL CA x			
	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						



	SSL/TLS QCP-w	Extend	ed Valid	lation S	erver (	Certificates
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	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 of 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 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)	✓		M	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 or Registration Agency at the state or province level MUST include both country and state or province information,
	localityName (2.5.4.7)	<b>√</b>		M	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	<b>√</b>		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	<b>√</b>		M	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	<b>√</b>		М	D	Depending on the Subject qualifications, this field contains one of the following String:  Private Organization Government Entity



	SSL/TLS QCP-w	Extend	ed Valid	dation S	erver (	Certificates
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	serialNumber			М	D	See EV Guidelines [13] :
	(OID: 2.5.4.5)	·				For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration 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			0	D	Postal code of the subject place of
	(OID: 2.5.4.17)	<b>~</b>				business.
	streetAddress	<b>√</b>		0	D	Number and Street of the physical
	(OID: 2.5.4.9)	•				location of the subject
subjectPublic		✓	False			
	algorithm	<b>√</b>				Public Key: Key length: 2048 bit (RSA);
Futanciana	subjectPublicKey	<b>√</b>		M		public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties						
authorityKey	Identifier	✓	False			
	keyldentifier	<b>~</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authorityInfo		<b>√</b>	False			
	AccessMethod accessLocation	✓ ✓				ld-ad-1
		<b>V</b> ✓				http://ssl.ocsp.luxtrust.lu <sup>23</sup>
	AccessMethod accessLocation	<b>✓</b>				ld-ad-2 http://ca.luxtrust.lu/LTSSLCAx.crt
cRLDistribut		<b>V</b>	False			nttp://ca.iuxtrust.iu/LTSSLCAx.crt
OKEDISKIBUK	distributionPoint	<b>√</b>	1 4100		S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx.crl
SCTs		✓	False	М	D	Values returned by Log Servers
Subject						
Properties subject AltNa	me	<b>√</b>	False			
JubjectAitild	SubjectAltName-dNSName		1 4130	М		FQDN (Fully Qualified Domain Name) of
	·	<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>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
	SubjectAltName-dNSName	<b>✓</b>		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates



	SSL/TLS QCP-w	Extend	ed Valid	lation S	erver (	Certificates
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
THE DATE	SubjectAltName-dNSName	<i>√</i>	32	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	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 bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			_
	digitalSignature	✓ ✓			S	True
	nonRepudiation keyEncipherment	<b>V</b>			S	False True
	dataEncipherment	<b>V</b> ✓			S	False
certificatePo		<b>✓</b>	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.5.6
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu





	SSL/TLS QCP-w Extended Validation Server Certificates								
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value			
	Policyldentifier	<b>√</b>				0.4.0.194112.1.4			
	Policyldentifier	<b>√</b>				0.4.0.2042.1.4			
	Policyldentifier	<b>√</b>			S	2.23.140.1.1			
Extended Ke	ey Usage	<b>√</b>	False						
	serverAuth	✓			S	True			
	clientAuth	✓			S	True			
	emailProtection	✓			S	False			
QualifiedCer	rtificateStat	<b>√</b>	False						
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True			
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repos itory/PDS.pdf			
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-web (0.4.0.1862.1.6.3)			

# 1.12.26 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 Server LCP Certificate Profile -Wildcard									
Attribute	Field	IN	CE	O/M	co	Value				
Base										
Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256				
						with RSA Encryption.				
signatureVa	lue	✓	False							
					D	Issuing CA Signature.				
issuer		<b>✓</b>	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust <b>SSL</b> 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							



	LuxTrust SSL Server LCP Certificate Profile -Wildcard									
Attribute	Field	IN	CE	O/M	со	Value				
	countryName	<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)				
	stateOrProvinceName	✓		0	D					
	localityName  organizationName			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)				
				М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)				
	organizationalUnitName1	✓		0	D	As provided by Subscriber				
	organizationalUnitName2	✓		0	D	As provided by Subscriber				
	commonName	<b>√</b>		М	D	FQDN (Fully Qualified Domain Name) of application/server registered for LuxTrust S.A.				
	serialNumber	✓		0	D	Serial Number as provided by subscriber				
subjectPubli	icKeyInfo	<b>✓</b>	False							
	algorithm	<b>✓</b>				Public Key: Key length: 2048 bit up to				
	subjectPublicKey	<b>√</b>		М		4096 bits (RSA); public exponent: Fermat-4 (=010001).				
Extensions										
Authority Properties										
authorityKey	/Identifier	<b>√</b>	False							
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key				
authorityInfo	Access	✓	False							
	AccessMethod	✓				ld-ad-1				
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu[1]				
	AccessMethod	✓				ld-ad-2				
	accessLocation	✓				http://ca.luxtrust.lu/LTSSLCA5.crt				
cRLDistribut	tionPoint	✓	False							
	distributionPoint	✓			S					
	fullName	✓				http://crl.luxtrust.lu/LTSSLCA5.crl				
Subject Properties										



	LuxTrust SSL So	erver	LCP Ce	rtifica	te Pro	file -Wildcard
Attribute	Field	IN	CE	O/M	СО	Value
subjectAltNa	ame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
	SubjectAltName-dNSName	<b>~</b>		М		FQDN (Fully Qualified Domain Name) of application/server registered for LuxTrust S.A.
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePo	licies	✓	False			
	Policyldentifier	✓			S	1.3.171.1.1.10.5.7
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	✓				2.23.140.1.2.2
	Policyldentifier	✓				0.4.0.2042.1.7
Extended Ke	ey Usage	<b>✓</b>	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	True

#### 1.12.27 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>18</sup> CE <sup>19</sup> O/M <sup>20</sup> CO <sup>21</sup> Value									
Base Profile									



	SPARE LuxTrust Signing Server LCP Certificate Profile										
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value					
Version			False								
					S	Version 3 Value = "2"					
SerialNumber			False								
					FDV	Validated on duplicates.					
signatureAlgo	rithm		False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.					
signatureValue	9		False								
					D	Issuing CA Signature.					
Issuer			False		S						
	countryName				S	LU					
	commonName				S	LuxTrust Global Qualified CA x					
	organizationName				S	LuxTrust S.A.					
Validity			False								
	NotBefore				D	Certificate generation process date/time.					
	NotAfter				D	Certificate generation process date/time + 36 Months					
Subject			False								
	serialNumber			М	D	Serial Number as constructed by LRAO					
	commonName			М	D	LGQCA XX CSS (XX a number selected internally by LuxTrust) or Concatenation of given name(s) and surname(s) separated by a "Space" character.					
	givenName			М	D	LGQCA XX (XX a number selected internally by LuxTrust) or Given name(s) as on ID document					
	Surname			М	D	CSS or Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)					
	countryName			М	D	LU or Nationality of holder (ISO3166)					
	emailAddress			0	D	N/A					
	Title			М	D	Private Person					
subjectPublich	KeyInfo		False								
	Algorithm										
	L				1						



	SPAR	E LuxTrus	t Signin	g Server L	.CP Certifi	icate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	subjectPublicKey			M		Public Key: Key length: 2048 bit (RSA) up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeyl	dentifier		False			
	keyldentifier					SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo <i>l</i>	Access		False			
	AccessMethod					Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod					ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>23</sup>
cRLDistributionPoint			False			
	distributionPoint				S	
	fullName					http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						
subjectAltNar	me		False			
	Rfc822Name			0	D	N/A
subjectKeylde	entifier		False			
	keyldentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
certificatePoli	icies		False			
	Policyldentifier					1.3.171.1.10.3.20
	policyQualifierID				S	Id-qt-1 (CPS)





	SPARE LuxTrust Signing Server LCP Certificate Profile											
Attribute Field IN <sup>18</sup> CE <sup>19</sup> O/M <sup>20</sup> CO <sup>21</sup> Value												
	Qualifier				S	https://repository.luxtrust.lu						
	Policyldentifier   0.4.0.2042.1.3											

#### 1.12.28 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] QCPl-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.21>. The following table provides the description of the fields for LuxTrust Qualified Certificates for digital signatue purpose.

						tificate Profile
Attribute	Field	IN <sup>24</sup>	CE <sup>25</sup>	O/M <sup>26</sup>	CO <sup>27</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	Algorithm	<b>✓</b>			S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	signatureValue		False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x1
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)

 $<sup>^{24}</sup>$  IN = Included: Attribute / field included within the certify cate profile.

