

Version number: 1.28 Publication Date: 20/07/2018 Effective Date: 03/08/2018

> LuxTrust S.A IVY Building | 13-15, Parc d'activités | L-8308 Capellen Luxembourg | VAT LU 20976985 | RCS B112233 Business Number N°00135240/0 Phone: +352 26 68 15 – 1 Fax: +352 26 68 15 – 789



Copyright © 2017 – All rights reserved



### **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
			<ul> <li>Modification of the CRL issuance algorithm (SHA256 to SHA1)</li> </ul>
1.05	MSC	19/03/2012	Modifications following review by Chris Quaresimin and Laurent Breuskin:         • Removal of + Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime for non-SSL products         • Display text for CSS integration product         • Correct CRL and AIA for CSS integration product
			SSL Object certificate profile
1.06	MSC	26/03/2012	Modifications for CSS certificates, signature will be performed using SHA1WithRsa. Changes performed in CSS certificate profile for prod and integration, page 43 and 51.
1.07	MSC	14/06/2012	Added: TimeStamping CA and TimeStamping certificate profile
1.08	MSC	29/06/2012	Added: Private key usage Period in TSP
1.09	LBR	01/08/2012	Added: Certificate Profiles under LuxTrust Global Qualified CA
			SC LORA & LRS Certificate Modified:     Table for OIDs & LuxTrust CA Hierarchy
1.09.1	LBR	02/08/2012	Update of OID Page 22
1.09.2	MSC	07/08/2012	Added: Certificate profile for Extended Validation Certificates : • EVCP – ETSI TS 102 042 • EVCP+ - ETSI TS 102 042 Added: Certificate profile for Secure Online File Exchange (SOFiE)
1.10	YNU	23/08/2012	Review for validation of CP
1.10	CSPBoard	24/08/2012	Validation
1.11	CSPBoard	20/09/2012	Typo update
1.12	YNU TKO	21/12/2012	<ul> <li>Added CP SSL/TLS Certificate for Client Authentication</li> <li>Added CP non SSCD NCP+ Certificates supporting Advanced Electronic Signatures for Mass Signature Services</li> <li>Various syntactical and format corrections</li> </ul>
1.13	CSP Board	23/04/2013	insertion of ILNAS logo including accreditation reference and technical standards reference
1.14	YNU	29/11/2013	Update specific requirements for CP under the SSL CA
1.15	YNU	18/01/2014	Clarification on Mozilla request
1.16	YNU	05/06/2014	Update Cp - for LuxTrust Global Root Renew - QcS2 et QcS3 - Typo Add CP Seal Signature Services
1.17	YNU	30/06/2014	Add certificate profile for eID • 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		44/44/0044	Unders AIA is OD we dear the OOL OA sizes 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	<ul> <li>Add:</li> <li>LuxTrust Qualified Timestamping Certificate profile with QC statements</li> <li>SPARE LuxTrust Signing Server LCP Certificate Profile</li> <li>Qualified/Advanced eSeal certificate profiles</li> <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	<ul> <li>Add Microsoft OIDs in SSL certificates profiles to ensure alignement with Microsoft Trusted Root certificate Program requirements (<u>https://technet.microsoft.com/en-</u> <u>us/library/cc751157.aspx</u>).</li> </ul>				
1.26	NDE DEL DEL	24/11/2017 15/12/2017 01/01/2018	<ul> <li>Increase CRL validity from 4h30min to 8h30min for SSL certificates</li> <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>				



### **Table of content**

DOCUMEN	IT INFORMATION	. 2
VERSION I	HISTORY	2
TABLE OF	CONTENT	. 4
INTELLEC	TUAL PROPERTY RIGHTS	. 7
REFERENC	CES	. 8
INTRODUC	CTION	9
1.1	THE LUXTRUST PROJECT	9
1.2	GOAL OF THE LUXTRUST PKI	9
1.3	LuxTrust PKI Hierarchy	9
LUXTRUST	CERTIFICATION AUTHORITIES	10
1.4	Two-level CA hierarchy	
CERTIFICA	ATE AND CRL PROFILES	12
1.5	CERTIFICATE TYPES	.12
1.6	LUXTRUST CERTIFICATION AUTHORITIES – CERTIFICATES PROFILES	.23
1.7	LUXTRUST GLOBAL ROOT CA	.23
1.8	LUXTRUST GLOBAL QUALIFIED CA	.24
1.9	LUXTRUST SSL CA	.25
1.10	LUXTRUST TSA (TIMESTAMPING) CA	.27
1.11	LUXTRUST CORPORATE CA	.28
1.11.1	Certificate extensions	.30
1.11.2	Algorithm object identifiers	.30
1.11.3	Name forms	. 30
1.11.4	Name constraints	.30
1.11.5	Certificate policy object identifier	. 30
1.11.6	Usage of Policy Constraints extension	.30
1.11.7	Policy qualifiers syntax and semantics	.30
1.12	LUXTRUST END-ENTITY – CERTIFICATES PROFILES	.30
1.12.1	Certificate profiles	.30
1.12.2	Version number(s)	.31
1.12.3	LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures	.31
1.12.4	LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption	. 33
1.12.5	LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures	.35
1.12.6	LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption	.38
1.12.7	LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption	
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	.45
1.12.11	LuxTrust Signing Server LCP Certificates supporting Signature, Authentication & Encryption for integr 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



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



1.23.1	Version number(s)	. 128
1.23.2	OCSP extensions	. 128
1.24	INTEGRATION CERTIFICATES	.129



VERSION 1.28

### **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.



VERSION 1.28

### References

- [1] The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the [2] protection of individuals with regards to the processing of personal data and on the free movement of such data.
- [3] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- [4] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities. [5]
- [6] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [7] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [8] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [9] Règlement Grand-Ducal du 1 juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [10] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [11] LuxTrust Time Stamping Policy, latest version in force.
- [12] Guidelines for the Issuance and Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.
- [13] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Latest version in force.
- [14] eID Certificate Life Cycle Procedure latest version in force
- [15] RNCID : National Register of identity cards as specified in the national law 19/06/2013, section 5, article 16
- [16] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité [17] [Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [18] Loi du 19 juin 2013 Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques
- [19] EN 319 411 1 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- [20] EN 319 411 2 Electronic Signatures and Infrastructures; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [21] According to EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security
- Requirements for Trust Service Providers issuing Time-Stamps (2016-03)
- [22] According to EN 319 422 V1.1.1, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (2016-03)
- [23] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)
- [24] According to EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (2016-02)
- [25] According to EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates (2016-02)
- [26] According to EN 319 412-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (2016-02)
- [27] According to EN 319 412-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (2016-02)
- [28] According to EN 319 412-3 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (2016-02)
- [29] According to EN 319 412-4 V1.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (2016-02)
- [30] According to EN 319 412-5 V2.1.1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements (2016-02)
- [31] eIDAS regulation: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L\_.2014.257.01.0073.01.ENG



## INTRODUCTION

#### 1.1The LuxTrust project

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

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

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

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

#### 1.2 Goal of the LuxTrust PKI

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

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

LuxTrust will also promote these services towards application service providers in order to facilitate the emergence of eapplications 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.



VERSION 1.28

### **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:
  - o 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.



VERSION 1.28

Figure 1- LuxTrust running CA Hierarchy

			bal Root CA x	
CA CPS OI	lobal Qualified CA x D: 13.171.1.1.103 Branch: 13.171.11.103	LuxTrust SSL CA x CA C9 5010: 13.171.1.10.5 Certificate 010 Branch: 13.171.1.10.5	LuxTrust Global Corporate CA x CA (CFS 00): 13.371.11.13.04 Certificates 010 Brank: 13.371.1.10.4	LuxTrust TSA CA x CACPS 00::13.17.11.11.03 Certificate 00 Banch: 13.17.11.134
	J Didnith: 1.5.171.1.1.10.5	Certificates OID Branch: 1.3.171.1.1.10.5	Certificates OID Branch: 1.3.171.1.1.10.4	Certificates OID Branch: 1.3.171.1.1.10.8
"External" personal certificates		SSL/TLS and Object certificates	Legal and Natural Personnal certificates	LuxTrust TimeStamping Certificat
QCP+ supporting Qualified Electronic Signature vith Qualified Certificate issued on SSCD (for Natural Persons) [1.3.171.1.1.10.3.1]	Qualified Certificate Policy for for LuxTrust Qualified Timestamping [ [1.3.171.1.10.3.19]	SSL/TLS Standard Server Certificates [1.3.171.1.1.10.5.1] SSL/TLS Extended ValidationServer	LuxTrust LCP certificate supporting Authentication [1.3.171.1.1.0.4.1]	LuxTrust Trusted TimeStamping certificate [1.3.171.1.1.10.8.1]
ICP+ supporting Authentication & Encryption or Natural Persons [1.3.171.1.1.10.3.2]	LuxTrust SPARE Signing Server LCP Certificate Profile [1.3.171.1.1.10.3.20]	Certificates [1.3.171.1.1.10.5.2]-EVCP SSL/TLS Extended Validation Server Certificates [1.3.171.1.1.10.5.3]-EVCP+		
CP supporting Advanced Electronic Signature ith a Qualified Certificate (for Natural ersons) [1.3.171.1.1.10.3.3]	LuxTrust Qualified eSEAL Certificate Profile supporting digital signature [1.3.171.1.1.10.3.21]	Object Signing(+) Certificates [1.3.171.1.1.10.5.4] SSL/TLS Client Certificate		
ICP supporting Authentication & Encryption or Natural Persons [1.3.171.1.1.10.3.4]	LuxTrust Advanced eSEAL - Certificate Profile supporting authentication [1.3.171.1.10.3.22]	[1.3.171.1.1.10.5.5] LuxTrust SSL/TLS QCP-w Extended Validation Server Certificate		
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons [1.3.171.1.1.10.3.5]	LuxTrust Advanced eSEAL Certificate Profile supporting signature [1.3.171.1.1.10.3.23]	[1.3.171.1.1.10.5.6]		
VCP+ supporting Advanced Electronic Signature for Mass Signature Services 1.3.171.1.1.10.3.6]	LuxTrust Advanced eSEAL Certificate Profile supporting authentication [1.3.171.1.1.10.3.24]			
uxTrust LCP+ supporting Electronic Signature or Integration Purposes. 1.3.171.1.1.10.3.7]	LuxTrust Advanced Automated eSEAL Certificate Profile supporting signature [1.3.171.1.1.10.3.25]			
uxTrust LCP+ certificate supporting Signature, Authentication & incryption for Integration Purposes 1.3.171.1.1.10.3.8]	LuxTrust Smart Card QCP-n-qscd Certificate profile [1.3.171.1.1.10.3.26]			
uxTrust Signing Server, LCP certificate supporting Signature, Authentication & incryption for Integration Purposes 1.3.171.1.1.0.3.9]	LuxTrust Smart Card NCP+ Certificate profile [1.3.171.1.1.10.3.27]			
CP+ supporting Qualified Electronic Signature with Qualified Certificate issued on SSCD for Natural Persons for LRAO Purposes[1.3.171.1.1.10.3.10]	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 [1.3.171.1.1.0.3.28]			
ICP+ supporting Authentication & Encryption or Natural Persons for LRAO Purposes 1.3.171.1.10.3.11]	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]			
QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) for Mass LRAO Signatures 1.3.171.1.1.10.3.12]	QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global			
QCP+ supporting Qualified Electronic signature with Qualified Certificate issued on EID SSCD (for Natural Persons) 1.3.171.1.10.3.13]	Qualified CA [1.3.171.1.1.10.3.30]			
NCP+ supporting Authentication & Encryption on eID SSCD for Natural Persons 1.3.171.1.1.10.3.14]	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]			
ICP+ supporting SEAL Electronic Signature ervices [1.3.171.1.1.10.3.15]	LuxTrust Signing Server QCP-n-qscd Certificate issued by LuxTrust Global Qualified CA [1.3.171.1.1.10.3.32]			
uxTrust LCP+ supporting Electronic Signature or Integration Purposes. 1.3.171.1.1.10.3.16]	LuxTrust Signing Server QCP-I-qscd Certificate issued by LuxTrust Global Qualified CA [1.3.171.1.1.10.3.33]			
uxTrust LCP+ certificate supporting ignature, Authentication & Encryption for ntegration Purposes [1.3.171.1.1.0.3.17]	LuxTrust Signing Stick QCP-n-qscd Certificate Profile [1.3.171.1.1.10.3.34]			
Normalized Certificate Policy for LuxTrust Qualified Timestamping [1.3.171.1.1.10.3.18]	LuxTrust Signing Stick NCP+ Certificate Profile [1.3.171.1.1.10.3.35]			
LuxTrust Signing Server Certificate Profile Certifi [1.3.171.1.1.10.3.36]	r Advanced Automated eSeal icate Profile			



### **CERTIFICATE AND CRL PROFILES**

#### 1.5Certificate types

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

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



CP identification	CP OID	CPS OID	Short Description	Ref.
LuxTrust Qualified eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.21	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-I-qscd certificate policy.	Qualified eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSeal - Certificate Profile supporting authentication issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.22	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced eSEAL Certificate Profile supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.23	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting digital signature
LuxTrust Advanced eSEAL Certificate Profile supporting authentication issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.24	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced eSEAL Certificate Profile supporting authentication
LuxTrust Advanced Automated eSEAL Certificate Supporting digital signature issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.25	1.3.171.1.1.1.10.3	LuxTrust Normalized Certificate on HSM compliant with ETSI EN 319 411- 1 NCP+ Normalized certificate policy. Key Generation by CSP. Sole Authorized Usage: Support of Advanced eSEAL.	Advanced Mass eSEAL Certificate Profile supporting digital signature
LuxTrust Smart Card QCP-n-qscd Certificate Profile issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.26	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 <b>QCP-n-qscd</b> 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, <b>issued by LuxTrust</b> <b>Global Qualified CA</b>	1.3.171.1.1.10.3.28	1.3.171.1.1.1.10.3	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-1 <b>QCP-n-qscd</b> certificate policy, with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature for LRAO Purposes.	LuxTrust Smart Card LORA QCP-n- qscd supporting Qualified Electronic Signature with Qualified Certificate issued for Natural Persons for LRAO Purposes,



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



CP identification	CP OID	CPS OID	Short Description	Ref.
SSL/TLS Standard Server Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	1.3.171.1.1.1.10.5	ETSI TS 102 042 <b>LCP</b> compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	LuxTrust SSL/TLS Standard Server Certificates – LCP certificates supporting Signature, Authentication & Encryption
SSL/TLS(+) Extended Validation Server Certificates - EVCP issued by LuxTrust SSL CA	1.3.171.1.1.10.5.2	1.3.171.1.1.1.10.5	ETSI TS 102 042 <b>EVCP</b> compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.	SSL/TLS Extended Validation Server Certificates – EVCP certificates supporting Signature, Authentication & Encryption
SSL/TLS(+) Extended Validation Server Certificates – EVCP+ issued by LuxTrust SSL CA	1.3.171.1.1.10.5.3	1.3.171.1.1.1.10.5	ETSI TS 102 042 <b>EVCP+</b> compliant certificate, on Secure User Device, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e- mail.	SSL/TLS Extended Validation Server Certificates - EVCP+ certificates supporting Signature, Authentication & Encryption
Object Signing(+) Certificates issued by LuxTrust SSL CA	1.3.171.1.1.10.5.4	1.3.171.1.1.1.10.5	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
•	mping) Certification Author	ority		
LuxTrust Trusted TimeStamping certificate issued by LuxTrust TSA CA	1.3.171.1.1.10.8.1	1.3.171.1.1.1.10.8	LuxTrust certificate compliant with ETSI TS 102 023. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time-stamping authority. These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2011/8/001 by the national registry of Accredited Certification Service Providers.	Timestamping certificate profile
LuxTrust Global Corpo	rate CA			



VERSION 1.28

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.

## LUXTPUST®

VERSION 1	20
VERSIONI	.20

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
<b>1</b> LuxTrust	LuxTrust Certif Statements	ication Practice							
PKI	1 CPS LuxTrust	<b>1</b> CPS Summary GTE/Verizon Chain	0			x	у	1.3.171.1 <b>.1.1.1.0.x.y</b>	N/A
		<b>2</b> Not Used		Not Used		-	-	not used	N/A
		<b>10</b> 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	<b>10</b> CP's LuxTrust Global Chain	3 LuxTrust Global Qualified CA	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



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 1.28

_									
		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	
			LuxTrust Advanced eSEAL Certificate supporting authentication	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.24</b>	0.4.0.2042.1.2	
		25	LuxTrust Advanced Automated eSEAL Certificate supporting digital signature	LuxTrust Advanced eSeal	-	-	1.3.171.1. <b>1.10.3.25</b>	0.4.0.2042.1.2	
		26	LuxTrust Smart Card QCP-n-gscd Certificate Profile	SmartCard PRI/PRO		-	1.3.171.1 <b>.1.10.3.26</b>	0.4.0.404142.4.2	
		20	Lux must smart Card QCP-n-qscd Certificate Profile	Signature Certificate	1	-	1.3.171.1 <b>.1.10.3.20</b>	0.4.0.194112.1.2	
		27	LuxTrust Smart Card NCP+ Certificate Profile	SmartCard PRI/PRO		_	1 2 171 1 1 10 2 27	0 4 0 2042 4 2	
		21	Lux must smart Card NCP+ Centificate 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			1.3.171.1 <b>.1.10.3.28</b>	0 4 0 2042 1 2	
		20	Certificate for LRAO Purposes	Signature Certificate	-	-	1.3.171.1 <b>.1.10.3.20</b>	0.4.0.2042.1.2	
			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	LuxTruct alD Smort Card OCD a good Cartificate	eID SmartCard		_	1.3.171.1 <b>.1.10.3.30</b>	0.4.0.104140.4.0	
		30	LuxTrust eID Smart Card QCP-n-qscd Certificate	Signature Certificate	1	-	1.3.171.1 <b>.1.10.3.30</b>	0.4.0.194112.1.2	
		31	LuxTrust eID Smart card NCP+ Certificate	eID SmartCard		_	1.3.171.1. <b>1.10.3.31</b>	0.4.0.2042.1.2	
		31	Lux must eid Smart card NCP+ Centificate	Authentication Certificate	1	-	1.3.171.1. <b>1.10.3.31</b>	0.4.0.2042.1.2	
		32	LuxTrust Signing Server QCP-n-qscd Certificate	Signing Server certificate for qualified signature	-	-	1.3.171.1. <b>1.10.3.32</b>	0.4.0.194112.1.2	
		33	LuxTrust Signing Server QCP-I-qscd Certificate	Signing Server certificate for qualified eSeal	-	-	1.3.171.1. <b>1.10.3.33</b>	0.4.0.194112.1.3	
		34	LuxTrust Signing Stick QCP-n-qscd Certificate Profile	Signing Stick certificate Signature Certificate	-	-	1.3.171. <b>1.1.10.3.34</b>	0.4.0.194112.1.2	
		35	LuxTrust Signing Stick NCP+ Certificate Profile	Signing Stick certificate Authentication certificate	-	-	1.3.171. <b>1.1.10.3.35</b>	0.4.0.2042.1.2	
		36	LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	Signing Server Advanced Automated eSeal Certificate Profile			1.3.171.1.1.10.3.36	0.4.0.2042.1.3	
	<b>5</b> 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	
			1	1	4			-	



VERS	

VERSION 1.28							1	1
			SSL/TLS(+) Extended Validation Server Certificates - EVCP+	SSL/TLS Extended Validation Server Certificates on Secure Device	-	-	1.3.171.1. <b>1.10.5.3</b>	0.4.0.2042.1.5
		4	Object Signing(+) Certificates	Object Signing(+) Certificates	-	-	1.3.171.1. <b>1.10.5.4</b>	0.4.0.2042.1.3
		5	SSL/TLS Client Certificate	SSL/TLS Client Certificate	-	-	1.3.171.1. <b>1.10.5.5</b>	0.4.0.2042.1.3
		6	SSL/TLS QCP-w Extended Validation Server Certificates	SSL/TLS Qualified website authentication certificate	-	-	1.3.171.1. <b>1.10.5.6</b>	0.4.0.194112.1.4
	8 LuxTrust Global Timestamping CA Certificates		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	-	-	1.3.171.1.1.10.4.1	0.4.0.2042.1.3



#### 1.6LuxTrust Certification Authorities – Certificates profiles

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

LuxTrust CAs certificate profiles description is available as follows:

#### 1.7LuxTrust Global Root CA

	LuxTrust Global Root CA								
Base Profile	OID	Include d	Critical	Value					
Version		х		V3					
SerialNumber		х		As provided by CA or by LuxTrust S.A.					
SignatureAlgorithm									
Algorithm	1.2.840.113549.1.1.11	х		SHA256 with RSA Encryption	Fixed				
SignatureValue		х		Issuing CA Signature					
Validity									
NotBefore		х		Key Generation Process Date/Time					
NotAfter		х		Key Generation Process Date/Time + 10;20 years	Fixed				
SubjectPublicKeyInf o		x		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						
policyIdentifier		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	TRUE <sup>6</sup>						

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

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



VERSION 1.28

	LuxTrust Global Root CA								
Base Profile	OID	Include d	Critical	Value					
CertificateSigning				Set	Fixed				
crlSigning				Set	Fixed				
authorityKeyldentifie r	{id-ce 35}	Х	FALSE						
Keyldentifier		х		SHA-1 Hash					
subjectKeyldentifier	{id-ce 14}	Х	FALSE						
Keyldentifier		х		SHA-1 Hash					
BasicConstraints	{id-ce 19}	Х	TRUE <sup>6</sup>						
CA		Х		TRUE	Fixed				
pathLenConstraint		Х		None	Fixed				

#### 1.8LuxTrust Global Qualified CA

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

 $<sup>^{3}</sup>$  X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.28

	LuxTrust Global Qualified CA									
Base Profile	OID	Include d	Critical	Value						
policyIdentifier		х		1.3.171.1.1.10.3	Fixed					
policyQualifiers				N/a						
policyQualifierId	{ id-qt-1 }	х		CPS	Fixed					
Qualifier	CPSuri	х		https://repository.luxtrust.lu	Fixed					
KeyUsage	{id-ce 15}	х	<b>TRUE<sup>6</sup></b>							
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	47						
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx <sup>17</sup> .crt	Fixed					
subjectKeyldentifier	{id-ce 14}	Х	FALSE							
Keyldentifier		х		SHA-1 Hash of Subject public key						
cRLDistributionPoin ts	{id-ce 31}	х	FALSE							
distributionPoint										
FullName		х		http://crl.luxtrust.lu/LTGRCAx <sup>5</sup> .crl	Fixed					
BasicConstraints	{id-ce 19}	Х	<b>TRUE<sup>6</sup></b>	N/A						
CA		Х		TRUE	Fixed					
pathLenConstraint		Х		0 (Zero)	Fixed					

#### 1.9LuxTrust SSL CA

LuxTrust SSL CA								
Base Profile	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				

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

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

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



VERSION 1.28

LuxTrust SSL CA							
Base Profile	OID	Included	Critical	Value			
Validity							
NotBefore		х		Key Generation Process Date/Time			
NotAfter		х		Key Generation Process Date/Time +up to 20 years	Fixed		
SubjectPublicKeyInfo		х		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). <b>20 years certificate requires a 4096</b> key length.			
Issuer							
CountryName	{ id-at-6 }	х		LU	Fixed		
CommonName	{ id-at-3 }	Х		LuxTrust Global Root x <sup>1</sup>	Fixed		
organizationName		х		LuxTrust S.A.	Fixed		
Subject							
CountryName	{ id-at-6 }	х		LU	Fixed		
CommonName	{ id-at-3 }			LuxTrust SSL CA x <sup>7</sup>	Fixed		
organizationName		Х		LuxTrust S.A.	Fixed		
CertificatePolicies	{id-ce 32}	Х	FALSE				
policyldentifier (1)		Х		1.3.171.1.1.1.10.5	Fixed		
policyQualifiers (1)				N/a			
policyQualifierId (1)	{ id-qt-1 }	Х		CPS	Fixed		
Qualifier (1)		Х		https://repository.luxtrust.lu	Fixed		
policyldentifier (2)	{ anyPolicy }	Х		2.5.29.32.0	Fixed		
policyQualifiers (2)				N/a			
policyQualifierId (2)							
Qualifier (2)							
KeyUsage	{id-ce 15}	Х	TRUE <sup>6</sup>				
keyCertSign				Set	Fixed		
crlSign				Set	Fixed		
authorityKeyIdentifier	{id-ce 35}	Х	FALSE				
Keyldentifier		х		SHA-1 Hash of Authority public key			
authorityInfoAccess <sup>8</sup>	{id-pe 1}		False				
AccessMethod accessLocation	{Id-ad-1}	x		http://ltgroot.ocsp.luxtrust.lu	Fixed		
AccessMethod	{Id-ad-2}		False				
accessLocation subjectKeyIdentifier	{id-ce 14}	×	FALSE	http://ca.luxtrust.lu/LTGRCAx <sup>17</sup> .crt	Fixed		
Keyldentifier		x		SHA-1 Hash of Subject public key			
cRLDistributionPoints	(id oc 21)	-					
	{id-ce 31}	Х	FALSE				

<sup>&</sup>lt;sup>7</sup> X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

<sup>8</sup> Since LuxTrust SSL CA 4



VERSION 1.28

LuxTrust SSL CA								
Base Profile	OID	Included	Critical	Value				
distributionPoint								
FullName		х		http://crl.luxtrust.lu/LTGRCAx <sup>1</sup> .crl	Fixed			
BasicConstraints	{id-ce 19}	х	<b>TRUE<sup>6</sup></b>	N/a				
CA		х		TRUE	Fixed			
pathLenConstraint		Х		0 (Zero)	Fixed			

#### 1.10 LuxTrust TSA (Timestamping) CA

	LuxTru	st Global 1	Fimestamp	bing 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		x		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001). 20 years certificate requires a 4096 key length.	
Issuer					
CountryName	{ id-at-6 }	х		LU	Fixed
CommonName	{ id-at-3 }	х		LuxTrust Global Root x <sup>1</sup>	Fixed
organizationName		х		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	х		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Global Timestamping CA x <sup>9</sup>	Fixed
organizationName		х		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	х	FALSE		
policyIdentifier		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

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



VERSION 1.28

	LuxTri	ust Global 1	imestamp	bing CA	
Base Profile	OID	Included	Critical	Value	
KeyUsage	{id-ce 15}	х	TRUE <sup>6</sup>		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	х	FALSE		
Keyldentifier		х		SHA-1 Hash of Authority public key	
authorityInfoAccess10	{id-pe 1}		False		
AccessMethod	{Id-ad-1}				
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed
AccessMethod	{Id-ad-2}		False		
accessLocation		х		http://ca.luxtrust.lu/LTGRCAx <sup>1</sup> .crt	Fixed
subjectKeyldentifier	{id-ce 14}	х	FALSE		
Keyldentifier		х		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	х	FALSE		
distributionPoint					
FullName		х		http://crl.luxtrust.lu/LTGRCA <sup>5</sup> .crl	Fixed
Basic Constraints	{id-ce 19}	Х	<b>TRUE</b> <sup>6</sup>	N/a	
CA		х		TRUE	Fixed
pathLenConstraint		х		0 (Zero)	Fixed

#### 1.11 LuxTrust Corporate CA

	LuxTrust Corporate CA						
Base Profile	OID	D Included		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 + <b>up</b>	Fixed		
SubjectPublicKeyInfo		x		to 20 years Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).			

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



LuxTrust Corporate CA						
Base Profile	OID	Included	Critical	Value		
				20 years certificate requires a 4096 key length.		
Issuer						
CountryName	{ id-at-6 }	х		LU	Fixed	
CommonName	{ id-at-3 }	х		LuxTrust Global Root 2	Fixed	
organizationName		х		LuxTrust S.A.	Fixed	
Subject						
CountryName	{ id-at-6 }	Х		LU	Fixed	
CommonName	{ id-at-3 }			LuxTrust Corporate CA x	Fixed	
organizationName		х		LuxTrust S.A.	Fixed	
CertificatePolicies	{id-ce 32}	х	FALSE			
policyIdentifier		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	<b>TRUE</b> <sup>6</sup>			
keyCertSign				Set	Fixed	
crlSign				Set	Fixed	
authorityKeyIdentifier	{id-ce 35}	Х	FALSE			
Keyldentifier		Х		SHA-1 Hash of Authority public key		
authorityInfoAccess	{id-pe 1}		False			
AccessMethod	{Id-ad-1}					
accessLocation		х		http://ltgroot.ocsp.luxtrust.lu	Fixed	
AccessMethod	{Id-ad-2}		False		Thur d	
	(	x		http://ca.luxtrust.lu/LTGRCA2.crt	Fixed	
subjectKeyIdentifier	{id-ce 14}	X	FALSE			
Keyldentifier		X	EN 05	SHA-1 Hash of Subject public key		
cRLDistributionPoints	{id-ce 31}	X	FALSE			
distributionPoint						
FullName		X		http://crl.luxtrust.lu/LTGRCA2.crl	Fixed	
BasicConstraints	{id-ce 19}	Х	TRUE	N/A	ļ	
CA		х		TRUE	Fixed	
pathLenConstraint		Х		0 (Zero)	Fixed	



VERSION 1.28

#### 1.11.1 Certificate extensions

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

#### 1.11.2 Algorithm object identifiers

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

#### 1.11.3 Name forms

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

#### 1.11.4 Name constraints

Name constraints are supported as per RFC 5280.

#### 1.11.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

#### 1.11.6 Usage of Policy Constraints extension

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

#### 1.11.7 Policy gualifiers 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+11 Qualified Certificate for Natural Persons for the purpose of creating qualified electronic
  - signatures, under the Certificate Policy OID 1.3.171.1.1.0.3.1, and One LuxTrust NCP+<sup>12</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.2.
  - Under eIDAs regulation, those profiles are updated to the following certificate policies:
    - LuxTrust Smart Card QCP-n-qscd Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.10.3.26.
    - LuxTrust Smart Card NCP+ Certificate Profile, under the Certificate Policy OID 1.3.171.1.1.0.3.27.
- LuxTrust non SSCD Signing Sticks: These physical user devices that are not considered as SSCD according to [1] (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP<sup>11</sup> Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy OID 1.3.171.1.1.0.3.3, and
  - One LuxTrust NCP<sup>12</sup> certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.4.
- LuxTrust Signing Server Accounts (Virtual Smartcards): These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy - One LuxTrust NCP<sup>12</sup> certificate for Natural Persons for the combined purposes of electronic signature,
  - data/entity authentication and encryption facilities, under the Certificate Policy OID 1.3.171.1.1.10.3.5.
- LuxTrust eSeal Smart card-based certificates: The eSeal smart card exists in two versions: advanced and qualified.

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

LuxTrust Qualified eSeal Certificate Profile supporting digital signature under the Certificate Policy OID 1.3.171.1.1.10.3.21

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

<sup>&</sup>lt;sup>12</sup> As defined in ETSI TS 102 042 (cf. [4]).