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

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

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



		LuxTr	ust Qual	ified eSI	EAL Cer	tificate Profile
Attribute	Field	IN <sup>24</sup>	CE <sup>25</sup>	O/M <sup>26</sup>	CO <sup>27</sup>	Value
	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 entitiy 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
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
subjectPubli	cKeyInfo	✓	False			
	Algorithm	<b>✓</b>				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	<b>✓</b>		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>28</sup>
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectKeylo	lentifier	<b>√</b>	False			
	keyldentifier	√ ·	1 0100		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			

<sup>&</sup>lt;sup>28</sup> SINCE LTGQCA3





	LuxTrust Qualified eSEAL Certificate Profile										
Attribute	Field	IN <sup>24</sup>	CE <sup>25</sup>	O/M <sup>26</sup>	CO <sup>27</sup>	Value					
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificatePo		✓	False								
	Policyldentifier	<b>~</b>				1.3.171.1.1.10.3.21					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)					
	Policyldentifier	✓				0.4.0.194112.1.3					
BasicConst											
	CA	✓			S	FALSE					
	pathLenConstraint	✓			S	0 (ZERO)					
QualifiedCe	rtificateStat	✓	False								
	QcCompliance (0.4.0.1862.1.1)	<b>✓</b>		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	<b>V</b>		М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>V</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf					
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)					





#### 1.12.29 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>.

	LuxTrust NCP+ Certificate Profile for authentication									
Attribute	Field	IN <sup>29</sup>	CE <sup>30</sup>	O/M <sup>31</sup>	CO <sup>32</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er I	✓	False		ED) /	Malidate describertos				
signatureAlg	norithm	<b>✓</b>	False		FDV	Validated on duplicates.				
SignatureAig	Algorithm	•	raise		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA				
	Aigoriann				3	Encryption.				
signatureVa	lue	<b>✓</b>	False			Enorypaon.				
					D	Issuing CA Signature.				
Issuer		✓	False		S	g - g - m -				
	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 + 24 Months				
Subject		✓	False							
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).				
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)				
	organisationIdentifier (2.5.4.97)	<b>√</b>		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  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).				

 $<sup>^{29}</sup>$  IN = Included: Attribute / field included within the certify cate profile.

 $<sup>^{30}\,\</sup>mathrm{CE}$  = Critical Extension.

 $<sup>^{31}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{32}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	LuxTrust NCP+ Certificate Profile for authentication										
Attribute	Field	IN <sup>29</sup>	CE <sup>30</sup>	O/M <sup>31</sup>	CO <sup>32</sup>	Value					
	organizationalUnitName	<b>√</b>	-	0	D	Company/institution department or other information item					
	serialNumber	✓		М	D	Serial Number as constructed by LRAO					
subjectPubli	icKeyInfo	✓	False								
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);					
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).					
Extensions											
Authority Properties											
authorityKey		✓	False								
	keyldentifier	✓				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key					
authorityInfo	Access	✓	False								
'-	AccessMethod	✓				ld-ad-2					
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt					
	AccessMethod	✓				ld-ad-1					
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/33					
cRLDistribut		✓	False								
	distributionPoint	✓			S						
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.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 bit-string bits).					
Policy Properties											
keyUsage		✓	True								
	digitalSignature	✓			S	True					
	nonRepudiation	✓			S	False					
	keyEncipherment	<b>√</b>			S	True					
	dataEncipherment	<b>√</b>			S	False					
certificatePo	olicies	<b>√</b>	False								
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.22					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	qualifier	<b>✓</b>			S	https://repository.luxtrust.lu					
	policyQualifierID	<b>✓</b>			S	Id-qt-2 (User Notice)					
	Policyldentifier	1				0.4.0.2042.1.2					

# 1.12.30 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

33	SINCE	ΙТ	GC	$C\Delta 3$
	SHILL	. ட เ	GU	UHU





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>.

	Lux	Trust A	Advance	ed eSEA	L Certif	icate Profile
Attribute	Field	IN <sup>34</sup>	CE <sup>35</sup>	O/M <sup>36</sup>	CO <sup>37</sup>	Value
Base Profile	Ticiu		OL.	0/111	- 00	Value
Version		<b>√</b>	False			
70101011			1 4150		S	Version 3 Value = "2"
SerialNumber		<b>√</b>	False			VOISION O VAIAC — Z
Contantantibol			1 4150		FDV	Validated on duplicates.
signatureAlgorithm		<b>√</b>	False		100	validated off duplicates.
Algorithm	<u> </u>		1 4130		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
Algorium	•				3	Encryption.
signatureValue		<b>√</b>	False			Encryption.
oignaturo varao			1 4150		D	Issuing CA Signature.
Issuer		<b>√</b>	False		S	issuing of Cignature.
countryN	ame	· ✓	1 4136		S	LU
commonl		·			S	LuxTrust Global Qualified CA x <sup>1</sup>
organizat		<i>√</i>			S	LuxTrust S.A.
	ionname	<b>∨</b>	Calaa		5	Lux Trust S.A.
Validity		<b>∨</b>	False		_	Contitionts are resting property data (times
NotBefore NotAfter	t	<b>✓</b>			D D	Certificate generation process date/time.
NotAfter		•			D	Certificate generation process date/time + 24 Months
Subject		<b>✓</b>	False			
commonl	Name	<b>✓</b>		М	D	Shall contain the full registered name of the subject (legal person).
countryN	ame	✓		М	D	the country in which the subject (legal person) is established (ISO3166)
_	tionIdentifier 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.
organizat		<b>√</b>		M	D	Shall contain the full registered name of the subject (legal person).  Company/institution department or other
organizat	ionalUnitName	<b>√</b>		0	D	information item
serialNun	nber	✓		М	D	Serial Number as constructed by LRAO
subjectPublicKeyInfo		✓	False			

 $<sup>^{34}</sup>$  IN = Included: Attribute / field included within the certify cate profile.

 $<sup>^{35}</sup>$  CE = Critical Extension.

<sup>&</sup>lt;sup>36</sup> O/M: O = Optional, M = Mandatory.

 $<sup>^{37}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



Extensions   Authority   Properties   authorityKeyldentifier   ✓ False   SHA-1 Hash of the LuxTrust Global Qualified public key		Lux	Trust	Advance	ed eSEA	L Certifi	icate Profile
Extensions   Authority   Properties   authorityKeyldentifier   ✓ False   SHA-1 Hash of the LuxTrust Global Qualified public key	Attribute	Field	IN <sup>34</sup>	CE <sup>35</sup>	O/M <sup>36</sup>	CO <sup>37</sup>	Value
Extensions   Authority   Properties   authorityKeyldentifier   ✓ False   SHA-1 Hash of the LuxTrust Global Qualified public key		Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
Authority Properties authorityKeyldentifier    keyldentifier	-		✓		М		
Properties   authorityKeyIdentifier	Extensions	•					
authorityKeyldentifier   V   False   SHA-1 Hash of the LuxTrust Global Qualified public key	Authority						
Reyldentifier   V	Properties						
authorityInfoAccess	authorityKeylde		✓	False			
AccessMethod		keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
accessLocation	authorityInfoAco	cess	✓	False			
AccessMethod   Id-ad-1   http://qca.ocsp.luxtrust.lu/38	_	AccessMethod	✓				ld-ad-2
CRLDistributionPoint		accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
CRLDistributionPoint		AccessMethod	✓				
distributionPoint   fullName   http://crl.luxtrust.lu/LTGQCAx.crl		accessLocation	✓				http://qca.ocsp.luxtrust.lu/38
FullName   ✓	cRLDistribution		✓	False			
Subject Properties subjectKeyldentifier  keyldentifier  keyldentifier  Fixed  The Key Identifier comprises a four-bit field wi 0100 value, followed by the least significant 60 of the SHA-1 hash of the value or subjectPublic bit string (tag, not including the length and number unused bit-string bits).  Policy Properties  keyUsage  digitalSignature nonRepudiation keyEncipherment dataEncipherment  S False  S False  S False		distributionPoint	✓			S	
Properties   SubjectKeyldentifier   ✓ False   Fixed   The Key Identifier comprises a four-bit field wing 0100 value, followed by the least significant 60 of the SHA-1 hash of the value or subjectPublic bit string (tag, not including the length and number unused bit-string bits).    Policy Properties		fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Reyldentifier   V	Properties						
Policy Properties    digitalSignature   ronRepudiation    subjectKeyldent		✓	False				
Properties   Variable   Variabl		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).
digitalSignature     ✓     S     False       nonRepudiation     ✓     S     True       keyEncipherment     ✓     S     False       dataEncipherment     ✓     S     False	Properties						
nonRepudiation     ✓     S     True       keyEncipherment     ✓     S     False       dataEncipherment     ✓     S     False	keyUsage			True			
keyEncipherment     ✓     S     False       dataEncipherment     ✓     S     False							
dataEncipherment ✓ S False			✓				True
						S	
cartificatePolicies \sqrt{False}						S	False
T GIOC	certificatePolici		✓	False			
Policyldentifier		Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.23
policyQualifierID ✓ S Id-qt-1 (CPS)		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			✓				
BasicConstraints	BasicConstraint						
CA ✓ S FALSE		CA	✓			S	FALSE
pathLenConstraint ✓ S 0 (ZERO)		pathLenConstraint	✓			S	

#### 1.12.31 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.

<sup>38</sup> SINCE LTGQCA3



		LuxTru	st Adva	nced eS	EAL Ce	rtificate Profile
Attribute	Field	IN <sup>39</sup>	CE <sup>40</sup>	O/M <sup>41</sup>	CO <sup>42</sup>	Value
Base						
Profile						
Version	1	✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er '	✓	False		ED) /	N P 1 6 1 1 P 6
olanotura Ala		<b>✓</b>	Гаја		FDV	Validated on duplicates.
signatureAl	Algorithm	•	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
					3	Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer	1	✓	False		S	
	countryName	<b>√</b>			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	1	<b>√</b>	False		_	
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 24 Months
Subject		✓	False			
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	<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).