VERSION 1.28

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

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

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

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

- LuxTrust SSL/TLS Standard Server Certificates: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.1.10.5.1.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP: SSL compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.10.5.2.
- LuxTrust SSL/TLS Extended Validation Server Certificates EVCP+: SSL compliant ETSI TS 102 042 [4] Certificate generated on Secure User Device, under the Certificate OID Policy 1.3.171.1.1.10.5.3.
- LuxTrust Object Signing (+) Certificates: Compliant ETSI TS 102 042 [4] Certificate not on SSCD Hardware token, under the Certificate OID Policy 1.3.171.1.10.5.4.
- 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>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
Base Profile									
Version	·	✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	jorithm	✓	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	ue	✓	False						
					D	Issuing CA Signature.			
Issuer		✓	False		S				
	countryName	~			S	LU			
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>			
	organizationName	✓			S	LuxTrust S.A.			

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

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

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

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

<sup>&</sup>lt;sup>17</sup> X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.



VERSION 1.28

Validity       NotBefore         NotAfter       Subject         Subject       serialNumbe         commonName       givenName         givenName       surname         countryName       emailAddres         title       organization         localityName       organization         1       1	Lux	Trust SS		P+ Cer	tificate	Profile
NotBefore         Subject       serialNumbe         Subject       commonNam         givenName       givenName         surname       countryName         countryName       emailAddres         ititle       organization         localityName       organization         organization       1         subjectPublicKeyInfo       Algorithm         subjectPublicKeyInfo       Algorithm         authorityKeyIdentifier       keyIdentifier         authorityInfoAccess       AccessMethe         authorityInfoAccess       AccessMethe	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Subject         Subject         SerialNumbe         commonNam         givenName         givenName         surname         countryName         emailAddres         ititle         organization         localityName         organization         1         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         authorityKeyIdentifier         keyIdentifier         authorityKeyIdentifier		√	False			
Subject       serialNumbe         Summe       commonName         givenName       givenName         givenName       surname         countryName       emailAddres         countryName       emailAddres         ititle       organization         localityName       organization         organization       1         subjectPublicKeyInfo       Algorithm         subjectPublicKeyInfo       Algorithm         Authority       properties         authorityKeyIdentifier       keyIdentifier         authorityInfoAccess       AccessMethe         accessLow       accessLow		<u>√</u>			D	Certificate generation process date/time.
serialNumbe commonNam givenName givenName surname countryName emailAddres title organization localityName organization localityName organization 1 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess		$\checkmark$			D	Certificate generation process date/time + <b>36</b> Months
serialNumbe commonNam givenName givenName surname countryName emailAddres title ititle organization localityName localityName organization localityName authorityEvidentifier subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier keyIdentifier		√	False			
commonNam givenName surname countryName emailAddres title organization localityName organization localityName organization 1 corganization 1 subjectPublicKeyInfo Algorithm subjectPublic keyIdentifier authorityKeyIdentifier keyIdentifier	her	✓		М	D	Serial Number as constructed by LRAO
givenName         givenName         surname         countryName         emailAddres         title         title         organization         localityName         organization         1         organization         1         organization         2         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         AccessMethe         accessLop				141		,
surname countryName emailAddres title organization localityName organization 1 organization 1 subjectPublicKeyInfo Algorithm subjectPublic KeyInfo Algorithm subjectPublic authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe	ame	$\checkmark$		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.
countryName         emailAddres         ititle         title         organization         localityName         organization         localityName         organization         1         organization         1         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Algorithm         subjectPublicKeyInfo         Authority         Properties         authorityKeyIdentifier         keyIdentifier         authorityInfoAccess         AccessMethe         accessLop	e	$\checkmark$		М	D	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
emailAddres  title  title  organization  localityName  organization  organization  subjectPublicKeyInfo  Algorithm  subjectPublic  Extensions  Authority Properties  authorityKeyIdentifier  keyIdentifier  authorityInfoAccess  AccessMethe accessLoe		$\checkmark$		М	D	<b>PRO and PRIVATE products</b> : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
title title organization localityName organization 1 organization 1 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe	me	$\checkmark$		М	D	Nationality of holder (ISO3166)
organization localityName organization 1 organization 1 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLot	ess	$\checkmark$		0	D	Subject's email address
IocalityName organization 1 organization 1 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe		~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
organization 1 organization 2 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLo	onName	✓		М	D	<b>PRO products only:</b> Name of company/institution as in articles of association or equivalent documents, including the legal form.
1 organization 2 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe	me	$\checkmark$		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
2 subjectPublicKeyInfo Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe	onalUnitName	V		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<b>PRO products:</b> Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoc	onalUnitName	✓		0	D	<b>PRO products only</b> : Company/institution department or other information item
Algorithm subjectPublic Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoc		✓	False			
Extensions Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe		√				Public Key: Key length: 2048bit (RSA); public
Authority Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe	blicKey	$\checkmark$		М		exponent: Fermat-4 (=010001).
Properties authorityKeyIdentifier keyIdentifier authorityInfoAccess AccessMethe accessLoe						
authorityKeyldentifier keyldentifier authorityInfoAccess AccessMethe accessLoe						
authorityInfoAccess AccessMetho accessLoo		√	False			
AccessMethe accessLo	er	✓ ✓	1 4100			SHA-1 Hash of the LuxTrust Global Qualified
AccessMethe accessLo		./	<b>Felce</b>			CA public key
accessLo	thod	✓ ✓	False			Id-ad-2
		✓ ✓				Id-ad-2 http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
		· ✓				http://ca.luxtrust.lu/LTGQCAx .crt Id-ad-1
accessLo		 ✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistributionPoint		· ✓	False			nup.//qca.ocsp.iuxtfust.iu/
distributionPoint	nPoint	 ✓	1 0156		S	
fullName		· ✓	†	L	۲Ŭ –	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl

<sup>18</sup> SINCE LTGQCA3



VERSION 1.28

	LuxTrust SSCD QCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
Subject Properties									
subjectAltNa		✓	False						
	Rfc822Name	✓		0	D	Certificate Holder's email address			
subjectKeylo		✓	False						
	keyldentifier	~			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	✓				1.3.171.1.1.10.3.1			
	policyQualifierID	~			S	Id-qt-1 (CPS)			
	qualifier	~			S	https://repository.luxtrust.lu			
	policyQualifierID	~			S	Id-qt-2 (User Notice)			
	noticeNumbers								
	DisplayText	~				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Support of Qualified Electronic Signature.			
	Policyldentifier	✓				0.4.0.1456.1.1			
QualifiedCer									
	QcCompliance	✓		М	S	0.4.0.1862.1.1			
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]			
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]			
	QcSSCD	✓		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 1.3.171.1.10.3.2>**.

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

	LuxTrust SSCD NCP+ Certificate Profile								
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg	jorithm	✓	False						
-	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	lue	✓	False						
					D	Issuing CA Signature.			



	Lux	Trust	SSCD	NCP+ Cer	tificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
issuer	1000	√	False	0/11	S	Value
	countryName	$\checkmark$			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False		_	
	NotBefore	$\checkmark$			D	Certificate generation process date/time.
	NotAfter	v			D	Certificate generation process date/time + 36 Months
subject		✓	False			Months
	serialNumber	~	1 0.00	М	D	Serial Number as constructed by LRAO
	SeriaiNumber	•		IVI		,
	commonName	~		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	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		М	D	<b>PRO and PRIVATE products</b> : 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	√	1	0	D	Subject's email address
	emanAddress	v		0	U	
	title	¥		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	<b>PRO products only:</b> 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	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<ul> <li>PRO products:</li> <li>Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)</li> <li>PRIVATE products:</li> <li>If the holder is underage: "Mineur jusqu'à : " &amp; (Date of birth + 18 years).</li> </ul>
	organizationalUnitName 2	~		0	D	<b>PRO products only</b> : Company/institution department or other information item
subjectPubli	icKeyInfo	✓	False			
	algorithm	<ul> <li>✓</li> </ul>				Public Key: Key length: 2048 bit (RSA); public
-	subjectPublicKey	~		М		exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	✓	False			
addiontyney	keyldentifier	✓ ✓	1 0130			SHA-1 Hash of the LuxTrust Global
						Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
	tionBoint	√	False	1		
cRLDistribut	lionFoint		1 0100			



VERSION 1.28

LuxTrust SSCD NCP+ Certificate Profile						
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	$\checkmark$		0	D	Certificate Holder's email address
subjectKeyld		✓	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	~			S	True
	nonRepudiation				S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo		✓	False			
	Policyldentifier	$\checkmark$				1.3.171.1.1.10.3.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓ 				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption.
	Policyldentifier	$\checkmark$				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>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value	
Base Profile							
Version		~	False				
					S	Version 3 Value = "2"	
SerialNumb	SerialNumber		False				
					FDV	Validated on duplicates.	
signatureAlgorithm		~	False				
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.	
signatureVa	signatureValue		False				
					D	Issuing CA Signature.	



	Lux	Trust	non SS		Certific	cate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Issuer		✓	False		S	
	countryName	~			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	~			S	LuxTrust S.A.
Validity	-	✓	False			
-	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 36 Months
Subject	·	~	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	<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	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		М	D	<b>PRO and PRIVATE products</b> : Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	¥		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	<b>PRO products only:</b> 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	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<b>PRO products:</b> Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitName 2	~		0	D	<b>PRO products only</b> : Company/institution department or other information item
sub	ojectPublicKeyInfo	~	False			
	Algorithm	~				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	~	İ	М		exponent: Fermat-4 (=010001).
Extensions						
Authority P	roperties					
authorityKe	eyldentifier	✓	False			



	Lu	xTrust	non SS	CD QCP	Certific	cate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
	keyldentifier	~				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInt	foAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
cRLDistrib	utionPoint	✓	False			
	distributionPoint	~			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Pro	operties					
subjectAltN	lame	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey	Identifier	✓	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 Prop	perties					
keyUsage	1	✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP	Policies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.3
	policyQualifierID	✓			S	ld-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	V				LuxTrust Qualified Certificate not on SSCD compliant with ETSI TS 101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert
	Policyldentifier	✓				0.4.0.1456.1.2
QualifiedCe	ertificateStat					
	QcCompliance	~		М	S	0.4.0.1862.1.1
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]
	QcSSCD	~				NOT SET



VERSION 1.28

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

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

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

The usage purpose of these NCP Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust non SSCD NCP OID, i.e., **<OID 1.3.171.1.10.3.4>**.

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

	LuxTi	rust non	SSCDN	ICP Cert	ificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile Version		√	E a la a			
version		•	False		S	Version 3 Value = "2"
SerialNumbe	) 2r	✓	False		5	
oonantanis			1 0100		FDV	Validated on duplicates.
signatureAlg	jorithm	√	False			
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
-					D	Issuing CA Signature.
issuer	a a construction of	✓ ✓	False		S	
	countryName commonName	V 			S S	
		· · ·			S S	LuxTrust Global Qualified CA x <sup>17</sup>
Validity	organizationName	✓ ✓	False		5	LuxTrust S.A.
valuity	NotBefore	· · · · · · · · · · · · · · · · · · ·	1 0150		D	Certificate generation process date/time.
	NotAfter	V			D	Certificate generation process date/time + 36 Months
subject	•	✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		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	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		М	D	<b>PRO and PRIVATE products:</b> Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	✓		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	title	~		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	<b>PRO products only:</b> 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)



	LuxTrus	st non	SSCD	ICP Cert	ificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationalUnitName 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<b>PRO products:</b> Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitName 2	~		о	D	<b>PRO products only</b> : Company/institution department or other information item
subjectPubli		✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	$\checkmark$				Id-ad-1
	accessLocation	$\checkmark$				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	✓ ✓		0	D	Certificate Holder's email address
subjectKeylo	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			Truce			
keyUsage	digitalSignature	✓ ✓	True		S	True
	nonRepudiation	•			S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo	lisios	✓	Falsa			
certificatePo		✓ ✓	False			
	Policyldentifier policyQualifierID	✓ ✓			S	1.3.171.1.1.10.3.4 Id-qt-1 (CPS)
	qualifier	✓	1		S	https://repository.luxtrust.lu
	policyQualifierID	· ✓	1		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. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption.
	Policyldentifier	$\checkmark$				0.4.0.2042.1.1



VERSION 1.28

#### 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 1.3.171.1.10.3.5>**.

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

	LuxTru	ust Signing	g Serve	r NCP C	ertificat	te Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile Version			False			
Version			T dise		S	Version 3 Value = "2"
SerialNumb	er	✓	False		Ŭ	
					FDV	Validated on duplicates.
signatureAl		✓	False			
	algorithm				S	OID = "1.2.840.113549.1.1.5" - if SHA1 with RSA Encryption. OID = "1.2.840.113549.1.1.11" - i SHA256 with RSA Encryption.
signatureVa	lue	√	False		_	
loouer		√	False		D S	Issuing CA Signature.
Issuer	countryName	✓ ✓	False		S	LU
	commonName	· ✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	organizationitanie	✓	False		0	
,	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time - 36 Months
subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	PRO and PRIVATE products Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character
	givenName	~		М	D	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		М	D	<b>PRO and PRIVATE products</b> Surname(s) as on ID card withou indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	✓		0	D	Subject's email address
	title	¥		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) of "Professional Administrator" (Other titles possible for special purposed certificates)



	LuxTrust	Signing	g Serve	er NCP C	ertifica	te Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
						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	<b>PRO products only</b> : Company/institutior country of HQ (as in articles of association)
	organizationalUnitName 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<b>PRO products</b> : Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à . " & (Date of birth + 18 years).
	organizationalUnitName 2	~		0	D	<b>PRO products only:</b> Company/institution department or other information item
subjectPublic		✓	False			
	algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: 2048 bit (RSA): public exponent: Fermat-4 (=010001).
Extensions	subjectPublickey	•		IVI		public exponent. Fermat-4 (=010001).
Authority						
Properties						
authorityKeylo	dentifier	√	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Globa
		,				Qualified CA public key
authorityInfoA		✓	False			
<u> </u>	AccessMethod	$\checkmark$				Id-ad-2
_	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
cRLDistributio		✓	False		-	
	distributionPoint	<ul> <li>✓</li> </ul>			S	17
	fullName	~				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
Subject Properties						
subjectAltNam	1e	√	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeylde	ntifier	✓	False			
	keyldentifier	<b>~</b>			Fixed	The Key Identifier comprises a four-bi 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 numbe of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	True
	-					
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePoli	cies	✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.5
F	policyQualifierID	✓	1		S	Id-qt-1 (CPS)
F	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					



VERSION 1.28

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

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

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

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

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

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

LuxTrust	non SSCD NCP+ Publi	ic Cert	ificate	Profile	for Ma	ass Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		✓	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 <sup>17</sup>
	organizationName	√			S	LuxTrust S.A.
Validity		√	False			
¥	NotBefore	~			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 36 Months
subject		✓	False			
	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	~		М	D	Country in which the organization's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	emailAddress	~		0	D	Subject's email address if available
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	localityName	~		М	D	Location in which the organization's registered office is established (as specified in the memorandum and articles of association or an equivalent document)



VERSION 1.28

Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Attribute				0/111	00	Value
	organizationalUnitName 1	~		0	D	As provided by Subscriber
	organizationalonitivame i	·		U	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						
Authority Properties						
authorityKeyldentifier		<b>√</b>	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Globa
autharity Jufa Access		./	<b>F</b> alse			Qualified CA public key
authorityInfoAccess	AccessMatherd	$\checkmark$	False			
	AccessMethod accessLocation	✓ ✓				ld-ad-2
						http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistributionPoint		$\checkmark$	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltName		✓	False			
•	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKeyldentifier	•	✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bi
						field with a 0100 value, followed by the
						least significant 60 bits of the SHA-
						hash of the value or subjectPublicKe
						bit string (tag, not including the length
Deliev Dreparties						and number of unused bit-string bits).
Policy Properties keyUsage		✓	True			
keyusaye	digitalSignature	* 	Tiue		S	False
	uigitaiSignature	•			3	i alse
	nonRepudiation	1	<u> </u>		S	True
					Ŭ	
	keyEncipherment	~			S	False
					_	
	dataEncipherment	✓	1		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	~				LuxTrust Certificate on Secure Use
						Device compliant with ETSI TS 102
						042 NCP+ certificate policy. Ke
						Generation by CSP.
						Sole Authorised Usage: Advance
						electronic massive signature services.
	Policyldentifier	✓				0 4 0 2042 1 2
	Folicyldenuller	•	L			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]).



VERSION 1.28

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 1.3.171.1.1.0.3.7>.

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

LuxTrust Integration Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base										
Profile Version		✓	Folgo							
Version		•	False		S	Version 3 Value = "2"				
SerialNumbe	r	✓	False							
					FDV	Validated on duplicates.				
signatureAlg		✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA				
signatureVal	ue	✓	False			Encryption.				
orginatarora			1 0100		D	Issuing CA Signature.				
Issuer		✓	False		S					
	countryName	✓			S	LU				
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>				
M - 11 - 11 (	organizationName	✓ ✓	E a la a		S	LuxTrust S.A.				
Validity	NotBefore	✓ ✓	False		D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 36 Months				
Subject		$\checkmark$	False							
	serialNumber	✓		М	D	Serial Number as constructed by LRAO				
	commonName	✓		М	D					
						Concatenation of given name(s) and surname(s)				
	air an Nama	~								
	givenName	~		М	D	<b>TEST ONLY + " " +</b> As provided by Subscriber				
	surname	~		М	D	As provided by Subscriber				
		-								
	countryName	$\checkmark$		М	D	LU				
	emailAddress	~		0	D	As provided by Subscriber				
	Title	~		М	D	<b>PRIVATE products:</b> Fixed value: " <b>Private Person</b> "				
						PRO products:				
						"Professional Person" (default) or "Professiona Administrator"				
						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	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)				
	organizationalUnitName 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<b>PRO products</b> : Company/Institution VAT number (or if no VA' number available, other unique nationa company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).				
	organizationalUnitName 2	~		0	D	<b>PRO products only</b> : Company/institution department or other information item				
subjectPubli		✓	False							
	Algorithm subjectPublicKey	✓ ✓		N4		Public Key: Key length: 2048bit (RSA); public				
	SUDIECTFUDIICNEV	V 1	1	M	1	exponent: Fermat-4 (=010001).				



VERSION 1.28

	L	uxTru	st Integ	gration	Certif	icate Profile
Attribute	Field	IN <sup>13</sup>		O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribut	tionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ime	✓	False			
	Rfc822Name	✓		0	D	N/A
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	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo		✓	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 1.3.171.1.10.3.8>**.

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

	LuxTrust SSCD LCP+ Integration Certificate Profile									
Attribute	Field	IN <sup>13</sup>		O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	r	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	orithm	✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	ue	✓	False							
					D	Issuing CA Signature.				



	LuxTru	st SSC	D LCP+	Integra	tion Cer	tificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	•	$\checkmark$	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 30
Subject		✓	False			Months
Subject			Faise		_	
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	LGQCA XX SC PRI V3 (XX a numbe selected internally by LuxTrust)
	givenName	~		М	D	LGQCA XX (XX a number selected internall by LuxTrust)
	Surname	~	1	М	D	SC PRI V3
	countryName	✓		М	D	LU
	emailAddress	√	1	0	D	N/A
	emanauuress		-	0	U	
	Title	~	1	М	D	Private Person
subjectPubli	cKeyInfo	✓	False	1		
	Algorithm	~				Public Key: Key length: 2048 bit (RSA); publi
	subjectPublicKey	√		М		exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties	de antifica		<b>F</b> -1			
authorityKey		✓ ✓	False			SHA-1 Hash of the LuxTrust Global Qualifie
	keyldentifier	<b>`</b>	1			
authorityInfo	Access	✓	False			CA public key
autiontymio	AccessMethod	· ·	1 2130			ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~	+		+	Id-ad-1
	accessLocation	· ✓				http://qca.ocsp.luxtrust.lu/
cRLDistribut		· ·	False			nup.//qca.ocsp.iuxtrust.iu/
	distributionPoint	✓ ✓	raise		S	
	fullName	▼ ✓	+		3	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject		· · · ·				nup.//ch.iuxtrust.iu/LTGQCAX . <u>.Cfi</u>
Properties						
subjectAltNa		✓ ✓	False	0		
subjectKeyld	Rfc822Name	✓ ✓	False	0	D	N/A
	keyldentifier	· ·			Fixed	The Key Identifier comprises a four-bit field wit a 0100 value, followed by the least significar 60 bits of the SHA-1 hash of the value of subjectPublicKey bit string (tag, not includin the length and number of unused bit-strin bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	· ·	inde		S	True
	nonRepudiation				S	False
	keyEncipherment	√			S	True
	dataEncipherment	✓			S	True
certificatePo		$\checkmark$	False			
	Policyldentifier	√				1.3.171.1.1.10.3.8
	policyQualifierID	√			S	Id-qt-1 (CPS)
	Qualifier	<ul> <li>✓</li> </ul>			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE o SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. <b>Sol</b> <b>Authorised Usage</b> : Authentication an



VERSION 1.28

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

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

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

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

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption for integration only. These Certificates include the corresponding LuxTrust Signing Server Account OID, i.e., **<OID** 1.3.171.1.10.3.9>.

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

Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	~	False			
					FDV	Validated on duplicates.
signatureAl		✓	False		S	OID = "1.2.840.113549.1.1.5" – if SHA
	Algorithm				5	OID         =         1.2.840.113549.1.1.5         – If         SHA           with RSA Encryption.         OID         =         "1.2.840.113549.1.1.11"         – if           SHA256 with RSA Encryption.         =         SHA256 with RSA Encryption.         =         =
signatureVa	alue	✓	False			
			L		D	Issuing CA Signature.
Issuer		✓ ✓	False		S	
	countryName	✓ ✓			S	LU
	commonName				S	LuxTrust Global Qualified CA x <sup>17</sup>
\/ - I! .I! (	organizationName	✓ ✓			S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Cartificate generation process data/time
	NotAfter	v 			D	Certificate generation process date/time. Certificate generation process date/time -
					_	36 Months
Subject	÷	✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	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	V		М	D	<b>CSS or</b> Surname(s) as on ID documer without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	~		М	D	LU or Nationality of holder (ISO3166)
	emailAddress	~		0	D	N/A
	Title	✓		М	D	Private Person
subjectPubl		$\checkmark$	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA)
	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).



VERSION 1.28

	LuxTru	st Signin	g Serve	r LCP C	ertificat	e Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Extensions					1	
Authority						
Properties						
authorityKey		✓	False			
	keyldentifier	$\checkmark$				SHA-1 Hash of the LuxTrust <b>Global</b> <b>Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	~				Id-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				Id-ad-1
	accessLocation	~				http://gca.ocsp.luxtrust.lu/18
cRLDistribut	ionPoint	✓	False			
	distributionPoint	√			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ime	~	False			
	Rfc822Name	~		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						
keyUsage		~	True			
	digitalSignature	~			S	True
	nonRepudiation				S	True
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo	licies	✓	False			
	Policyldentifier	✓			1	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	×				INTEGRATION Certificate not on SSCD compliant with ETSI TS 102 042 LCP cert.policy. Key Generation by CSP. <b>Sole</b> <b>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 1.3.171.1.10.3.10>.

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

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



	LuxTru	ust SSCD	LORA	QCP+	Certific	ate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile			Falsa			
Version		~	False		S	Version 3 Value = "2"
SerialNumbe	er	√	False		3	
					FDV	Validated on duplicates.
signatureAlg	orithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256
signatureVal	ue	√	False			with RSA Encryption.
orginatarova			1 0100		D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓ ✓	E a la a		S	LuxTrust S.A.
Validity	NotBefore	✓ ✓	False		D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + <b>36</b>
						Months
Subject		$\checkmark$	False			
	serialNumber	$\checkmark$		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	$\checkmark$		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	✓ ✓				Public Key: Key length: 2048bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	subjectPublicKey	~		М		
Authority						
Properties						
authorityKey		√	False			
	keyldentifier	$\checkmark$				SHA-1 Hash of the LuxTrust <b>Global</b> <b>Qualified</b> CA public key
authorityInfo	Access	✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	√				ld-ad-1
	accessLocation	✓				http://gca.ocsp.luxtrust.lu/18
cRLDistribut		✓ ✓	False			
	distributionPoint	✓ ✓			S	17
0.1	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa		√	False			
	Rfc822Name	✓ ✓		0	D	Certificate Holder's email address
subjectKeylo	lentifier	$\checkmark$	False			



VERSION 1.28

	LuxTrust SSCD LORA QCP+ Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	False				
	nonRepudiation	✓			S	True				
	keyEncipherment	✓			S	False				
	dataEncipherment	✓			S	False				
certificatePo	licies	✓	False							
	Policyldentifier	√				1.3.171.1.1.10.3.10				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	~				LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Support of Qualified Electronic Signature for LRAO purposes				
	Policyldentifier	✓				0.4.0.1456.1.1				
QualifiedCer	tificateStat									
	QcCompliance	✓		М	S	0.4.0.1862.1.1				
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [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 1.3.171.1.10.3.11>**.

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

	LuxTrust SSCD LORA NCP+ Certificate Profile									
Attribute	Field	<b>IN</b> <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	er	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	jorithm	✓	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	ue	✓	False							
					D	Issuing CA Signature.				
Issuer	•	√	False		S					
	countryName	√			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>				
	organizationName	√			S	LuxTrust S.A.				



	LuxTru	ust SS		RA NCP+	Certific	cate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	$\checkmark$			D	Certificate generation process date/time + 36
Subject		~	False			Months
Subject	· · · · ·		Faise			
	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	$\checkmark$				Public Key: Key length: 2048 bit (RSA); public
Extensions	subjectPublicKey	•		М		exponent: Fermat-4 (=010001).
Authority Properties						
authorityKey	/Identifier	✓	False			
	keyldentifier	$\checkmark$				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo	Access	✓	False			
	AccessMethod	~				Id-ad-2
	accessLocation	$\checkmark$				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	√				ld-ad-1
	accessLocation	$\checkmark$				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint	✓			S	2/
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa		✓	False			
	Rfc822Name	<b>√</b>		0	D	Certificate Holder's email address
subjectKeylo		<b>√</b>	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation				S	False
	keyEncipherment	~			S	True
	dataEncipherment	✓			S	True
certificatePc	olicies	✓	False			
	-					



VERSION 1.28

	LuxTrust SSCD LORA NCP+ Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
	Policyldentifier	√				1.3.171.1.1.10.3.11				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	Qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	✓			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	~				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption for LRAO purposes.				
	Policyldentifier	✓				0.4.0.2042.1.2				

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

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

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

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate for Mass LRAO Signature purposes. These Certificates include the corresponding LuxTrust QCP OID, i.e., < OID 1.3.171.1.10.3.12>.

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

	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value				
Base Profile	)									
Version		~	False							
					S	Version 3 Value = "2"				
SerialNumb	er	✓	False							
					FDV	Validated on duplicates.				
signatureAl	gorithm	~	False							
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	lue	✓	False							
					D	Issuing CA Signature.				
Issuer		~	False		S					
	countryName	~			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>				
	organizationName	~			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	~			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 36 Months				
Subject		~	False							
	serialNumber	~		М	D	Serial Number as constructed by LRAO				
	commonName	~		М	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character				
	givenName	✓		М	D	Given name(s) as on ID card				



	LuxTrust non SS	SCD Q	CP Ma	ss LRAO	Signat	ures Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"LuxTrust RA officer – LRS"
	organizationName	~		М	D	"RA" & RA number & " – " & Name of the LuxTrust RA
	localityName	~		М	D	Country of RA (as in articles of association)
	organizationalUnitName 1	~		м	D	RA code Constructed by LuxTrust
	organizationalUnitName 2	~		0	D	RAO code Constructed by LuxTrust
sub	jectPublicKeyInfo	~	False			
	Algorithm	✓				Public Key: Key length: 2048 bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensions						
Authority P	roperties					
authorityKe	yldentifier	~	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInf	oAccess	~	False			
	AccessMethod	~				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribu	itionPoint	~	False			
	distributionPoint	~			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Pro	perties					
subjectAltN	ame	✓	False			
	Rfc822Name	~		0	D	Certificate Holder's email address
subjectKeyl	dentifier	✓	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Prop	erties					
keyUsage		~	True			
	digitalSignature	~			S	False
	nonRepudiation	~			S	True
	keyEncipherment	~			S	False
	dataEncipherment	~			S	False
certificatePo	olicies	✓	False			



VERSION 1.28

	LuxTrust non SSCD QCP Mass LRAO Signatures Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value					
	Policyldentifier	✓				1.3.171.1.1.10.3.12					
	policyQualifierID	✓			S	ld-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	V				LuxTrust Qualified Certificate not SSCD compliant with ETSI TS101456 QCP certificate policy.Key Generation by CSP.Sole Authorised Usage: Support of Advanced Electronic Signature for Mass LRAO purposes					
	Policyldentifier	~				0.4.0.1456.1.2					
QualifiedCe	rtificateStat										
	QcCompliance	✓		М	S	0.4.0.1862.1.1					
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcSSCD	~				NOT SET					

### 1.12.15 LuxTrust 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 1.3.171.1.10.3.13>.

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

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

The certificate re-key is not allowed.

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

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

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

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

<sup>&</sup>lt;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 SSCD QCP+ Certificate Profile									
Attribute	Field	IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>	CO <sup>22</sup>	Value			
Allibule	Algorithm			0/141	S	OID = "1.2.840.113549.1.1.11" - SHA256 with			
	Algorithm				Ũ	RSA Encryption.			
signatureVa	lue	√	False						
					D	Issuing CA Signature.			
Issuer	•	✓	False		S				
	countryName	✓			S	LU			
	commonName	~			S	LuxTrust Global Qualified CA x <sup>23</sup>			
	organizationName	✓			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore	✓			D	Certificate generation process date/time.			
	NotAfter	×			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate			
Subject		✓	False						
	serialNumber	~		М	D	Serial Number as constructed by LRAO			
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character			
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID			
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID			
	countryName	~		М	D	LU			
	emailAddress	~		0	D	Subject's email address			
	Title	~		М	D	"Private Person"			
	organizationalUnitName 1	~		ο	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).			
subjectPubli	icKeyInfo	✓	False						
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit			
	subjectPublicKey	✓		M		(RSA); public exponent: Fermat-4 (=010001).			
Extensions									
Authority									
Properties									
authorityKey		✓ ✓	False						
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key			
authorityInfo		✓	False						
	AccessMethod	✓				Id-ad-2			
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt			
	AccessMethod	✓				ld-ad-1			
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>			
cRLDistribut		✓	False						
	distributionPoint	✓			S				
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl			
Subject Properties									
subjectAltNa	ame	✓	False						
	Rfc822Name	~		0	D	Subject email address			
subjectKeyle		✓	False	-					
	keyldentifier	<b>v</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit- string bits).			
Policy Properties									
keyUsage		✓	True						
	digitalSignature	✓			S	False			
	nonRepudiation	✓			S	True			

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



VERSION 1.28

	LuxTrust eID SSCD QCP+ Certificate Profile										
Attribute	Field	IN <sup>19</sup>	CE <sup>20</sup>	O/M <sup>21</sup>	CO <sup>22</sup>	Value					
-	keyEncipherment	✓			S	False					
	dataEncipherment	✓			S	False					
certificatePo	olicies	✓	False								
	Policyldentifier	✓				1.3.171.1.1.10.3.13					
	policyQualifierID	✓			S	Id-qt-1 (CPS)					
	Qualifier	✓			S	https://repository.luxtrust.lu					
	policyQualifierID	✓			S	Id-qt-2 (User Notice)					
	noticeNumbers										
	DisplayText	✓ 				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					
QualifiedCe	rtificateStat										
	QcCompliance	✓		М	S	0.4.0.1862.1.1					
	QcLimitValue			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcRetentionPeriod			0	D	As provided by LuxTrust S.A. in compliance with [3]					
	QcSSCD	✓		М	D	OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }					

### 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 1.3.171.1.10.3.14>**.

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

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

The certificate re-key is not allowed.