 $<sup>^{39}</sup>$  IN = Included: Attribute / field included within the certify cate profile.

 $<sup>^{40}\,\</sup>mathrm{CE}$  = Critical Extension.

 $<sup>^{41}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{42}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.





					1	
	organizationalUnitName	✓		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 (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	/Identifier	✓	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/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/43
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectKeylo	dentifier	✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bitstring bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePo	licies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.24
	policyQualifierID	<b>√</b>			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 oneylacitines					0.4.0.2042.1.2

<sup>43</sup> SINCE LTGQCA3





#### 1.12.32 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>44</sup>	CE <sup>45</sup>	O/M <sup>46</sup>	CO <sup>47</sup>	Value					
Base Profile											
Version	T	✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	er T	✓	False		ED) (	N. P. L. C. L. P. C.					
olamatuma Ala	n o nittle me		F-1		FDV	Validated on duplicates.					
signatureAlg		✓	False			OID #4.0.040.440540.4.4.44" OI IA.050 with DOA					
<u> </u>	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVa	lue	✓	False		_						
					D	Issuing CA Signature.					
Issuer	1	<b>√</b>	False		S						
	countryName	<b>√</b>			S	LU					
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x1					
	organizationName	<b>√</b>	_		S	LuxTrust S.A.					
Validity	T	<b>√</b>	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 24 Months					
Subject	1	✓	False								
	commonName	✓		М	D	Shall contain the full registered name of the subject (legal person).					
	countryName	✓		М	D	the country in which the subject (legal person) is established (ISO3166)					
	organisationIdentifier (2.5.4.97)	*		М	D	Shall contain information using the following structure in the presented order:  - 3 character legal person identity type reference;  - 2 character ISO 3166 country code;  - hyphen-minus "-" and  - identifier (according to country and identity type reference).  The three initial characters shall have one of the following defined values:  1) "VAT" for identification based on a national value added tax identification number.  2) "NTR" for identification based on an identifier from a national trade register.  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).					

 $<sup>^{44}</sup>$  IN = Included: Attribute / field included within the certify cate profile.

 $<sup>^{45}</sup>$  CE = Critical Extension.

 $<sup>^{46}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{47}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	LuxTrust Advanced Automated eSEAL Certificate Profile											
Attribute	Field	IN <sup>44</sup>	CE <sup>45</sup>	O/M <sup>46</sup>	CO <sup>47</sup>	Value						
	organizationalUnitName	<b>√</b>		0	D	Company/institution department or other information item						
subjectPubli		<b>✓</b>	False									
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);						
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).						
Extensions												
Authority Properties												
authorityKey		<b>✓</b>	False									
	keyldentifier	<b>&gt;</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key						
authorityInfo	Access	<b>✓</b>	False									
	AccessMethod	✓				Id-ad-2						
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt						
	AccessMethod	<b>&gt;</b>				Id-ad-1						
	accessLocation	<b>\</b>				http://qca.ocsp.luxtrust.lu/48						
cRLDistribut		<b>✓</b>	False									
	distributionPoint	✓			S							
	fullName	<b>&gt;</b>				http://crl.luxtrust.lu/LTGQCAx.crl						
Subject Properties												
subjectKeylo	dentifier	✓	False									
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).						
Policy												
Properties												
keyUsage		✓	True									
	digitalSignature	✓			S	False						
	nonRepudiation	✓			S	True						
	keyEncipherment	✓			S	False						
	dataEncipherment	✓			S	False						
certificatePo		✓	False									
	Policyldentifier	✓				1.3.171.1.1.10.3.25						
	policyQualifierID	<b>✓</b>			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						
BasicConstr												
	CA	✓			S	FALSE						
	pathLenConstraint	✓			S	0 (ZERO)						

<sup>48</sup> SINCE LTGQCA3



# 1.12.33 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 <sup>49</sup>	CE <sup>50</sup>	O/M <sup>51</sup>	CO 52	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	nber	✓	False								
					FDV	Validated on duplicates.					
signature	Algorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signature	Value	✓	False			,					
					D	Issuing CA Signature.					
Issuer		✓	False		S	ÿ ÿ					
	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								

 $<sup>^{\</sup>rm 49}$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{50}\,\</sup>mathrm{CE}$  = Critical Extension.

 $<sup>^{51}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{52}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	Lux	Trust	Smart	Card Q	CP-n-c	qscd Certificate Profile
Attribut e	Field	IN <sup>49</sup>	CE <sup>50</sup>	O/M <sup>51</sup>	CO 52	Value
	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		M	D	<b>PRO and PRIVATE products</b> : Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	<b>✓</b>		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		М	D	Subject's email address
	title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	<b>√</b>		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	<b>✓</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT 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	ıblicKeyInfo	✓	False			
	Algorithm subjectPublicKey	✓ ✓		M		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extensi	Subjecti ubilertey			IVI		oxponent. Fermat 1 (=0 1000 1).
Authorit y Properti es						
authority	Keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA
	keyldentifier					public key
authorityl	nfoAccess	<b>√</b>	False			14 - 4 0
	AccessMethod accessLocatio	✓ ✓				ld-ad-2 http://ca.luxtrust.lu/LTGQCAx.crt
	n					·
	AccessMethod accessLocatio	✓ ✓				Id-ad-1
	n					http://qca.ocsp.luxtrust.lu/ <sup>53</sup>
cRLDistril	butionPoint	✓ ✓	False		C	
	distributionPoint fullName	<b>✓</b>			S	http://crl.luxtrust.lu/LTGQCAx.crl
	rum <b>t</b> ame	L .	l	l	l	http://on.iuxtruot.iu/L1GQOAX.011

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



	LuxTrust Smart Card QCP-n-qscd Certificate Profile										
Attribut e	Field	IN <sup>49</sup>	CE <sup>50</sup>	O/M <sup>51</sup>	CO 52	Value					
Subject Properti es											
subjectAlt	Name	✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKe	yldentifier	✓	False								
	keyldentifier	<b>√</b>			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 bitstring bits).					
Policy Properti es											
keyUsage		✓	True								
	digitalSignature	✓			S	False					
	nonRepudiation	✓			S	True					
	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificate		✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.26					
	policyQualifierI D	✓			S	Id-qt-1 (CPS)					
	qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2					
Qualified	CertificateStat	✓	False								
	QcCompliance (0.4.0.1862.1.1)	✓		М	S	True					
	QcSSCD (0.4.0.1862.1.4)			М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/P DS.pdf					
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign					

#### 1.12.34 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>.

	LuxTrust Smart Card NCP+ Certificate Profile											
Attribut e	Field	IN 54	CE <sup>55</sup>	O/M <sup>56</sup>	CO <sup>57</sup>	Value						
Base Profile												
Version		✓	False									
					S	Version 3 Value = "2"						
SerialNum	nber	✓	False									
					FDV	Validated on duplicates.						
signature	Algorithm	✓	False									
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.						
signature\	Value	✓	False									
					D	Issuing CA Signature.						

 $<sup>^{54}</sup>$  IN = Included: Attribute / field included within the certificate profile.

<sup>&</sup>lt;sup>55</sup> CE = Critical Extension.

 $<sup>^{56}</sup>$  O/M: O = Optional, M = Mandatory.

<sup>&</sup>lt;sup>57</sup> CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



		LuxT	rust Sm	art Card	NCP+ Ce	rtificate Profile
Attribut	Field	IN	CE <sup>55</sup>	O/M <sup>56</sup>	CO <sup>57</sup>	Value
е		54				
Issuer	countryName	<b>✓</b>	False		S S	LU
	commonName	·			S	LuxTrust Global Qualified CA x <sup>1</sup>
	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	organization tanto	<b>✓</b>	False			Editified 6.7 t.
	NotBefore	<b>✓</b>			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 3
01.11						Months
Subject	T	<b>√</b>	False		_	
	serialNumber	✓		M	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 car separated by a "Space" character.
	givenName	<b>√</b>		М	D	PRO and PRIVATE products: Given name(s) a on ID card
	surname	✓		М	D	PRO and PRIVATE products: Surname(s) as o ID card without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	<b>√</b>		М	D	Subject's email address
	emanaduress			IVI		+ *
	title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) of "Professional Administrator" (Other titles possible for special purpos certificates)
	organizationName	<b>✓</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution counts 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 nation 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	<b>√</b>				Public Key: Key length: 2048bit (RSA); publi
Extensi	subjectPublicKey	✓		M		exponent: Fermat-4 (=010001).
Authorit y Properti						
	Keyldentifier	<b>√</b>	False			
•	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified C
						public key
authorityl	nfoAccess	<b>√</b>	False			14 4 0
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation	_ v				http://ca.luxtrust.lu/LTGQCAx.crt



	LuxTrust Smart Card NCP+ Certificate Profile										
Attribut e	Field	IN 54	CE <sup>55</sup>	O/M <sup>56</sup>	CO <sup>57</sup>	Value					
	AccessMethod	<b>\</b>				ld-ad-1					
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/58					
cRLDistrik	outionPoint	✓	False								
	distributionPoint	<b>\</b>			S						
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCAx.crl					
Subject Properti es											
subjectAlt		✓	False								
	Rfc822Name	✓		0	D	Certificate Holder's email address					
subjectKe	yldentifier	<b>√</b>	False								
	keyldentifier	V			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).					
Policy Properti es											
keyUsage		✓	True								
	digitalSignature	✓			S	True					
	nonRepudiation	✓			S	False					
	keyEncipherment	<b>√</b>			S	True					
	dataEncipherment	<b>√</b>	F-1		S	False					
certificate		<b>✓</b>	False			4 2 474 4 4 40 2 27					
	PolicyIdentifier	<b>✓</b>			-	1.3.171.1.1.10.3.27					
	policyQualifierID qualifier	<b>✓</b>			S S	ld-qt-1 (CPS) https://repository.luxtrust.lu					
	policyQualifierID	<b>∨</b>		-	S	Id-qt-2 (User Notice)					
	Policyldentifier	<b>√</b>		1	3	10-41-2 (OSEI NOIICE)					
	1 oneyidentinei	•				0.4.0.2042.1.2					

# 1.12.35 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 Smart Card LORA NCP+ - Signature Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	er	✓	False							
					FDV	Validated on duplicates.				
signatureAl	gorithm	✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	alue	✓	False							
					D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	✓			D	Certificate generation process date/time + <b>36</b> Months				
Subject		✓	False							

<sup>58</sup> SINCE LTGQCA3



	LuxTrust Sn	nart C	ard LOR	RA NCP-	- Sign	ature Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	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	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		М	D	Constructed by LuxTrust
	localityName	<b>✓</b>		М	D	Country of RA
	organizationalUnitNa me 1	<b>√</b>		М	D	RA code Constructed by LuxTrust
	organizationalUnitNa me 2	<b>✓</b>		М	D	RAO code Constructed by LuxTrust
subjectPubl	licKeyInfo Algorithm	<b>✓</b>	False			Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	<b>✓</b>		M		exponent: Fermat-4 (=010001).
Extension s	cuajoon unitro			101		
Authority Propertie s						
authorityKe		<b>✓</b>	False			
	keyldentifier	•				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf		✓	False			
	AccessMethod	<b>✓</b>				Id-ad-2
	accessLocation AccessMethod	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt Id-ad-1
	accessLocation	<b>/</b>				http://qca.ocsp.luxtrust.lu/ <sup>13</sup>
cRLDistribu		· ·	False			nttp://qca.ocsp.iuxtrust.iu/
CKLDISTIBU	distributionPoint	V /	raise		S	
-	fullName	√ ·				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Propertie s						
subjectAltN		✓	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKeyl	dentifier keyldentifier	✓ ✓	False		Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		<b>√</b>	True			
	digitalSignature	✓ ✓	1	1	S	False
	nonRepudiation keyEncipherment	<b>✓</b>	-	-	S S	True False
	dataEncipherment	<b>∨</b>	1	1	S	False
certificatePo		<b>✓</b>	False			1 4100
20	Policyldentifier	√	. 4.00			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)



	LuxTrust Smart Card LORA NCP+ - Signature Certificate Profile									
Attribute	tribute Field IN <sup>9</sup> CE <sup>10</sup> O/M <sup>11</sup> CO <sup>12</sup> Value									
	Policyldentifier         ✓         0.4.0.2042.1.2									

# 1.12.36 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 Sma	rt Caı	d LOR	A NCP+	- authen	tication Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Base Profile						
Version	T	✓	False		_	
		,			S	Version 3 Value = "2"
SerialNumb	er I	✓	False		ED) /	M-Pataday day Parta
signatureAl	gorithm	<b>√</b>	False		FDV	Validated on duplicates.
SignatureAi	Algorithm	•	i aise		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	Aigoniiiii					Encryption.
signatureVa	alue	✓	False			- 71
					D	Issuing CA Signature.
Issuer	<del>,</del>	✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x
37 11 117	organizationName	<b>√</b>			S	LuxTrust S.A.
Validity	NetPetere	<b>✓</b>	False		_	Contitionto gonoration processa detailemen
	NotBefore NotAfter	✓ ✓	1		D D	Certificate generation process date/time.  Certificate generation process date/time + 36 Months
Subject	Notaitei	<b>V</b>	False		D	Certificate generation process date/time + 30 Months
Oubject	serialNumber	✓	1 alse	M	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	✓		М	D	Given name(s) as on ID card
	Surname	✓		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	✓		М	D	"LuxTrust RA Officer"
	organizationName	✓		М	D	Constructed by LuxTrust
	localityName	✓		М	D	Country of RA
	organizationalUnitNa me 1	<b>√</b>		М	D	RA code Constructed by LuxTrust
	organizationalUnitNa me 2	✓		М	D	RAO code Constructed by LuxTrust
subjectPub		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
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			



	LuxTrust Sma	art Cai	d LOR	A NCP+	- authen	tication Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistribu	utionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.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	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificateP		✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.29
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>√</b>			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2

# 1.12.37 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 elD Smart Card QCP-n-qscd Certificate Profile									
Attribute	Field	IN <sup>59</sup>	CE <sup>60</sup>	O/M 61	CO <sup>62</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumb	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False			·				
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	llue	✓	False			Ž,				
					D	Issuing CA Signature.				
Issuer		✓	False		S	<u> </u>				
	countryName	✓			S	LU				
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x <sup>1</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							

 $<sup>^{59}</sup>$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{60}\,\</sup>mathrm{CE}$  = Critical Extension.

 $<sup>^{61}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{62}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	Luxiius	. 0.0	illait o	u. u. u.	, qo	cd Certificate Profile
Attribute	Field	IN <sup>59</sup>	CE <sup>60</sup>	O/M 61	CO <sup>62</sup>	Value
	NotBefore	<b>√</b>			D	Certificate generation process date/time.
	NotAfter	· /			D	Certificate generation process date/time + maximum
	Notation	-				120 Months;
						Certificate generation process date/time + 1 day for
						PSEUDONYM Certificate
Subject		✓	False			
	serialNumber	✓		M	D	Serial Number as constructed by LRAO
						Connectoration of sixon name(a) and symposis
	commonName	✓		M	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 th
	giverilianie	•		IVI		RNCID
						Surname(s) as on ID card without indication "épouse
	Surname	✓		М	D	"ép." or similar and the subsequent name(s) or a
	Carrianic					provided by the RNCID
					_	
	countryName	✓		M	D	LU
	emailAddress	✓		0	D	Subject's email address
	T:u -	<b>√</b>			_	"Directo Domono"
	Title	<b>v</b>		M	D	"Private Person"
	organizationalUnitName	<b>√</b>				If the holder is underage: "Mineur jusqu'à : " & (Date o
	1	·		0	D	birth + 18 years).
subjectPubl	icKevInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extension						
S						
Authority						
Properties	de estifica		Falsa			
authorityKe	keyldentifier	<b>√</b>	False			SHA-1 Hash of the LuxTrust Global Qualified CA
	keyiderililei	•				public key
authorityInfo	Access	<b>√</b>	False			public key
addiontyiii	AccessMethod	✓	1 0.00			ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/13
cRLDistribu	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						
Properties						
subjectAltN		✓	False		_	
	Rfc822Name	✓		0	D	Subject email address
subjectKeyl		<b>√</b>	False		F: 1	T 16 11 17 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 010
						value, followed by the least significant 60 bits of th SHA-1 hash of the value or subjectPublicKey bit strin
						(tag, not including the length and number of unused bit
						string bits).
Policy						g/-
Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓		ļ	S	False
	dataEncipherment	<b>√</b>			S	False
certificatePo		✓	False			10.474.4.40.000
	PolicyIdentifier	✓		<u> </u>		1.3.171.1.10.3.30
	policyQualifierID Qualifier	✓ ✓		-	S	Id-qt-1 (CPS)
	Qualifier policyQualifierID	<b>✓</b>		<b> </b>	S S	https://repository.luxtrust.lu Id-qt-2 (User Notice)
	viaiiieiii		ĺ	ĺ	ာ	10-41-2 (USEI NULLE)
		/				
	Policyldentifier	<b>✓</b>				0.4.0.194112.1.2
		<b>√</b>				0.4.0.194112.1.2