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

	LuxTrust SSCD NCP+ Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	r	✓	False								
					FDV	Validated on duplicates.					
signatureAlg	orithm	✓	False								
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signatureVal	ue	✓	False								
					D	Issuing CA Signature.					
issuer		✓	False		S						
	countryName	~			S	LU					
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	~			D	Certificate generation process date/time.					



	Lux	(Trust	SSCD N	ICP+ Cer	tificate	Profile
Attribute	Field	IN <sup>13</sup>		<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
	NotAfter	<b>v</b>			D	Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate
subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID
	surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	~		М	D	LU
	emailAddress	~		0	D	Subject's email address
	title	~		М	D	"Private Person"
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPublic		✓ ✓	False			Dublis Konstantin 0040 bitum ta 4000bit
	algorithm subjectPublicKey	✓ ✓		М		Public Key: Key length: 2048 bit up to 4096bit (RSA); public exponent: Fermat-4 (=010001).
Extensions	Subjecti ubilercey	-		IVI		
Authority Properties						
authorityKey		✓	False			
authorityInfo	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
autiontylino	AccessMethod	✓ ✓	raise			ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint fullName	✓ ✓			S	17
Quality of	fullname	•				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	me	~	False			
	Rfc822Name	✓		0	D	Subject email address
subjectKeyld		✓ ✓	False		Ebrad	The Vey Identifier commisses a four bit 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 keyUsage		√	True			
reyusaye	digitalSignature	<ul> <li>✓</li> </ul>	The		S	True
	nonRepudiation				S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo		~	False			
	Policyldentifier	<b>√</b>				1.3.171.1.1.10.3.14
	policyQualifierID qualifier	✓ ✓			S S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	policyQualifierID	✓ ✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
			1	1		l



VERSION 1.28

	LuxTrust SSCD NCP+ Certificate Profile									
Attribute	Field	<b>IN</b> <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value				
	DisplayText	~				LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Data or Entity Authentication and Data Encryption.				
	PolicyIdentifier	✓				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 SSCD LCP Integration Signature Certificate Profile									
Attribute	Field	IN <sup>24</sup>	<b>CE</b> <sup>25</sup>	<b>O/M</b> <sup>26</sup>	<b>CO</b> <sup>27</sup>	Value				
Base Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	e <mark>r</mark>	✓	False							
					FDV	Validated on duplicates.				
signatureAlg	gorithm	✓	False							
	Algorithm	×			S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	signatureValue		False							
					D	Issuing CA Signature.				
Issuer		$\checkmark$	False		S					
	countryName	✓			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x <sup>28</sup>				
	organizationName	$\checkmark$			S	LuxTrust S.A.				
Validity		$\checkmark$	False							
	NotBefore	$\checkmark$			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 12 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate				
Subject		✓	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				

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

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

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

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

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



	LuxTrust eID S	SCD LCP				e Certificate Profile
Attribute	Field	IN <sup>24</sup>	<b>CE</b> <sup>25</sup>	<b>O/M</b> <sup>26</sup>	<b>CO</b> <sup>27</sup>	Value
	givenName	~		М	D	specimen-x provided by the RNCID
	surname	✓		М	D	specimen-x as provided by the RNCID
					_	
	countryName	✓		М	D	LU
	emailAddress	$\checkmark$		0	D	specimen-x Subject's email address as provided by the RNCID
	title	$\checkmark$		М	D	"Private Person"
	organizationalUnitName 1	$\checkmark$		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bi
	subjectPublicKey	~		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties						
authorityKey	/Identifier	√	False			
	keyldentifier	√				SHA-1 Hash of the LuxTrust Global Qualified
						CA x public key
authorityInfo		<ul> <li>✓</li> </ul>	False			
	AccessMethod	✓ ✓				Id-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/18
cRLDistribut		✓	False			
	distributionPoint	✓ ✓			S	17
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ime	✓	False			
	Rfc822Name	✓		0	D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo		✓ ✓	False			
	keyldentifier	•			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the leas significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, no including the length and number of unused bit string bits).
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓ √			S	False
certificatePo	dataEncipherment	✓ ✓	False		S	False
certificatero	Policyldentifier	✓ ✓	Faise			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	V				LuxTrust INTEGRATION CERTIFICATE of eID SSCD compliant with ETSI TS 102 04: 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	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]



VERSION 1.28

#### 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 2048bit 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:

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

The certificate re-key is not allowed.

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

	LuxTrust eID SSCD LCP Integration AE Certificate Profile									
Attribute	Field	IN <sup>13</sup>	<b>CE</b> <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value				
Base Profile										
Version		✓	False							
Version			1 0130		S	Version 3 Value = "2"				
SerialNumbe	r	✓	False		Ŭ					
					FDV	Validated on duplicates.				
signatureAlg	orithm	✓	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	ue	✓	False							
					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	~			S	LU				
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity	·	✓	False							
<u> </u>	NotBefore	✓			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 12 Months; Certificate generation process date/time + 1 day for PSEUDONYM Certificate				
subject		✓	False							
	serialNumber	~		М	D	Serial Number as constructed by LRAO				
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character				
	givenName	~		М	D	specimen-x provided by the RNCID				
	surname	~		М	D	specimen-x provided by the RNCID				
	countryName	~		М	D	LU				
	emailAddress	~		0	D	specimen-x Subject's email address as provided by the RNCID				
	title	~		М	D	"Private Person"				
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).				
subjectPublic	cKeyInfo	✓	False							
<b>*</b>	algorithm	✓				Public Key: Key length: 2048 bit up to 4096bit				
	subjectPublicKey	✓		М		(RSA); public exponent: Fermat-4 (=010001).				
Extensions										



VERSION 1.28

	LuxTrust	eID SSCI	D LCP li	ntegratio	n AE Ce	ertificate Profile
Attribute	Field	<b>IN</b> <sup>13</sup>	<b>CE</b> <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Authority Properties						
authorityKey	Identifier	√	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA x public key
authorityInfo		√	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	ionPoint	✓	False			
	distributionPoint	√			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	ime	✓	False			
•	Rfc822Name	~		0	D	specimen-x Subject's email address as provided by the RNCID
subjectKeylo	subjectKeyIdentifier		False			
	keyldentifier					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						<u> </u>
keyUsage	•	√	True			
	digitalSignature	~			S	True
	nonRepudiation				S	False
	keyEncipherment	~			S	True
	dataEncipherment	~			S	True
certificatePo		✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.17
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	noticeNumbers DisplayText	✓				LuxTrust INTEGRATION CERTIFICATE on eID SSCD compliant with ETSI TS 102 042 LCP certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Authentication and Encryption for Integration Purposes
	Policyldentifier	✓			1	0.4.0.2042.1.2

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

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

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

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

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



LuxTrust	non SSCD NCP+ Public	: Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber	1	✓	False			
		✓	<b>-</b> .		FDV	Validated on duplicates.
signatureAlgorithm	algerithm	~	False		S	OID = "1.2.840.113549.1.1.11" -
	algorithm				5	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption
signatureValue		✓	False			Shazoo with NSA Encryption
orginataro Falao			1 0100		D	Issuing CA Signature.
Issuer	1	✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	·	✓	False			
	NotBefore	~			D	Certificate generation process
		L .				date/time.
	NotAfter	~			D	Certificate generation process
aubiaat	l		<b>F</b> elow			date/time + 36 Months
subject	1	✓	False			
						Name commonly used by the subject
	commonName	$\checkmark$		М	D	to represent itself as stated in ETSI TS 119 412-3, the name should not be
						domain-shaped
						domain-snaped
						Country in which the organization's
	countryName	~		М	D	registered office is established (as
	-					specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	~		0	D	
	emailAddress	$\checkmark$		0	D	Subject's email address if available
						Names as in articles of association,
	organizationNamo	~		NA	D	including the legal form (as specified in
	organizationName	v		М		the memorandum and articles of
						association or an equivalent document)
						Location in which the organization's
						registered office is established (as
	localityName	~		М	D	specified in the memorandum and
						articles of association or an equivalent
						document)
	organizationalUnitName 1	~		0	D	As provided by Subscriber
	organizationalUnitName 2	$\checkmark$		0	D	As provided by Subscriber
subjectPublicKeyInfo	-	✓	False			
	algorithm	✓				Public Key: Key length: 2048 bit (RSA);
Forte and in	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority Properties authorityKeyIdentifier		<ul> <li>✓</li> </ul>	False			
admontykeyidentiller	keyldentifier	▼ ✓	1 8158			SHA-1 Hash of the LuxTrust Global
						Qualified CA public key
authorityInfoAccess		✓	False		1	
	AccessMethod	✓				ld-ad-2
	accessLocation	√				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓			İ	http://qca.ocsp.luxtrust.lu/
cRLDistributionPoint	1	✓	False			
	distributionPoint	~			S	
	fullName	✓			-	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						



VERSION 1.28

LuxTrust	non SSCD NCP+ Public	Cert	ificate	Profile	for Ma	ss Signature Services
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
subjectAltName		✓	False			
	Rfc822Name	$\checkmark$		0	D	Certificate Holder's email address
subjectKeyldentifier		$\checkmark$	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		~	True			
	digitalSignature	~			S	True
	nonRepudiation				S	True
	keyEncipherment	~			S	False
	dataEncipherment	~			S	False
certificatePolicies		✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.15
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	DisplayText	~				LuxTrust Certificate on Secure User Device compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. <b>Sole Authorised Usage</b> : Advanced electronic seal signature services.
	Policyldentifier	✓				0.4.0.2042.1.2

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

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

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

The usage purpose of these LuxTrust SSL/TLS Standard Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding LuxTrust LCP OID for SSL/TLS server certificates, i.e., <1.3.171.1.10.5.1>.

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

	LuxTrust SSL Server LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base Profile											
Version		$\checkmark$	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 SSL CA x <sup>17</sup>					
	organizationName	~			S	LuxTrust S.A.					
Validity		✓	False								



LuxTrust SSL Server LCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
	NotBefore	~			D	Certificate generation process date/time.			
	NotAfter	~			D	Certificate generation process date/time			
subject		✓	False			+ 12;24;36 Months			
Subject	countryName		1 0130	М	D	Country in which the company's o			
		~				institution's registered office is established (as specified in the memorandum and articles o association). (ISO3166)			
	stateOrProvinceName	✓		0	D				
	localityName			М	D	Location in which the company's			
		~				registered office is established (as specified in the memorandum and articles of association or an equivalen document)			
	organizationName	~		Μ	D	Names as in articles of association including the legal form (as specified in the memorandum and articles o 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 ful URL for a Web Server or IP address o unique name of server.			
	serialNumber	~		0	D	Serial Number as provided by subscriber			
	emailAddress	~		0	D	Subject's email address			
subjectPubli	cKeyInfo	√	False						
	algorithm	✓				Public Key: Key length: 2048 bit (RSA)			
	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).			
Extensions Authority									
Properties									
authorityKey	Identifier	✓	False						
	keyldentifier	$\checkmark$				SHA-1 Hash of the LuxTrust SSL C/ public key			
authorityInfo	Access	✓	False						
	AccessMethod	✓				Id-ad-1			
	accessLocation	~				http://ssl.ocsp.luxtrust.lu <sup>29</sup>			
	AccessMethod	$\checkmark$				Id-ad-2			
	accessLocation					http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt			
cRLDistribut		✓ ✓	False		S				
	distributionPoint fullName	× ×			5	http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl			
SCTs	1	~	False	М	D	Values returned by Log Servers			
Subject Properties									
subjectAltNa	ime	✓	False						
	Rfc822Name	~		0	D	Certificate Holder's email address			
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name of application/server – Exact DNS for a Web Server or IP address or unique name of server.			

 $<sup>^{\</sup>rm 29}$  Since SSL CA 2



	LuxTrus	t SSL S	erver LCP C	ertificate	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup> O	/M <sup>15</sup> CO <sup>1</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-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-dNSName	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.
	SubjectAltName-URL	~		0	FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.



VERSION 1.28

LuxTrust SSL Server LCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value			
	SubjectAltName-URL	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.			
subjectKeyle	dentifier	✓	False						
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).			
Policy Properties									
keyUsage		✓	True						
	digitalSignature	~			S	True			
	nonRepudiation	~			S	False			
	keyEncipherment	~			S	True			
	dataEncipherment	~			S	True			
certificatePo	olicies	✓	False						
	PolicyIdentifier	✓				1.3.171.1.1.10.5.1			
	policyQualifierID	✓			S	Id-qt-1 (CPS)			
	qualifier	✓			S	https://repository.luxtrust.lu			
	Policyldentifier	✓				0.4.0.2042.1.7			
	Policyldentifier					2.23.140.1.2.2			
Extended Ke	ey Usage	~	False						
	serverAuth	✓			S	True			
	clientAuth	✓		1	S	True			
	emailProtection	$\checkmark$			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:



VERSION 1.28

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

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

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

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

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

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

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

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

SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
SerialNumbe	er	✓	False						
					FDV	Validated on duplicates.			
signatureAlg		✓	False						
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.			
signatureVal	ue	✓	False						
					D	Issuing CA Signature.			
issuer		✓	False		S				
	countryName	✓			S	LU			
	commonName	✓			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>			
	organizationName	√			S	LuxTrust S.A.			
Validity	· •	✓	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)	~		М	D	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)			



	SSL/TLS Extended Validation Server Certificates										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value					
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	~		М	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.					
	stateOrProvinceName (OID: 2.5.4.8)	✓		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)					
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	✓		0	D	Contains the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information,					
	localityName (2.5.4.7)	✓		Μ	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)	✓		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.					
	organizationName (OID: 2.5.4.10)	✓		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.					
	businessCategory (OID: 2.5.4.15)	✓		Μ	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity					
	serialNumber (OID: 2.5.4.5)	~		М	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.					
	postalCode (OID: 2.5.4.17)	✓		0	D	Postal code of the subject place of business.					



SSL/TLS Extended Validation Server Certificates										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value				
	streetAddress			0	D	Number and Street of the physical				
	(OID: 2.5.4.9)	✓				location of the subject				
	· · · ·									
subjectPublic		✓	False							
	algorithm	✓ ✓				Public Key: Key length: 2048 bit (RSA);				
Extensions	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).				
Authority										
Properties										
authorityKey	Identifier	✓	False							
	keyldentifier	✓				SHA-1 Hash of the LuxTrust SSL CA				
			E a la a			public key				
authorityInfo		✓ ✓	False							
	AccessMethod accessLocation	▼ ✓				Id-ad-1				
		· · ·				http://ssl.ocsp.luxtrust.lu <sup>29</sup>				
	AccessMethod accessLocation	▼ ✓				Id-ad-2				
cRLDistributi		✓ ✓	- False		-	http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt				
CREDISTIDUT	distributionPoint	✓ ✓	False		S					
	fullName	▼ ✓		-	3	http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl				
						nup.//ch.iuxurusi.iu/LTSSLGAX .Cl				
SCTs		✓	False	М	D	Values returned by Log Servers				
Subject										
Properties										
subjectAltNa		✓	False							
	SubjectAltName-dNSName			М		FQDN (Fully Qualified Domain Name) of				
						application/server – Exact DNS for a				
		~				Web Server or IP address or unique name of server, owned or controlled by				
						the subject and to be associated with the				
						Subject's server. Wildcard name not				
						allowed for EV SSL Certificates.				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
						application/server - Exact DNS for a				
		~				Web Server or IP address or unique name of server, owned or controlled by				
		v				the subject and to be associated with the				
						Subject's server. Wildcard name not				
						allowed for EV SSL Certificates.				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
						application/server - Exact DNS for a				
						Web Server or IP address or unique				
		~				name of server, owned or controlled by				
						the subject and to be associated with the Subject's server. Wildcard name not				
						allowed for EV SSL Certificates				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
	-					application/server - Exact DNS for a				
						Web Server or IP address or unique				
		~				name of server, owned or controlled by				
						the subject and to be associated with the				
						Subject's server. Wildcard name not allowed for EV SSL Certificates.				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
				Ĭ		application/server – Exact DNS for a				
						Web Server or IP address or unique				
		✓				name of server, owned or controlled by				
						the subject and to be associated with the				
						Subject's server. Wildcard name not				
	SubjectAltName-dNSName	+	+	0	+	allowed for EV SSL Certificates. FQDN (Fully Qualified Domain Name) of				
	SubjectAnname-unoname					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	1	1	allowed for EV SSL Certificates.				