	LuxTrust elD Smart Card QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>59</sup>	CE <sup>60</sup>	O/M 61	CO <sup>62</sup>	Value					
	QcCompliance (0.4.0.1862.1.1)	<b>~</b>		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	<b>~</b>		М	S	True					
	QcPDS (0.4.0.1862.1.5)	<b>✓</b>		М	S	https://www.luxtrust.lu/upload/data/repository/P DS.pdf					
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign					

#### 1.12.38 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>.

	LuxTr	ust eID	Smart o	ard N	CP+ Ce	rtificate Profile
Attribute	Field	IN <sup>63</sup>	CE <sup>64</sup>	O/M 65	CO <sup>66</sup>	Value
Base Profile						
Version	<u>-</u>	✓	False			
					S	Version 3 Value = "2"
SerialNumb	per	✓	False		==>/	
-1	l	<b>✓</b>			FDV	Validated on duplicates.
signatureA		V	False		0	OID #4.0.040.440540.4.4.4# OI IA050*!! DOA
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureV	alue	✓	False			
•					D	Issuing CA Signature.
Issuer	a a contro Alama	<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	T	✓	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	✓	1 0.00	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	<b>√</b>		0	D	Subject's email address
	Title	<b>√</b>		М	D	"Private Person"

 $<sup>^{63}</sup>$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{64}</sup>$  CE = Critical Extension.

 $<sup>^{65}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{66}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	LuxTru	st eID	Smart o	card N	CP+ Ce	rtificate Profile
Attribute	Field	IN <sup>63</sup>	CE <sup>64</sup>	O/M 65	CO <sup>66</sup>	Value
	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 (=010001).
Extension s						
Authority Properties						
authorityKe		✓	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInf		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistribu		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properties						
subjectAltN	ame	✓	False			
	Rfc822Name	✓		0	D	Subject email address
subjectKeyl	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			
<u></u>	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificateP		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.31
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>√</b>				0.4.0.2042.1.2

## 1.12.39 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>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNuml	oer	✓	False							
					FDV	Validated on duplicates.				
signatureA	Igorithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.				
signatureV	alue	✓	False							



	LuxTrust	Signin	ıg Serv	er QCP	-n-qscd	l Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	<b>√</b>			S	LuxTrust Global Qualified CA x
Validit.	organizationName	<b>√</b>	F-1		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Contificate generation process data/time
	NotAfter	<b>√</b>			D	Certificate generation process date/time.  Certificate generation process date/time + 36  Months
subject		<b>√</b>	False			Worth
	serialNumber	<b>√</b>	. 4.00	М	D	Serial Number as constructed by LRAO
	Serialivullibei			IVI	D	<u> </u>
	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	<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:
	title	<b>√</b>		М	D	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)
	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	<b>√</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPub		✓	False			
_	algorithm	<b>✓</b>				Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
Extension s Authority						
Propertie s						
authorityKe	evldentifier	<b>/</b>	False			
	keyldentifier	1	. 4.50			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf	foAccess	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt



	LuxTrus	t Signir	ıg Serv	er QCF	-n-qsc	d Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistrib	utionPoint	✓	False			
01122101110	distributionPoint	<b>✓</b>	. 4.00		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx-yy <sup>67</sup> .crl
Subject Propertie s						in the state of th
subjectAltN	lame	✓	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 of subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		✓	True			
	digitalSignature	<b>~</b>			S	False
	nonRepudiation				S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	✓			S	False
certificateP		✓	False			
	Policyldentifier	<b>~</b>				1.3.171.1.1.10.3.32
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2
QualifiedCe	ertificateStat	✓	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>		M	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf
	QcType (0.4.0.1862.1.6)	<b>*</b>		M	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)

## 1.12.40 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.

LuxTrust Signing Server QCP-I-qscd Certificate Profile									
Attribute	Attribute Field IN <sup>9</sup> CE <sup>10</sup> O/M <sup>11</sup> CO <sup>12</sup> Value								
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNum	SerialNumber   ✓ False								
					FDV	Validated on duplicates.			

 $<sup>^{67}</sup>$  X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

YY are the last two digits of the corresponding OID



A ( ( . ! )			_			Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup> False	O/M <sup>11</sup>	CO <sup>12</sup>	Value
signatureA	algorithm	•	raise		S	OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.
signatureV	alue	✓	False			71
					D	Issuing CA Signature.
Issuer	e e un tru Alema	✓ ✓	False		S	
	countryName commonName	<b>∨</b>			S	LU LuxTrust Global Qualified CA x
	organizationName	· ✓			S	LuxTrust S.A.
Validity	ga <u>-</u> a	<b>√</b>	False		J	
•	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 12, 24
		<b>√</b>	False			Months
subject			False		_	
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>✓</b>		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	<b>✓</b>		М	D	the country in which the subject (legal person) is established (ISO3166)
	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 entitiy when the identifier is provided by the legal entitity 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).
	organizationalUnitNa me 1	✓		0	D	Company/institution department or othe information item
	organizationalUnitNa me 2	✓		0	D	Company/institution department or othe information item
subjectPub		<b>√</b>	False			Dublin Kon Kon I il in 1999 il il il il il il il il il il il il il
	algorithm	✓ ✓		M		Public Key: Key length: up to 4096 bit (RSA) public exponent: Fermat-4 (=010001).
Extensio	subjectPublicKey	V		IVI		public expolient.
ns Authority Propertie s						
authorityKe		<b>√</b>	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified C/
authoritylni	inArress	<b>✓</b>	False			public key
autitorityilli	AccessMethod	<b>V</b> ✓	i aise			Id-ad-2
				•	ī	14 44 <u>-</u>
	accessLocation	<b>✓</b>				http://ca.luxtrust.lu/LTGQCAx.crt



	LuxTrus	st Sign	ing Ser	ver QC	P-I-qscd	l Certificate Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/13
cRLDistrib	utionPoint	✓	False			
	distributionPoint	<b>✓</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx-yy.crl
Subject Propertie s						
subjectKey		<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 Propertie s						
keyUsage		✓	True			
	digitalSignature	~			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateF		✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.33
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	<b>√</b>				0.4.0.194112.1.3
BasicCons	traints					
	CA	✓			S	FALSE
	pathLenConstraint	✓			S	0 (ZERO)
QualifiedCo	ertificateStat	✓	False			
,	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

### 1.12.41 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>.

	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribut e	Field	IN <sup>68</sup>	CE <sup>69</sup>	O/M <sup>70</sup>	<b>CO</b> 71	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								

 $<sup>^{68}\,\</sup>mathrm{IN}$  = Included: Attribute / field included within the certificate profile.

 $<sup>^{69}</sup>$  CE = Critical Extension.

 $<sup>^{70}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{71}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	LuxT	rust S	Sianina	Stick Q	CP-n-c	qscd Certificate Profile
Attribut e	Field	IN <sup>68</sup>	CE <sup>69</sup>	O/M <sup>70</sup>	CO 71	Value
oi an oturo	A lara vith va	<b>√</b>	Falsa		FDV	Validated on duplicates.
signature	Algorithm	•	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature\	/alue	✓	False		D	Jacobing CA Signature
Issuer		✓	False		S	Issuing CA Signature.
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>1</sup>
Validity	organizationName	✓ ✓	False		S	LuxTrust S.A.
validity	NotBefore	· ✓	i aise		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36 Months
Subject	T	✓	False		_	
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<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	✓		М	D	PRO and PRIVATE products: Given name(s) as on ID card
	surname	✓		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	<b>✓</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>✓</b>		М	D	PRO products only:  Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	<b>~</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no VAT 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	<b>✓</b>	False			Public Koyr Koy longth, 2049hit /DCA million and
	Algorithm subjectPublicKey	<b>✓</b>		M		Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extensi						
ons Authorit						
y Properti						
es	 Keyldentifier	<b>√</b>	False			
addiontyr	keyldentifier	<b>→</b>	1 0100			SHA-1 Hash of the LuxTrust Global Qualified CA public
	-					key



	LuxT	rust S	igning	Stick Q	CP-n-c	qscd Certificate Profile
Attribut e	Field	IN <sup>68</sup>	CE <sup>69</sup>	O/M <sup>70</sup>	<b>CO</b> 71	Value
authorityli	nfoAccess	<b>✓</b>	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>72</sup>
cRLDistrik	outionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject Properti es						
subjectAlt		✓	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKe	yldentifier	✓	False		F: '	T1 1/2 11 0/2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	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 Properti es						
keyUsage		✓	True		_	
	digitalSignature	✓			S	False
	nonRepudiation	<b>√</b>			S	True
	keyEncipherment	<b>√</b>			S	False
	dataEncipherment	<b>√</b>			S	False
certificate		<b>√</b>	False			40.474.4.40.004
	Policyldentifier	✓ ✓			_	1.3.171.1.10.3.34
	policyQualifierI D	<b>V</b>			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>√</b>				0.4.0.194112.1.2
QualifiedC	CertificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	<b>√</b>		М	S	True
	QcSSCD (0.4.0.1862.1.4)			М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	<b>√</b>		М	S	id-etsi-qct-esign

## 1.12.42 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 1.3.171.1.10.3.35>.

LuxTrust proprietary and confidential

<sup>72</sup> SINCE LTGQCA3



	L	uxTr	ust Sigr	ning Stick	NCP+ Ce	ertificate Profile
Attribut e	Field	IN 73	CE <sup>74</sup>	O/M <sup>75</sup>	CO <sup>76</sup>	Value
Base Profile						
Version		<b>✓</b>	False			
7 01 01011			1 0.00		S	Version 3 Value = "2"
SerialNum	nber	✓	False			
					FDV	Validated on duplicates.
signature		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 wit RSA Encryption.
signature	Value	✓	False			
					D	Issuing CA Signature.
Issuer	1	✓	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 + 3
Subject		<b>√</b>	False			Months
Gubject			i aise		_	0.114.1
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	✓		М	D	PRO and PRIVATE products: Concatenation of given name(s) and surname(s) as on ID car separated by a "Space" character.
	givenName	✓		М	D	PRO and PRIVATE products: Given name(s) a on ID card
	surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as of ID card without indication "épouse", "ép." or similal 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	le 🗸		М	D	"Professional Person" (default) ("Professional Administrator"
						(Other titles possible for special purpos certificates)
						PRO products only:
	organizationName	✓		М	D	Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	✓		М	D	PRO products only: Company/institution countr of HQ (as in articles of association)
	organizationalUnit Name 1	<b>✓</b>		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products:  Company/Institution VAT number (or if no 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).

 $<sup>^{73}</sup>$  IN = Included: Attribute / field included within the certificate profile.

 $<sup>^{74}</sup>$  CE = Critical Extension.

 $<sup>^{75}</sup>$  O/M: O = Optional, M = Mandatory.

 $<sup>^{76}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.



	L	uxTr	_	ning Sticl	NCP+ Ce	rtificate Profile
Attribut e	Field	IN 73	CE <sup>74</sup>	O/M <sup>75</sup>	CO <sup>76</sup>	Value
	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); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensi ons						
Authorit y Properti es						
authorityK	Ceyldentifier	✓	False			
	keyldentifier	<b>V</b>				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityli		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	<b>√</b>				ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>77</sup>
cRLDistrik	outionPoint	<b>√</b>	False			
	distributionPoint fullName	<b>√</b>			S	http://ed.houteset.hu//TOOOA.com/
Subject	tuliname	· ·				http://crl.luxtrust.lu/LTGQCAx.crl
Properti es						
subjectAlt	Name	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKe		✓	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properti es						
keyUsage		✓	True			
	digitalSignature	<b>√</b>			S	True
	nonRepudiation	<b>√</b>			S	False
	keyEncipherment	<b>√</b>			S	True
	dataEncipherment	<b>✓</b>	Гаја		S	False
certificate		<b>✓</b>	False			4 2 474 4 4 40 2 25
	Policyldentifier policyQualifierID	<b>∨</b>			S	1.3.171.1.10.3.35 Id-qt-1 (CPS)
	qualifier	<b>∨</b>			S	https://repository.luxtrust.lu
	policyQualifierID	<b>V</b>			S	Id-qt-2 (User Notice)
	Policyldentifier	<b>√</b>			<u> </u>	0.4.0.2042.1.2

## 1.12.43 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	Attribute Field IN9 CE10 O/M11 CO12 Value									
Base										
Profile										

<sup>77</sup> SINCE LTGQCA3



	Adva	ance	d eSea	I - LCP	Certif	ficate Profile
Attribute	Field	IN <sub>9</sub>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
Version		<b>√</b>	False			
					S	Version 3 Value = "2"
SerialNumb	er	<b>✓</b>	False			
					FDV	Validated on duplicates.
signatureAl	gorithm	<b>✓</b>	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256 with
						RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer		<b>✓</b>	False		S	
	countryName	<b>✓</b>			S	LU
	commonName	<b>✓</b>			S	LuxTrust Global Qualified CA x
	organizationName	<b>✓</b>			S	LuxTrust S.A.
Validity		<b>√</b>	False			
	NotBefore	<b>✓</b>			D	Certificate generation process date/time.
	NotAfter	<b>✓</b>			D	Certificate generation process date/time + 12, 24
						Months
subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	<b>√</b>		М	D	Shall contain the full registered name of the subject (legal person).
	countryName	<b>✓</b>		М	D	the country in which the subject (legal person) is established (ISO3166)



Attribute Field INº CE¹º O/M¹¹ CO¹² Value  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 are 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 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 entitity or LU when the identifier is provided by LuxTrust.
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 are 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 entitity or LU when the identifier is
organizationName ✓ M D Shall contain the full registered name of the subject (legal person).
organizationalUnitNam e 1  O D Company/institution department or oth information item
organizationalUnitNam e 2  D Company/institution department or oth information item
subjectPublicKeyInfo False
algorithm Public Key: Key length: up to 4096 bit (RS.
subjectPublicKey   M public exponent: Fermat-4 (=010001).
Extension s
Authority
Properties



	Ad	vance	a esea	II - LCF	Certi	ficate Profile
Attribute	Field	IN <sub>9</sub>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInf	oAccess	<b>✓</b>	False			
	AccessMethod	~				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ <sup>13</sup>
cRLDistribu	rtionPoint	~	False			
	distributionPoint	<b>✓</b>			S	
	fullName	<b>✓</b>				http://crl.luxtrust.lu/LTGQCA.crl
Subject						
Properties						
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 o
						subjectPublicKey bit string (tag, not including the
						length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		<b>✓</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation	<b>✓</b>			S	False
	keyEncipherment	<b>✓</b>			S	False
	dataEncipherment	<b>✓</b>			S	False
certificateP	-	✓	False			
	Policyldentifier	<b>✓</b>				
	,					1.3.171.1.1.10.3.36
	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

### 1.12.44 LuxTrust Corporate LCP Certificate Profile

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



LuxTrust Corporate LCP Certificate Profile – Corporate CA								
Attribute	Field	IN¹ 8	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value		
Base Profile								
Version		<b>√</b>	False					
					S	Version 3 Value = "2"		
SerialNumber		<b>√</b>	False					
					FDV	Sequential CSN		
signatureAlgo	rithm	<b>√</b>	False					
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with RSA Encryption.		
signatureValu	e	<b>√</b>	False					
					D	Issuing CA Signature.		
Issuer		<b>√</b>	False		S			
	countryName	<b>~</b>			S	LU		
	commonName	<b>√</b>			S	LuxTrust Corporate CA x		
	organizationName	<b>√</b>			S	LuxTrust S.A.		
Validity		<b>√</b>	False					
	NotBefore	<b>~</b>			D	Certificate generation process date/time.		
	NotAfter	<b>√</b>			D	Certificate generation process date/time + 36 Months		
Subject		<b>~</b>	False					
	serialNumber	<b>√</b>		М	D	Serial Number as constructed by LRAO		
	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		



	LuxTrust C	orpora	ite LCP C	ertificate P	rofile – C	orporate CA
Attribute	Field	IN¹ 8	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	Surname	<b>√</b>		М	D	PRO and PRIVATE products: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	Title	<b>√</b>		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	<b>√</b>		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)
	organizationalUnitName 1			M for PRO prod., conditional (O) for PRIV prod	D	PRO products: Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) PRIVATE products: If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitName 2	<b>√</b>		0	D	PRO products only:  Company/institution department or other information item
subjectPublicKe	eyInfo	<b>√</b>	False			
	Algorithm					Public Key: Key length: 2048 bit up to 4096
	subjectPublicKey	<b>√</b>		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKeylde	ntifier	<b>√</b>	False			



	orporate CA					
Attribute	Field	IN¹ 8	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
	keyldentifier	<b>*</b>				SHA-1 Hash of the LuxTrust <b>Corporate</b> CA public key
authorityInfoAccess		<b>√</b>	False			
	AccessMethod	<b>√</b>				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTCCAx2.crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	<b>√</b>				http://cca.ocsp.luxtrust.lu/ <sup>23</sup>
cRLDistributionPoint		<b>√</b>	False			
	distributionPoint	<b>√</b>			S	
	fullName	<b>√</b>				http://crl.luxtrust.lu/LTCCAx <sup>22</sup> .crl
Subject Properties						
subjectAltName		<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	N/A
subjectKeylde	ntifier	<b>√</b>	False			
	keyldentifier	<b>√</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		<b>√</b>	True			
	digitalSignature	<b>✓</b>			S	True
	nonRepudiation	<b>✓</b>			S	False
	keyEncipherment	<b>√</b>			S	False