VERSION 1.28

	SSL/TLS Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
	SubjectAltName-dNSName			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				
				Ū.		application/server – Exact DNS for a				
						Web Server or IP address or unique				
		$\checkmark$				name of server, owned or controlled by				
						the subject and to be associated with the				
						Subject's server. Wildcard name not				
						allowed for EV SSL Certificates.				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
						application/server – Exact DNS for a Web Server or IP address or unique				
		~				name of server, owned or controlled by				
		•				the subject and to be associated with the				
						Subject's server. Wildcard name not				
						allowed for EV SSL Certificates.				
	SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of				
						application/server - Exact DNS for a				
						Web Server or IP address or unique				
		$\checkmark$				name of server, owned or controlled by				
						the subject and to be associated with the				
						Subject's server. Wildcard name not allowed for EV SSL Certificates.				
subjectKeyld	entifier	✓	False			allowed for EV 33E Certificates.				
casjeenteyla	keyldentifier	✓	1 0.50		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							
hojodago	digitalSignature	✓	1140		S	True				
	<b>3 1 3 1</b>									
	nonRepudiation	~			S	False				
		,				_				
	keyEncipherment	~			S	True				
	dataEncipherment	✓			S	True				
	uataEncipherment				5	nue				
certificatePo		✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.5.2				
	policyQualifierID	<b>√</b>	ļ		S	Id-qt-1 (CPS)				
	qualifier	<b>√</b>			S	https://repository.luxtrust.lu				
	Policyldentifier Policyldentifier	✓ √				0.4.0.2042.1.4				
Extonded	Policyldentifier	$\checkmark$	Folco			2.23.140.1.1				
Extended Ke	y Usage	v	False							
	serverAuth	✓			S	True				
	clientAuth	✓			S	True				
	emailProtection	$\checkmark$			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).



VERSION 1.28

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

#### Appropriate Certificate uses:

The primary purposes of these Certificates are to:

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

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

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

#### Prohibited Certificate uses:

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

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

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

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

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

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

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

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

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

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



	SSL/TLS Extended Validation	Serv	er Certi	ficates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
					S	Version 3 Value = "2"
SerialNumbe		✓	False			
signatureAlg	lorithm	✓	False		FDV	Validated on duplicates.
SignatureAlg	Algorithm	•	I alse		S	OID = "1.2.840.113549.1.1.11" -
						SHA256 with RSA Encryption.
signatureVal	ue	~	False			
					D	Issuing CA Signature.
Issuer	countryName	✓ ✓	False		S S	LU
	commonName	✓ ✓			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>
	organizationName	~			S	LuxTrust S.A.
Validity	organizationitanie	√ 	False		0	Edit Hust O.A.
<b>-</b>	NotBefore	✓			D	Certificate generation process
						date/time.
	NotAfter	✓			D	Certificate generation process
Subject		✓	False			date/time + 12;24 Months
Subject		•	Faise		5	
	countryName			М	D	Country in which the company's or institution's registered office is
	(OID: 2.5.4.6)	~				established (as specified in the
						memorandum and articles of
						association). (ISO3166)
	jurisdictionCountryName			М	D	Contains the country information
	(OID: 1.3.6.1.4.1.311.60.2.1.3)			141		specified using the applicable ISO
	(010. 1.3.0.1.4.1.311.00.2.1.3)					country code for the jurisdiction of
		~				Incorporation for the Incorporating
						Agency or Jurisdiction of
						Registration for a Registration Agency that operates at the country
						level, at state/pr.
	state Or Drawin as Name					Olata an Dravina is achief the
	stateOrProvinceName			М	D	State or Province in which the company's registered office is
	(OID: 2.5.4.8)					established (as specified in the
		~				memorandum and articles of
						association or an equivalent
						document)
	jurisdictionStateOrProvinceName			0	D	Contains the jurisdiction for the
	(OID: 1.3.6.1.4.1.311.60.2.1.2)					applicable Incorporating Agency or
		~				Registration Agency at the state or
						province level MUST include both country and state or province
						information,
					_	· · · · · · · · · · · · · · · · · · ·
	localityName			М	D	Location in which the company's registered office is established (as
	(2.5.4.7)	~				specified in the memorandum and
						articles of association or an
						equivalent document)
	jurisdictionLocalityName		1	0	D	Jurisdiction for the applicable
	(1.3.6.1.4.1.311.60.2.1.1)			Ŭ		Incorporating Agency or Registration
	(1.3.0.1.4.1.311.00.2.1.1)					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			м	D	Full legal organization name as
				IVI		listed in the official records of the
	(OID: 2.5.4.10)					Incorporating or Registration Agency
		✓				in the Subject's Jurisdiction of
						Incorporation or Registration or as
						otherwise verified by the CA as provided herein
						provided herein



	SSL/TLS Extended Validation	n Serve	er Certif	ficates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	businessCategory (OID: 2.5.4.15)	~		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)	~		М	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	~		0	D	Number and Street of the physical location of the subject
subjectPublic	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 bit
	subjectPublicKey	~		М		(RSA); public exponent: Fermat-4 (=010001).
Extensions Authority						
Properties authorityKey	Identifier	✓	Folgo			
authoritykey	keyldentifier	✓ ✓	False			SHA-1 Hash of the LuxTrust SSL
	-		5-1			CA public key
authorityInfo	Access AccessMethod	$\checkmark$	False			ld-ad-1
	accessLocation	▼ ✓				http://ssl.ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	· ·				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt
cRLDistribut		✓	False			Interior interior interior interior
	distributionPoint	~			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa	me	<ul> <li>✓</li> </ul>	False			
	SubjectAltName-dNSName	~		М		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.



	SSL/TLS Extended Validation	Serve	er Certif	icates	on Sec	ure User Device
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.
	SubjectAltName-dNSName	✓		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EVCP+ Certificates.



VERSION 1.28

	SSL/TLS Extended Validation Server Certificates on Secure User Device									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
subjectKey	Identifier	✓	False							
	keyldentifier	~			Fixed	The Key Identifier comprises a four- bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).				
Policy Properties										
keyUsage		✓	True							
	digitalSignature	✓			S	True				
	nonRepudiation	~			S	False				
	keyEncipherment	~			S	True				
	dataEncipherment	~			S	True				
certificateP	olicies	✓	False							
	Policyldentifier	✓				1.3.171.1.1.10.5.3				
	policyQualifierID	✓			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	Policyldentifier	✓				0.4.0.2042.1.5				
Extended K		~	False							
	serverAuth	✓			S	True				
	clientAuth	✓			S	True				
	emailProtection	✓			S	False				

#### 1.12.23 LuxTrust Object (or Code) Signing Certificates

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

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

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., <1.3.171.1.10.5.4>. This profile is not currently implemented.

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

		LuxTrust	LCP Code	Signing C	ertificate F	Profile					
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base Prof	Base Profile										
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ıber	✓	False								
					FDV	Validated on duplicates.					
signature	Algorithm	~	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signature	/alue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	~			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>					



		LuxTrust	LCP Code	Signing C	Certificate P	Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationName	✓			S	LuxTrust S.A.
Validity	I	✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 12; 24; 36 months
Subject	I	✓	False			
	countryName	~		М	D	Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	✓		0	D	
	localityName	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName1	~		0	D	As provided by Subscriber
	organizationalUnitName2	✓		0	D	As provided by Subscriber
	commonName	~		М	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	serialNumber	~		0	D	NA or Serial Number as provided by subscriber
	emailAddress	~		0	D	Subject's email address if available
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048 (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extension	s					
Authority	Properties					
authorityK	Keyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>SSL</b> CA public key
authoritylr	nfoAccess	✓	False			
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://ssl.ocsp.luxtrust.lu <sup>29</sup>
	AccessMethod	✓				Id-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt
CRLDistril	butionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl
Subject Pr		I		I	l	
subjectAlt	-	✓	False			
,,	Rfc822Name	✓		0	D	Subject's email address
	1			-	-	,



VERSION 1.28

	LuxTrust LCP Code Signing Certificate Profile											
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value						
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).						
Policy Pro	perties											
keyUsage		~	True									
	digitalSignature	~			S	True						
	nonRepudiation	~			S	False						
	keyEncipherment	~			s	False						
	dataEncipherment	~			S	False						
certificate	Policies	~	False									
	Policyldentifier	~			s	1.3.171.1.1.10.5.4						
	policyQualifierID	~			s	Id-qt-1 (CPS)						
	Qualifier	~			s	http://repository.luxtrust.lu						
	policyQualifierID	~			s	Id-qt-2 (User Notice)						
	noticeNumbers											
	DisplayText	~			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on http://repository.luxtrust.lu. 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., <1.3.171.1.10.5.5>.

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

	LuxTrust SSL Client LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNumbe	SerialNumber		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 SSL CA					



LuxTrust SSL Client LCP Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value			
-	organizationName	√			S	LuxTrust S.A.			
Validity		✓	False						
	NotBefore NotAfter	✓ ✓			D	Certificate generation process date/time. Certificate generation process date/time +			
	NotArter	v			D	12; 24; 36 Months			
Subject		✓	False						
	countryName			М	D	Country in which the company's or			
		~				institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)			
	stateOrProvinceName	~		0	D				
	localityName	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)			
	organizationName	~		Μ	D	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)			
	organizationalUnitName 1	~		0	D	As provided by Subscriber			
	organizationalUnitName 2	~		0	D	As provided by Subscriber			
	commonName	~		М	D	As provided by Subscriber			
	serialNumber	✓		0	D	Serial Number as provided by subscriber			
	emailAddress	~		0	D	Subject's email address			
subjectPubli	icKeyInfo	✓	False						
	Algorithm	√				Public Key: Key length: 2048 bit (RSA);			
-	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).			
Extensions Authority									
Properties									
authorityKey	dentifier	√	False						
	keyldentifier	~				SHA-1 Hash of the LuxTrust SSL CA public key			
authorityInfo	Access	✓	False						
	AccessMethod	√				Id-ad-1			
	accessLocation	$\checkmark$				http://ssl.ocsp.luxtrust.lu <sup>29</sup>			
	AccessMethod	✓				Id-ad-2			
	accessLocation	~				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt			
cRLDistribut		✓	False						
	distributionPoint fullName	✓ ✓	+		S				
Quitiest		, ·				http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl			
Subject Properties									
subjectAltNa	ame	✓	False						
	Rfc822Name	~		0	D	Certificate Holder's email address			
subjectKeylo		· ✓	False						
subjectivelyi	keyldentifier	✓ ✓	1 0156		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						
reyusaye	digitalSignature	×	Tue		S	True			
	nonRepudiation	✓			S	False			
					Ű				



VERSION 1.28

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

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

QCP-w: certificate policy for European Union (EU) qualified website authentication certificates, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key encryption as well as extended key usage for server and client authentication. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.5.6>.

	SSL/TLS QCP-w Extended Validation Server Certificates									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Base			1							
Profile										
Version		✓	False							
					S	Version 3 Value = "2"				
SerialNumbe	r	$\checkmark$	False							
					FDV	Validated on duplicates.				
signatureAlg		√	False							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVal	ue	$\checkmark$	False							
-					D	Issuing CA Signature.				
issuer		✓	False		S					
	countryName	<ul> <li>✓</li> </ul>		-	S	LU				
	commonName	✓			S	LuxTrust <b>SSL</b> CA x <sup>17</sup>				
	organizationName	✓			S	LuxTrust S.A.				
Validity		✓	False							
	NotBefore	<b>√</b>			D	Certificate generation process date/time.				
	NotAfter	~			D	Certificate generation process date/time + 12;24 Months				
subject		✓	False							
	countryName (OID: 2.5.4.6)	V		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)				
	jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	~		М	D	Contains the country information specified using the applicable ISO country code for the jurisdiction of Incorporation for the Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level, at state/pr.				
	stateOrProvinceName (OID: 2.5.4.8)	V		М	D	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)				
	jurisdictionStateOrProvinceNa me (OID: 1.3.6.1.4.1.311.60.2.1.2)	V		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,				



	SSL/TLS QCP-w	Extend	ed Valio	dation S	Server (	Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
	localityName (2.5.4.7)	~		М	D	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	V		0	D	Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
	organizationName (OID: 2.5.4.10)	¥		М	D	Full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein.
	businessCategory (OID: 2.5.4.15)	¥		М	D	Depending on the Subject qualifications, this field contains one of the following String: Private Organization Government Entity
	serialNumber (OID: 2.5.4.5)	*		Μ	D	See EV Guidelines [13] : For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.
	postalCode (OID: 2.5.4.17)	~		0	D	Postal code of the subject place of business.
	streetAddress (OID: 2.5.4.9)	~		0	D	Number and Street of the physical location of the subject
subjectPublic		✓	False			
	algorithm subjectPublicKey	✓ ✓		м		Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).
Extensions		v		IVI		
Authority Properties						
authorityKey		$\checkmark$	False			SHA 1 Hook of the LuxTrust COL OA
	keyldentifier	~				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 <sup>29</sup>
	AccessMethod	<ul> <li>✓</li> </ul>				ld-ad-2
	accessLocation	<ul> <li>✓</li> </ul>				http://ca.luxtrust.lu/LTSSLCAx <sup>17</sup> .crt
cRLDistributi	ionPoint	✓	False			



subjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of server or IP address or unique name of server, windcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server = Exact DNS for a very owned or controlled by the subject and to be associated with the subject and to be asso		SSL/TLS QCP-w	Extend	ed Valio	dation S	erver (	Certificates
distributionPoint         ✓         S           SCTs         ✓         Http://crl.txtrust.iul.TSSLCAr, <sup>17</sup> crl.           SUbject         ✓         False         M         D         Values returned by Log Servers           Properties         ✓         False         M         D         Values returned by Log Servers           Subject         SubjectAltName         ✓         False         M         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a subject and to be associated with the subject and to be a	Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
SCTs       ✓       False       M       D       Values returned by Log Servers         Properties		distributionPoint					
SCTs       ✓       False       M       D       Values returned by Log Servers         Properties		fullName	~				http://crl.luxtrust.lu/LTSSLCAx <sup>17</sup> .crl
Subject         Failse         M           SubjectAltName         ✓         Failse         M           SubjectAltName-dNSName         ✓         M         FQDN (Fully Qualified Domain Name) of application/server - Back DNS for a web Server or IP address or unque name of server, owned or controlled by the subject and to be associated with the Subject's server. Witcard name not server, owned or controlled by the subject and to be associated with the Subject's server. Witcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unque name of server, owned or controlled by the subject and to be associated with the subject's server. Witcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unque name of server, owned or controlled by the subject and to be associated with the subject's server. Witcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unque name of server, owned or controlled by the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject s	SCTs		✓	False	М	D	Values returned by Log Servers
Properties							
SubjectAltName-dNSName         M         FODN (Fully Cualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique harme of server, owned or controlled by the subject and to be associated with the Subject Server. Wildcard name not allowed for EV SSL certificates.           SubjectAltName-dNSName         O         FODN (Fully Cualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique or the subject and to be associated with the Subject Server. Wildcard name not allowed for EV SSL certificates.           SubjectAltName-dNSName         O         FODN (Fully Cualified 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         O         FODN (Fully Cualified 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         O         FODN (Fully Cualified 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's server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FODN (Fully Cualified 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.	Properties						
SubjectAltName-dNSName     O     FODN (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 AltName-dNSName       SubjectAltName-dNSName     O     FODN (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 AltName-dNSName       SubjectAltName-dNSName     O     FODN (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 Server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FODN (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     O     FODN (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     O     FODN (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's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a	subjectAltNa		✓	False			
v         web_Server or IP address or unique harabe 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         O         FODN (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         O         FODN (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         O         FODN (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         O         FODN (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         O         FODN (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.           Subjec		SubjectAltName-dNSName			M		
✓         name of server, owned or controlled by the subject and to be associated with the Subject as every. Wildcard name not allowed for EV SSL Certificates.      SubjectAltName-dNSName    O    FODN (Fully Qualified Domain N							
SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a web Server or IP address or unique name of server, winded or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a web Server or IP address or unique name of server, winded or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server = Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualifie							
Subject AltName-dNSName         O         Subject AltName-dNSName         O           Subject AltName-dNSName         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			v				
SubjectAltName-dNSName         0         FQCN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, wined or controlled by the subject and to be associated with the SubjectAltName-dNSName           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, wined or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         0         FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a application/server – Exact DNS for a allowed for EV SSL Certificates.							
SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, winded or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, winded or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Centificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Centificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, wildcard name not allowed for EV SSL Centificates.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, windcard n							
SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a lowed server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a lowed server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a lowed server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a lowed server.       SubjectAltName-dNSName     0     FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a lowed server.       Subje		SubjectAltName-dNSName			0		FQDN (Fully Qualified Domain Name) of
SubjectAltName-dNSName     0     arame 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     application/server - Exact DNS for a web Server. Wildcard name not allowed tor EV SSL Certificates.       SubjectAltName-dNSName     0     application/server - Exact DNS for a web Server. Wildcard name not allowed tor EV SSL Certificates.       SubjectAltName-dNSName     0     application/server - Exact DNS for a web Server. Wildcard name not allowed tor EV SSL Certificates.       SubjectAltName-dNSName     0     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server. owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server. owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a allowed for EV SSL Certificates.       SubjectAltName-dNSName     0     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a allowed for EV SSL Certificates.       SubjectAltName-dNSName<		-					application/server - Exact DNS for a
SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exac							
Subject AltName-dNSName         0         Subject AltName-dNSName         0           v         allowed for EV SSL Certificates.           subject AltName-dNSName         0         FODN (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.           Subject AltName-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.           Subject AltName-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.           Subject AltName-dNSName         0         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a veb 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.           Subject AltName-dNSName         0         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a veb 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.           Subject AltName-			~				
SubjectAltName-dNSName         O         Found for EV SSL certificates.           SubjectAltName-dNSName         O         FODN (Fully Qualified Domain Name) of aplication/server – Exact DNS for a unique name of server, owned or controlled by the subject and to be associated with the Subject Server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         O         FODN (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         O         FCDN (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         O         FCDN (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         O         FODN (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         O         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP ad							
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 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 server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard n							
subjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a value of server, owned or controlled by the subject and to be associated with the Subject AltName-dNSName         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a value of server, owned or controlled by the subject and to be associated with the Subject AltName-dNSName         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a value of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server -		SubjectAltName-dNSName			0		
v     Web Server or IP address or unique name of server, word or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O       v     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, word or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O       v     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, wined or controlled by the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with 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     O       v     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, word or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O       v     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     O     FQDN (Fully							
Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server. Windcard name not allowed for EV SSL Certificates.							Web Server or IP address or unique
SubjectAltName-dNSName     O     SubjectAltName-dNSName       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject Server. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a subjectAltName-dNSName       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a subjectAltName-dNSName       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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     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.       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server.       V     V     Server or IP address or unique name of server.       SubjectAltName-dNSName     O			✓				name of server, owned or controlled by
SubjectAltName-dNSName       O       FODN (Full) 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 Server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FODN (Full) 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 Server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FODN (Full) 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 and to be associated with the subject Server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FODN (Full) 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 and to be associated with the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FODN (Full) 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 server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FODN (Full) Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique n							,
SubjectAltName-dNSName       0       FODN (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       FODN (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       FODN (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       FODN (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       FODN (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 server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FODN (Fully Qualified Domain Name) of application/server - Exact DNS for a pplication/server - Exact DNS for a pplication/server - Exact DNS for a allowed for EV SSL Certificates.         SubjectAltName-dNSName       0 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
subjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject and to be associated with the Subject and to be associated with the Subject and to be associated with the Subject server. Wildcard name not 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 Subjects server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>							
SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a very of the subject and to be associated with the subject as enver, wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a very the subject and to be associated with the subject as envery. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a very be associated with the subject as envery. Wildcard name not allowed for EV SSL Certificates.       SubjectAltName-dNSName     O     FQDN		SubjectAltname-dnSname			0		
SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique ame of server, owned or controlled by the subject and to be associated with the Subject Server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique mame of server, owned or controlled by the subject and to be associated with the Subject Server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique mame of server, owned or controlled by the subject and to be associated with the Subject's server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique mame of server, owned or controlled by the subject and to be associated with the Subject's server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server.           SubjectAltName-dNSName         O         FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a UVeb Server or IP address or unique name of server, owned or con							
SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the SubjectAltName-dNSName           SubjectAltName-dNSName         0         FODN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.           SubjectAltName-dNSName         0         FODN (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. <t< td=""><td></td><td></td><td>~</td><td></td><td></td><td></td><td></td></t<>			~				
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 and to be associated with the Subject AltName-dNSName         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name							the subject and to be associated with the
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'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'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'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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       0       FQDN (Fully Qualif							Subject's server. Wildcard name not
Image: Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, windcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         Subject AltN							
Image: subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of Server. Wildcard name not allowed for EV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of TeV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of TeV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of TeV SSL Certificates.         Subject AltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a UNdext of TeV SSL Certificates.         Subject AltName-dNSName       O		SubjectAltName-dNSName			0		
Image: state of the subject and to be associated with the subject and to be associated with the subject and to be associated with the subject is server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Full) 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       O       FQDN (Full) 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       O       FQDN (Full) 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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							application/server – Exact DNS for a
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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       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 server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subjects server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificat			1				
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, winde or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.			·				
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a pplication/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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.							
Image: SubjectAltName-dNSName       O       FGDN (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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FGDN (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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FGDN (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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.							
V       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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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
Image: sever control in 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.							application/server - Exact DNS for a
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL certificates.			,				
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not 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 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 Subject's server. Wildcard name not Subject's server. <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>,</td>							,
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.		SubjectAltName-dNSName		1	0		
Image: SubjectAltName-dNSName       Image: SubjectAltName-dNSName		,			_		application/server – Exact DNS for a
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       ✓       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.							Web Server or IP address or unique
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       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's server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.			✓				name of server, owned or controlled by
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not 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 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 server.							
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, 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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server. Wildcard name not allowed for EV SSL Certificates.         SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not and the subject's server. Wildcard name not and the subject's server.							
✓       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       O       FQDN (Fully Qualified Domain Name) of application/server - Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.         ✓       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		Subject AltName_dNSName			0		
✓       ✓       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       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.		SubjectAttivanie-unonanie					
✓       Image: Subject AltName-dNSName       ✓       Image: Subject AltName-dNSName       ✓       ✓       Image: Subject AltName-dNSName       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's server. Wildcard name not 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 application for the subject and to be associated with the subject's server. Wildcard name not server.							
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject's server. Wildcard name not allowed for EV SSL Certificates.			✓				name of server, owned or controlled by
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not							the subject and to be associated with the
SubjectAltName-dNSName       O       FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not							Subject's server. Wildcard name not
<ul> <li>✓</li> <li>✓</li> <li>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</li> </ul>				<u> </u>			allowed for EV SSL Certificates.
<ul> <li>✓</li> <li>✓</li> <li>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</li> </ul>		SubjectAltName-dNSName			0		
<ul> <li>✓ name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not</li> </ul>							
the subject and to be associated with the Subject's server. Wildcard name not			1				
Subject's server. Wildcard name not			•				
allowed for EV SSL Certificates.							



VERSION 1.28

	SSL/TLS QCP-w	/ Extend	ed Valio	lation S	Server (	Certificates
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	SubjectAltName-dNSName	~		0		FQDN (Fully Qualified Domain Name) of application/server – Exact DNS for a Web Server or IP address or unique name of server, owned or controlled by the subject and to be associated with the Subject's server. Wildcard name not allowed for EV SSL Certificates.
subjectKeyld		✓	False			
De l'est	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			
keyUsage	digitalSignature	▼ ✓	True		S	True
					_	
	nonRepudiation	~			S	False
	keyEncipherment	~			S	True
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	~				1.3.171.1.1.10.5.6
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	Policyldentifier	~				0.4.0.194112.1.4
	Policyldentifier	~				0.4.0.2042.1.4
	Policyldentifier	~			S	2.23.140.1.1
Extended Ke	y Usage	~	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	False
QualifiedCer	tificateStat	~	False			
	QcCompliance (0.4.0.1862.1.1)	~		М	S	True
	QcPDS (0.4.0.1862.1.5)	<b>v</b>		М	S	https://www.luxtrust.lu/upload/data/repos itory/PDS.pdf
	QcType (0.4.0.1862.1.6)	✓		М	S	id-etsi-qct-web (0.4.0.1862.1.6.3)

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

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

These LuxTrust Signing Server Account LCP Certificates are compliant with and include the OID reference of the LCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.3; cf. [4]). The usage purpose of these Certificates is only authentication <OID 1.3.171.1.1.0.3.20>.

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

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



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			
					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.			
signatureValu	e		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						
ranary			1 0.00						
	NotBefore				D	Certificate generation process date/time.			
	NotAfter				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 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	<b>CSS or</b> Surname(s) as on ID document without indication "épouse", "ép." or similar and the subsequent name(s)			
	countryName		1	М	D	LU or Nationality of holder (ISO3166)			
	emailAddress			0	D	N/A			
	Title			М	D	Private Person			
subjectPublic	l KeyInfo		False						
	Algorithm					Public Key: Key length: 2048 bit (RSA); public exponent: Fermat-4 (=010001).			
	subjectPublicKey			М					



	SPARE	LuxTrus	st Signing	g Server LO	CP Certifie	cate Profile
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
Extensions						
Authority Properties						
authorityKeyld	lentifier		False			
	keyldentifier					SHA-1 Hash of the LuxTrust <b>Global</b> <b>Qualified</b> CA public key
authorityInfoA	ccess		False			
	AccessMethod					ld-ad-2
	accessLocation					http://ca.luxtrust.lu/LTGQCAx <sup>22</sup> .crt
	AccessMethod					ld-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>23</sup>
cRLDistributio	nPoint		False			
	distributionPoint				S	
	fullName					http://crl.luxtrust.lu/LTGQCAx <sup>22</sup> .crl
Subject Properties						
subjectAltNam	ie		False			
	Rfc822Name			0	D	N/A
subjectKeylde	ntifier		False			
	keyldentifier				Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage			True			
	digitalSignature				S	True
certificatePolic	cies		False			
	Policyldentifier					1.3.171.1.1.10.3.20
	policyQualifierID				S	Id-qt-1 (CPS)
	Qualifier				S	https://repository.luxtrust.lu
	Policyldentifier					0.4.0.2042.1.3



VERSION 1.28

#### 1.12.27 LuxTrust Qualified eSEAL - Certificate Profile supporting digital signature

LuxTrust Certificates for Qualified Seal Signature Services are Qualified Certificates certified as generated on Secure User Device, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing qualified electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of qualified eseals supported by Qualified Certificate compliant with ETSI EN 319 411-2 [20] QCP-l-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.21>. The following table provides the description of the fields for LuxTrust Qualified Certificates for digital signatue purpose.

	LuxTrust Qualified eSEAL Certificate Profile										
Attribute	Field	IN <sup>30</sup>		O/M <sup>32</sup>	<b>CO</b> <sup>33</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	lue	✓	False								
					D	Issuing CA Signature.					
Issuer		✓	False		S						
	countryName	✓			S	LU					
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>34</sup>					
	organizationName	✓			S	LuxTrust S.A.					
Validity		✓	False								
	NotBefore	✓			D	Certificate generation process date/time.					
	NotAfter	✓			D	Certificate generation process date/time + 24 Months					
Subject		✓	False								
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).					
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)					

 $<sup>^{30}</sup>$  IN = Included: Attribute / field included within the certify

cate profile.

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

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

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

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



VERSION 1.28

	organisationldentifier (2.5.4.97)	~		М	D	<ul> <li>Shall contain information using the following structure in the presented order: <ul> <li>3 character legal person identity type reference;</li> <li>2 character ISO 3166 country code;</li> <li>hyphen-minus "-" and</li> <li>identifier (according to country and identity type reference).</li> </ul> </li> <li>The three initial characters shall have one of the following defined values: <ul> <li>"VAT" for identification based on a national value added tax identification number.</li> <li>"NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).</li> <li>When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identify type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.</li> </ul></li></ul>
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPubli	cKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	√		М		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	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/35
cRLDistribut	ionPoint	√	False			
	distributionPoint	√			S	
	fullName	$\checkmark$				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeylo	lentifier	√	False			
	keyldentifier	<b>v</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).

<sup>35</sup> SINCE LTGQCA3



VERSION 1.28

Policy						
Properties						
keyUsage		$\checkmark$	True			
dig	italSignature	$\checkmark$			S	False
nor	nRepudiation	✓			S	True
key	/Encipherment	✓			S	False
dat	aEncipherment	✓			S	False
certificatePolicie	S	✓	False			
	Lu	xTrust	NCP+	Certifica	te Profil	le for authentication
						1.0.171.1.11.10.0.21
	licyQualifierID	✓			S	Id-qt-1 (CPS)
	alifier	✓			S	https://repository.luxtrust.lu
	licyQualifierID	✓			S	Id-qt-2 (User Notice)
Pol	licyldentifier	$\checkmark$				0.4.0.194112.1.3
QualifiedCertifica	ateStat	$\checkmark$	False			
Qc	Compliance	✓		М	S	True
(0.4	4.0.1862.1.1)					
Qc	SSCD	✓		М	S	True
(0.4	4.0.1862.1.4)					
Qcl	PDS	✓		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
(0.4	4.0.1862.1.5)					
Qc	Туре (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-eseal
						(0.4.0.1862.1.6.2)

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

Keys are generated on Secure User Device, with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date. This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eseals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.22>.



VERSION 1.28

Attribute	Field	IN <sup>36</sup>	CE <sup>37</sup>	O/M <sup>38</sup>	CO <sup>39</sup>	Value
Base						
Profile						
Version	1	✓	False			
O a si a lh la sea la s		✓	Estas		S	Version 3 Value = "2"
SerialNumbe	er	v	False			Validated an durblaster
oignoturo Ale		✓	Foloo		FDV	Validated on duplicates.
signatureAlg	Algorithm	•	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	Algorithm				3	Encryption.
signatureVa		✓	False			
Signature Val		-	1 2130		D	Issuing CA Signature.
Issuer		✓	False		S	
10000	countryName	✓	1 0100		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>40</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	<u>j</u>	✓	False			
y	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
				101		established (ISO3166)
	organisationIdentifier (2.5.4.97)	~		М	D	<ul> <li>Shall contain information using the following structure in the presented order: <ul> <li>3 character legal person identity type reference;</li> <li>2 character ISO 3166 country code;</li> <li>hyphen-minus "-" and</li> <li>identifier (according to country and identity type reference).</li> </ul> </li> <li>The three initial characters shall have one of the following defined values: <ul> <li>1) "VAT" for identification based on a national value added tax identification number.</li> <li>2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).</li> <li>When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.</li> </ul></li></ul>
	organizationName	~		м	D	Shall contain the full registered name of the subject (legal person).