	LuxTrust Corporate LCP Certificate Profile – Corporate CA										
Attribute	Field	IN <sup>1</sup> 8	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value					
	dataEncipherment	✓			S	False					
certificatePolicie	es	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.4.1					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	Policyldentifier	<b>√</b>				0.4.0.2042.1.3					

## 1.13 Timestamping Certificate Profile

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

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

LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</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	llue	✓	False						
					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust Global Timestamping CA x			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			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			



	LuxTru	ist Time	estampi	ng Cert	ificate I	Profile
Attribute	Field	IN <sup>9</sup>	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value
subjectPubli		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrust
						Timestamping CA public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	<b>√</b>				http://ca.luxtrust.lu/LTGTSACAx.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistribut		<b>√</b>	False		_	
	distributionPoint	<b>√</b>			S	
	fullName	✓				http://crl.luxtrust.lu/LTGTSACAx.crl
Subject						
Properties			<u> </u>			
subjectAltNa		<b>√</b>	False			
	Rfc822Name	<b>√</b>		0	D	info@luxtrust.lu
subjectKeylo	dentifier 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 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		✓	False			
	TimeStamping (1.3.6.1.5.5.7.3.8)	<b>✓</b>			S	Set
Private Key I	Usage Period	✓	False			
	Usage period (2.5.29.16)	~		М	D	Certificate generation process date/time + 12 Months
certificatePo	licies	✓	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.8.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	<b>✓</b>				LuxTrust LCP certificate compliant with ETSI TS 102 042. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority.
	Policyldentifier	<b>√</b>	+	+	<b>.</b>	0.4.0.2042.1.3

# 1.13.1 Normalized Certificate Policy for LuxTrust Qualified Timestamping

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



Normalized Certificate Policy for LuxTrust Qualified Timestampling   Normalized Certificate		Normalized (	Cortific	ata Poli	cy for Li	vTruet (	Qualified Timestamping
SerialNumber	Attribute						
Version   Vers		Ju		02	C/141	- 00	74140
SerialNumber							
Serial Number	Version		✓	False			
signatureValue						S	Version 3 Value = "2"
SignatureAlgorithm	SerialNumbe	r	✓	False			
						FDV	Validated on duplicates.
signatureValue	signatureAlg	orithm	✓	False			
signature/Value		algorithm				S	
issuer	oiamatura\/al	•	./	Folso			RSA Encryption.
CountryName	signatureval	ue	· ·	raise		_	Issuing CA Signature
CountryName	issuar		1	False			Issuing CA Signature.
CommonName	ISSUEI	countryName		i aise			111
Validity			<b>√</b>				_
Validity			✓				
NotAfter	Validity		✓	False			
subject  organizationIdentifier (2.5.4.97)  commonName organizationName ountryMame ountr		NotBefore	✓			D	
subject  organisationIdentifier (25.4.97)  commonName (7 M D LuXTrust Qualified Timestamping organizationName (8 M D LuXTrust Qualified Timestamping organizationName (9 M D LuXTrust Qualified Timestamping organizationName (9 M D LuXTrust Qualified Timestamping organizationName (9 M D LuXTrust Qualified Timestamping organizationName (9 M D LuXTrust Qualified Timestamping organizationName (9 M D LuXTrust Qualified Timestamping (125.4.97)  LuXTrust Qualified Timestamping (126.4.97)  LuXTrust Qualified Timestamping  LuXTrust Qualified Timestamping		Not After	1			ם	
OrganisationIdentifier (2.6.4.97)   CommonName organizationName organiza		Notaitei					Months
C.2.5.4.97	subject		✓	False			
C.2.4.9/)			✓		М	D	VATLU-20976985
OrganizationName			./				
CountryName							
SubjectPublicKeyInfo							
algorithm subjectPublicKey	subjectPubli	cKevinfo		Falso	IVI	U	LO
SubjectPublicKey   V	Subjecti ubii			i aisc			Public Key: Key length: up to 4096 bit (RSA)
Authority Properties authorityInfoAccess  ReyIdentifier AccessMethod A			<b>✓</b>		М		
Authority   Properties   authorityReyIdentifier	Extensions				.,,		pasie experient i emat i ( e rece i).
Reyldentifier	Authority Properties						
authorityInfoAccess    AccessMethod	authorityKey	Identifier		False			
AccessMethod accessLocation							SHA-1 hash of the LuxTrust Global Qualified CA
CREDistributionPoint   AccessMethod   AccessMethod   AccessLocation   AccessMethod	authorityInfo			False			
AccessMethod accessLocation   V							
accessLocation							
CRL Distribution Point   V   False   S							
distributionPoint fullName	a DI Diatribut			Falsa			nttp://qca.ocsp.luxtrust.lu/
Full   Subject   Full	CKLDISTIBUT			raise		-	
Subject Properties subjectAltName						3	http://crl luxtruet.lu/LTGOCAx.vvv.crl
Properties   SubjectAltName	Subject	Tullivallie	•				nttp://cm.tuxtrust.tu/ETGQCAx.yy.cn
Rfc822Name   V   False   D   Info @luxtrust.lu							
SubjectKeyldentifier		me	✓	False			
SubjectKeyldentifier		Rfc822Name	✓		0	D	info@luxtrust.lu
Reyldentifier   V	subjectKeylo	lentifier	✓	False			
Properties		keyldentifier	<b>✓</b>			Fixed	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
Marcon   M							
digitalSignature			,	т.			
nonRepudiation	кеуUsage	digitalCianatura		True			True
ReyEncipherment   V							
Certificate Policies   Certificate PolicyQualifier   Certificate Generation process date/time + 24   Months   Certificate Generation Process date					<del>                                     </del>		
Extended Key Usage					<del>                                     </del>		
TimeStamping (1.3.6.1.5.5.7.3.8)  Private Key Usage Period  Usage period (2.5.29.16)  CertificatePolicies  PolicyIdentifier policyQualifierID qualifier policyQualifierID qualifier policyQualifierID qualifier	Extended Ke			True			1 4100
Certificate Policies   PolicyQualifier   Polic				.100		_	
Private Key Usage Period  Usage period (2.5.29.16)  Certificate Policies  Policy Qualifier Policy Qualifier Signal Figure 1			<b> </b>			S	Set
Usage period (2.5.29.16)  certificatePolicies  PolicyIdentifier policyQualifierID qualifier policyQualifierID policyQualifierID policyQualifierID policyQualifierID Sid-qt-1 (CPS) qualifier policyQualifierID Sid-qt-2 (User Notice)	Private Key l		✓	False			
(2.5.29.16)			./		B 4	_	Certificate generation process date/time + 24
PolicyIdentifier     ✓     1.3.171.1.1.10.3.18       policyQualifierID     ✓     S     Id-qt-1 (CPS)       qualifier     ✓     S     https://repository.luxtrust.lu       policyQualifierID     ✓     S     Id-qt-2 (User Notice)		(2.5.29.16)			IVI	U	,
policyQualifierID     ✓     S     Id-qt-1 (CPS)       qualifier     ✓     S     https://repository.luxtrust.lu       policyQualifierID     ✓     S     Id-qt-2 (User Notice)	certificatePo			False			
qualifier     ✓     S     https://repository.luxtrust.lu       policyQualifierID     ✓     S     Id-qt-2 (User Notice)		Policyldentifier					
policyQualifierID   ✓ S Id-qt-2 (User Notice)							Id-qt-1 (CPS)
						S	https://repository.luxtrust.lu
<b>PolicyIdentifier</b>   ✓   0.4.0.2042.1.2						S	
		Policyldentifier	<b>√</b>				0.4.0.2042.1.2



#### 1.13.2 Qualified Timestamping Certificate Profile

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

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

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

		ficate P			
Field	IN 9	CE1 0	O/M1 1	CO1 2	Value
		T-I-			
	<b>V</b>				
		C		S	Version 3 Value = "2"
er	<b>√</b>	Fals			
		е			
				FDV	Validated on duplicates.
gorithm	✓	Fals			·
		е			
algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
					Encryption.
alue	✓	Fals			
		е			
					Issuing CA Signature.
	✓	Fals		S	
		е			
					LU
			ļ	_	LuxTrust Global Qualified CA x
organizationName				S	LuxTrust S.A.
	✓				
NetDefere	./	е		<u> </u>	Certificate generation process date/time.
NotAfter		Folo		U	Certificate generation process date/time + 60 Months
	•				
organisationIdentifi		E			
				_	VATLU-20976985
o.	<b>~</b>		M	D	7/1/20 2007 0000
(2.5.4.97)					
, ,	_				
commonName	<b>V</b>		M	טן	LuxTrust Qualified Timestamping
organizationName	✓		М	D	LuxTrust S.A.
countryName	✓		М	D	LU
licKeyInfo	✓	Fals			
		е			
	✓				Public Key: Key length: up to 3072 bit (RSA)
subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
vldentifier	<b>√</b>	Fals			
,					
keyldentifier	<b>✓</b>				
• · · · · · · · · · · · · · · · · · · ·					SHA-1 hash of the LuxTrust Global Qualified CA
oAccess	✓	Fals			20 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
		е			
AccessMethod	✓				Id-ad-2
			ì	1	1
accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	<b>√</b>				http://ca.luxtrust.lu/LTGQCAx.crt Id-ad-1
	gorithm algorithm algorithm algorithm countryName commonName organizationName NotBefore NotAfter  organisationIdentifier (2.5.4.97) commonName organizationName countryName licKeyInfo algorithm subjectPublicKey  yldentifier keyIdentifier	Field IN 9  Field	Field  IN CE1 9 0  Fals e  gorithm  alue  Fals e  algorithm  Alue  Fals e  CountryName commonName organizationName  V Fals e  CountryName  CommonName  OrganizationIdentifi er  (2.5.4.97)  CommonName  OrganizationName  V Fals e  Fals e	Field  IN CE1 O/M1  Fals e  ger  Fals e  gorithm  Alue  Fals e  Fals e  Fals e  Fals e  CountryName commonName organizationName  Fals e  NotBefore NotAfter  V Fals e  NorganisationIdentifier  Fals e  NorganizationName  Fals e  NorganizationName  Fals e  NorganizationName  Fals e  NorganizationName  Fals e  M  Gammania M  M  M  M  M  M  M  M  M  M  M  M  M	S



						Trust Qualified Timestamping
Attribute	Field	IN	CE1	O/M1	CO1	Value
		9	0	1	2	
cRLDistrib	utionPoint	✓	Fals			
			е			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						
Propertie						
s						
subjectAltN	Name	✓	Fals			
•			е			
	Rfc822Name	✓		0	D	info@luxtrust.lu
subjectKey		<b>✓</b>	Fals			
,,			е			
	keyldentifier	<b>√</b>	-		Fixe	The Key Identifier comprises a four-bit field with a 0100
	,				d	value, followed by the least significant 60 bits of the
					_	SHA-1 hash of the value or subjectPublicKey bit string
						(tag, not including the length and number of unused bit-
						string bits).
Policy						ouring who).
Propertie						
S						
keyUsage		<b>1</b>	True			
Reyosage	digitalSignature	1	Truc		S	True
	nonRepudiation	· /			S	False
	keyEncipherment	· /			S	False
	dataEncipherment	<b>V</b> ✓			S	
Extended k		<b>V</b> ✓	T		5	False
Extended r	TimeStamping	V /	True			0-1
		<b>V</b>			S	Set
D: 11	(1.3.6.1.5.5.7.3.8)					
Private Key	/ Usage Period	✓	Fals			
		1	е			
	Usage period	<b>✓</b>		M	D	Certificate generation process date/time + 12 Months
	(2.5.29.16)					
certificateP	Policies	✓	Fals			
	T =		е			
	Policyldentifier	<b>√</b>			<u> </u>	1.3.171.1.10.3.19
	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
certificateP	Policies	✓				
	QcType	<b>✓</b>		М	S	id-etsi-qct-eseal
	(0.4.0.1862.1.6)					(0.4.0.1862.1.6.2)
	,					, ,
	QcCompliance	✓		М	S	True
	(0.4.0.1862.1.1)					
	QcPDS	<b>√</b>		М	S	https://www.luxtrust.lu/upload/data/repository/GTC_F_v2
		1		l	-	
	(0.4.0.1862.1.5)					_4.pdf

### 1.13.3 TimeStamp Request and Response Format

## 1.13.3.1 TimeStamp Request Format

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

	LuxTrust Time Stamp Request
Field	Value / comment
Document Hash	Hash of the document on which the TimeStamp must be computed
Hash OID	(SHA-256/SHA-512)  Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.



LuxTrust Time Stamp Request							
Field	Value / comment						
Policy OID	1.3.171.1.1.10.3.18.1  The OID of the policy that should be applied by the TTS during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp. The developer has to ensure that the specified policy is available on the TTS; otherwise the returned token will include a policy identifier that is not defined by LuxTrust.						
Nonce	A random number, also referred to as "nonce", allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.						
Should TSA Certificate be included?	TRUE/FALSE						
Request Extensions	Value *						
None	None						

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

## 1.13.3.2 TimeStamp Response Format

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

LuxTrust Time Stamp Response							
Field	Value / comment						
Generation Time	The time at which the time-stamp token has been created by the TSA. It is expressed as U 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

### 1.14 Certificate extensions

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



### 1.15 Algorithm object identifiers

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

#### 1.16 Name forms

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

#### 1.17 Name constraints

Name constraints are supported as per RFC 5280.

## 1.18 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

### 1.19 Usage of Policy Constraints extension

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

### 1.20 Policy qualifiers syntax and semantics

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

## 1.21 Processing semantics for the critical Certificate Policies

Not applicable.

### 1.22 CRL profile

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

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

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

LuxTrust CRL Profile							
Field	Comments						
Version	v2						
Signature	Same signature algorithm as related CA						
Issuer	<subjectca></subjectca>						
thisUpdate	<creation time=""></creation>						
nextUpdate	<pre><creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" qualified="" subordinate="" time=""></creation></creation></pre>						
	<pre><creation (8="" +="" 30="" 8,5="" and="" cas="" for="" hours="" minutes)="" ssl="" subordinate="" time=""> <creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></creation></pre>						
revokedCertificates							
userCertificate	<pre><certificate number="" serial=""></certificate></pre>						
revocationDate	<revocation time=""></revocation>						





LuxTrust CRL Profile						
Field	Comments					
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></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>					
authorityKeyldentifier	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>						
	<creation (8="" +="" 30="" 8,5="" and="" for="" hours="" minutes)="" p="" subordinate<="" time=""></creation>						
	SSL CAs>						
	<pre><creation +="" 24="" cas="" for="" hours="" other="" subordinate="" time=""></creation></pre>						
revokedCertificates							
userCertificate	<pre><certificate number="" serial=""></certificate></pre>						
revocationDate	<revocation time=""></revocation>						
crlEntryExtensions							
reasonCode	<insert code="" list="" of="" reason="" revocation="" used=""></insert>						
crlExtensions							
cRLNumber	Non-critical <subject ca="" identifier="" key=""></subject>						
authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>						
IssuingDistributionPoint	<pre><distributionpoint> http://crl.test.luxtrust.lu/LTTGQCAx-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.

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	<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>					





LuxTrust Complete CRL Profile				
Field		Comments		
	authorityKeyIdentifier	Non-critical <ca assigned="" number="" unique=""></ca>		

### 1.22.1 Version number(s)

See section 3.4.

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

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

## 1.22.2 CRL entry extensions

See section 3.4.

### 1.23 OCSP profile

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

### 1.23.1 Version number(s)

See section 3.5.

#### 1.23.2 OCSP extensions

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

LuxTrust OCSP Certificate Profile						
Attribute	Field	IN18	CE19	O/M20	CO21	Value
Base Profile						
Version			False			
					S	Version 3 Value = "2"
SerialNumbe	er		False			
					FDV	Validated on duplicates.
signatureAlg	gorithm		False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue		False			
					D	Issuing LTGRCA Signature
issuer			False		S	
	countryName				S	LU
	commonName				S	LuxTrust Global Root x
	organizationName				S	LuxTrust S.A.
Validity			False			
	NotBefore				D	Certificate generation process date/time.
	NotAfter				D	Certificate generation process date/time + maximum 12 Months
subject			False			
	countryName			M	D	LU
	organizationName			М	D	LuxTrust S.A.
	organizationalUnitName 1			0	D	Pki entity
	commonName			M	D	LuxTrust S.A. OCSP Server 2
subjectPubl	icKeyInfo		False			
	algorithm					Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey			М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	yldentifier		False			
	keyldentifier					SHA-1 Hash of the LuxTrust LTGR x CA public key

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





LuxTrust OCSP Certificate Profile						
Attribute	Field	IN18	CE19	O/M20	CO21	Value
id-ocsp-noch	id-ocsp-nocheck		False			
					S	NULL
Subject Properties						
subjectKeylo	dentifier		False			
	keyldentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
	nonRepudiation				S	False
	keyEncipherment				S	False
	dataEncipherment				S	False
certificatePo	licies		False			
	Policyldentifier					1.3.171.1.1.1.1.0.1.0
	policyQualifierID				S	Id-qt-1 (CPS)
	qualifier				S	https://repository.luxtrust.lu
	policyQualifierID				S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText					LuxTrust S.A. Online Certificate Status Server. IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported.
	Policyldentifier					0.4.0.2042.1.3
Extended Ke	Extended Key Usage		False			
	OCSPSigning				S	True

## 1.24 Integration certificates

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)}.