 $<sup>^{36}</sup>$  IN = Included: Attribute / field included within the certify

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

cate profile.

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

 $<sup>^{39}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

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



VERSION 1.28

		1		1	1	
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPubli	icKevInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
		LuvT	rust Adv	anced a	SEAL C	Certificate Profile
		Luxi	I USI AUI			
Authority						
Properties						
authorityKey	/Identifier	✓	False			
uuiioiiijitoj	keyldentifier	√	1 4100			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
additiontyline	AccessMethod	✓	1 0100			Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	√				Id-ad-1
	accessLocation	, ,				http://qca.ocsp.luxtrust.lu/ <sup>41</sup>
cRLDistribut		√	False			
CILEDISTIDU	distributionPoint	· √	1 0136		S	
	fullName	· ·			3	http://crl.luxtrust.lu/LTGQCAx17.crl
Subject	Tullivallie					
Properties						
subjectKeylo	lentifier	√	False			
Subjective yre	keyldentifier	· •	1 2130		Fixed	The Key Identifier comprises a four-bit field with a 0100
					TIXEG	value, followed by the least significant 60 bits of the SHA- 1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy						
Properties						
keyUsage		~	True			
	digitalSignature	~			S	True
	nonRepudiation	~			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.22
	policyQualifierID	✓	1		S	Id-gt-1 (CPS)
	qualifier	✓	1		S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	√				0.4.0.2042.1.2

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

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

<sup>&</sup>lt;sup>41</sup> SINCE LTGQCA3



Attribute	Field	IN <sup>42</sup>	CE <sup>43</sup>	O/M <sup>44</sup>	<b>CO</b> <sup>45</sup>	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
		✓	<b>_</b> .			Encryption.
signatureVal	lue	~	False			
locuor		√	Falaa		D S	Issuing CA Signature.
Issuer	e e un tru Nome	▼ ✓	False		S	
	countryName commonName	▼ ✓			S	LU LuxTrust <b>Global Qualified</b> CA x <sup>46</sup>
	organizationName	· ✓			S	LuxTrust S.A.
Validity	organizationName	▼ ✓	False		3	Lux Trust S.A.
Validity	NotBefore	v √	raise		D	Certificate generation process data/time
	NotAfter	▼ ✓			D	Certificate generation process date/time. Certificate generation process date/time + 24 Months
Subject	NotAitei	<b>↓</b>	False		D	Certificate generation process date/time + 24 Months
Subject	commonName	✓	Faise	М	D	Shall contain the full registered name of the subject (legal person).
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)
	organisationIdentifier (2.5.4.97)	×		М	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier.
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).

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

cate profile.

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

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

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

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



VERSION 1.28

			1		1	
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPubli	icKevInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
		LuvT	rust Adv	anced e	SEAL C	Certificate Profile
		Luxi				
Authority Properties						
authorityKey	/Identifier	✓	False			
uuliontynoj	keyldentifier	~	1 0.00			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo	Access	✓	False			
· · · · · ·	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/4/
cRLDistribut		$\checkmark$	False			
	distributionPoint	~			S	
	fullName	~			-	http://crl.luxtrust.lu/LTGQCAx17.crl
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	False
	nonRepudiation	√			S	True
	keyEncipherment	√			S	False
	dataEncipherment	✓	1		S	False
certificatePo		✓	False		_	
	Policyldentifier	~				1.3.171.1.1.10.3.23
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	$\checkmark$			-	0.4.0.2042.1.2

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

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

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





Attribute	Field	IN <sup>48</sup>	<b>CE</b> <sup>49</sup>	O/M <sup>50</sup>	CO <sup>51</sup>	Value
Attribute Base	Field		UE .	0/1	0.0	Value
Profile						
Version		✓	False			
Version			1 0.50		S	Version 3 Value = "2"
SerialNumb	er en en en en en en en en en en en en en	✓	False			
Genandumb		-	1 2130		FDV	Validated on duplicates.
signatureAl	norithm	✓	False		TDV	
SignatureAi	Algorithm	-	1 0.50		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	,				Ŭ	Encryption.
signatureVa	lue	✓	False			
orginatarora			1 0100		D	Issuing CA Signature.
Issuer		✓	False		S	
100001	countryName	✓	1 0100		S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>52</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	o.gamzatomane	· ·	False			
valialty	NotBefore	· ·	1 0130		D	Certificate generation process date/time.
	NotAfter	· ✓			D	Certificate generation process date/time + 24 Months
Subject	NotAltei	· ✓	False			
Jubject			1 2130			Shall contain the full registered name of the subject (legal
	commonName	$\checkmark$		М	D	person).
		-				the country in which the subject (legal person) is
	countryName	$\checkmark$		М	D	established (ISO3166)
	organisationIdentifier (2.5.4.97)	*		М	D	Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified
	organizationName	~		М	D	uniformResourceIdentifier. Shall contain the full registered name of the subject (legal person).

 $<sup>^{\</sup>rm 48}$  IN = Included: Attribute / field included within the certify

 $^{50}$  O/M: O = Optional, M = Mandatory.

cate profile.

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

 $<sup>^{51}</sup>$  CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

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



VERSION 1.28

г		1	1			
	organizationalUnitName	~		0	D	Company/institution department or other information item
	serialNumber	~		М	D	Serial Number as constructed by LRAO
subjectPublic	cKevInfo	√	False			
	Algorithm	√				Public Key: Key length: 2048bit up to 4096bit (RSA);
	subjectPublicKey	√		М		public exponent: Fermat-4 (=010001).
Extensions	, ,					
Authority Properties						
authorityKey	Identifier	√	False		1	
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInfo		✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	$\checkmark$				http://ca.luxtrust.lu/LTGQCAx17.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/53
cRLDistributi		$\checkmark$	False			
_	distributionPoint	$\checkmark$			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCAx17.crl
Subject Properties						
subjectKeyld		$\checkmark$	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			
Reyusaye	digitalSignature	▼ ✓	nue		S	True
	nonRepudiation	· •			S	False
ŀ	keyEncipherment	· ✓			S	True
ŀ	dataEncipherment	· •			S	False
certificatePol		· √	False			
certificater of	Policyldentifier	√	1 0130			
	,					1.3.171.1.1.10.3.24
ľ	policyQualifierID	√			S	Id-qt-1 (CPS)
ſ	qualifier	√			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	ponoyquanterib					

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

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

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

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





Base Profile       Version       ✓       False       Version 3 Value = "2"         SerialNumber       ✓       False       S       Version 3 Value = "2"         SerialNumber       ✓       False       FDV       Validated on duplicates.         signatureAlgorithm       ✓       False       DID = "1.2.840.113549.1.1.11" - SHA256 with RSA         SignatureValue       ✓       False       D       Issuing CA Signature.         (signatureValue       ✓       False       D       Issuing CA Signature.         (signatureValue       ✓       False       S       LU         (countryName       ✓       S       LuxTrust Global Qualified CA x <sup>m</sup> (roganizationName       ✓       S       LuxTrust Global Qualified CA x <sup>m</sup> Validity       ✓       False       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       D       Certificate generation process date/time + 24 Months         (countryName       ✓       M       D       Shall contain the full registered name of the subject (legal person) is established (ISO3166)         (countryName       ✓       M       <		Lux <sup>-</sup>			d Automated eSEAL Certificate Profile					
Profile       v       False       v         Version       v       False       S       Version 3 Value = "2"         SerialNumber       v       False       FDV       Validated on duplicates.         signatureAlgorithm       v       False       FDV       Validated on duplicates.         signatureAlgorithm       v       False       S       OID = "1.2.840.113549.11.11" - SHA256 with RSA Encryption.         signatureAlgorithm       v       False       S       OID = "1.2.840.113549.11.11" - SHA256 with RSA Encryption.         issuer       v       False       S       U       Staing CA Signature.         issuer       v       False       S       LU       S         commonName       v       S       LuxTrust Global Qualified CA x <sup>38</sup> S         validity       v       False       D       Certificate generation process date/time.         NotAfter       v       D       Certificate generation process date/time.       A Moths         subject       v       False       D       Certificate generation process date/time.       A Moths         countryName       v       M       D       Shall contain the full registered name of the subject (legal person) is estaished (ISO3166)       Shall contain information	Attribute	Field	IN <sup>54</sup>	CE	O/M <sup>56</sup>	CO <sup>57</sup>	Value			
SerialNumber       Version 3 Value = "2"         SerialNumber       Validated on duplicates.         signatureAlgorithm       Validated on duplicates.         Algorithm       Validated on duplicates.         SignatureValue       Validated on duplicates.         countryName       S         validity       Validated on duplicates.         validi										
SerialNumber       ✓       False       ✓         signatureAlgorithm       ✓       False       OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.         signatureValue       ✓       False       OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.         signatureValue       ✓       False       D       Issuing CA Signature.         issuer       ✓       False       S       UU         commonName       ✓       S       LU       Uu         organizationName       ✓       S       LuxTrust Global Qualified CA x <sup>100</sup> NotEfere       ✓       S       LuxTrust S.A.         NotEfere       ✓       D       Certificate generation process date/time.         NotAfter       ✓       D       Certificate generation process date/time.         Subject       ✓       False       O       Certificate generation process date/time.         commonName       ✓       M       D       Ball contain the full registered name of the subject (legal person) is established (ISO3166)         countryName       ✓       M       D       Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character legal field. Unity and identifier (according to country and identifier from a national trade register. Or two characters accord	Version		✓	False						
signatureAlgorithm     ✓     False     ✓       Algorithm     ✓     False     ✓       signatureValue     ✓     False     ✓       Super Su						S	Version 3 Value = "2"			
signatureAlgorithm       ✓       False       ✓         Algorithm       ✓       False       S       OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.         signatureValue       ✓       False       D       Issuing CA Signature.         Issuer       ✓       False       S       Uu         countryName       ✓       S       LU         commonName       ✓       S       LuxTrust Global Qualified CA x <sup>ise</sup> organizationName       ✓       False       D       Certificate generation process date/time.         NotAfter       ✓       False       D       Certificate generation process date/time.         Subject       ✓       False       D       Certificate generation process date/time.         validity       ✓       False       D       Certificate generation process date/time.         countryName       ✓       False       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       Shall contain information using the following structure in the presented order:         scharacter SQL       K       M       D       Shall contain full registered name of the subject (legal person).         relation       Y       M       D       Shall	SerialNumbe	er	✓	False						
Algorithm       ✓       S       OID = "1.2840.113549.1.1.11" - SHA256 with RSA Encryption.         signatureValue       ✓       False       D       Issuing CA Signature.         Issuer       ✓       False       S       LuxTrust Global Qualified CA X <sup>38</sup> commonName       ✓       False       S       LuxTrust Global Qualified CA X <sup>38</sup> organizationName       ✓       False       S       LuxTrust Global Qualified CA X <sup>38</sup> Validity       ✓       False       D       Certificate generation process date/time.         Validity       ✓       False       D       Certificate generation process date/time.         Subject       ✓       False       D       Certificate generation process date/time.         countryName       ✓       M       D       Shall contain the full registered name of the subject (legal person) is established (ISO3166)         sharacter legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus ** and identifier (according to country and identifier (according to country and identifier form a national trade register. Or two characters according to looke; hyphen-minus ** and identifier doralues:         (2.5.4.97)       ✓       M       D       Increation attender (actording to country and identifier form a national trade register is on an ational value added tax identification name registration authority. Identifing a national ach						FDV	Validated on duplicates.			
signatureValue       ✓       False       Encryption.         issuer       ✓       False       D       Issuing CA Signature.         issuer       ✓       False       S       LU         commonName       ✓       S       LU         organizationName       ✓       S       LuxTrust Global Qualified CA x <sup>set</sup> Validity       ✓       False       S       LuxTrust S.A.         Validity       ✓       False       Certificate generation process date/time.         NotAfter       ✓       D       Certificate generation process date/time.         NotAfter       ✓       False       CommonName       ✓         commonName       ✓       False       False       False         commonName       ✓       M       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       Shall contain information using the following structure in the presented order:       3 character legal person identity type reference;         commonName       ✓       M       D       Shall contain information using the following structure in the presented order:         scalaritifier       (cooffiguate contry in which the subject (legal person identity type reference;)       2 character legal p	signatureAlg		✓	False						
Issuer     V     False     D     Issuing CA Signature.       Issuer     ✓     False     S     LU       commonName     ✓     S     LuXTrust Global Qualified CA x <sup>36</sup> organizationName     ✓     S     LuXTrust Global Qualified CA x <sup>36</sup> Validity     ✓     False     D     Certificate generation process date/time.       NotAfter     ✓     D     Certificate generation process date/time.       NotAfter     ✓     False     D       CommonName     ✓     False     D       countryName     ✓     False     D       countryName     ✓     M     D     Shall contain the full registered name of the subject (legal person) is established (ISO3166)       countryName     ✓     M     D     Shall contain information using the following structure in the presented order: 3 character IsO3 3166 country code; hyphen-minus ** and identifier (according to country and identify type reference). The three initial characters shall have one of the following defined values:       organisationIdentifier     ✓     M     D       (2.5.4.97)     ✓     M     D		-				S				
Issuer       ✓       False       S         countryName       ✓       S       LuxTrust Global Qualified CA x <sup>38</sup> organizationName       ✓       S       LuxTrust S.A.         Validity       ✓       False       D       Certificate generation process date/time.         NotBefore       ✓       D       Certificate generation process date/time.       24 Months         Subject       ✓       False       D       Certificate generation process date/time.       24 Months         Subject       ✓       False       D       Certificate generation process date/time.       24 Months         Subject       ✓       False       D       Certificate generation process date/time.       24 Months         Subject       ✓       False       D       Certificate generation process date/time.       24 Months         countryName       ✓       M       D       Shall contain information using the following structure in the presented order:       3 character legal person identify type reference;       3 character legal person identify type reference;       2 character lSO 3166 country and identifier (according to country and identifier (according to country and identifier (according to country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).         M	signatureVal	ue	✓	False						
countryName       ✓       S       LU         commonName       ✓       S       LuxTrust Global Qualified CA x <sup>301</sup> organizationName       ✓       S       LuxTrust S.A.         Validity       ✓       False       D       Certificate generation process date/time + 24 Months         NotAfter       ✓       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       O       Certificate generation process date/time + 24 Months         Subject       ✓       False       O       Certificate generation process date/time + 24 Months         Subject       ✓       False       O       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       Shall contain information using the following structure in the presented order:         scharacter ISO 3166       Shall contain information using the following structure in the presented order:       Scharacter ISO 3166 country code; hyphen-minus '-'' and identification number.         (z.5.4.97)       ✓       M       D       Subracter legal person identify type reference; 2 character ISO 3166 country and identify type reference).         (z.5.4.97)       ✓       M       D       Interface daperopriate for national and European level, followed by the character ''. (coln).							Issuing CA Signature.			
commonName         ✓         S         LuxTrust Global Qualified CA x <sup>36</sup> organizationName         ✓         S         LuxTrust SA.           Validity         ✓         False         ✓           NotAfter         ✓         D         Certificate generation process date/time + 24 Months           Subject         ✓         False         ✓         D         Certificate generation process date/time + 24 Months           Subject         ✓         False         ✓         D         Certificate generation process date/time + 24 Months           CommonName         ✓         M         D         Shall contain the full registered name of the subject (legal person).           countryName         ✓         M         D         the country in which the subject (legal person) is established (ISO3166)           commonName         ✓         M         D         Shall contain information using the following structure in the presented order: 3 character ISO 3166 country code; hyphen-mius "-" and identifier (according to country and identifier (according to country and identifier (according to country and identifier form a national trade register: Or Two characters according to local definition within the specified country and name registration authority, identification name           (2.5.4.97)         ✓         M         D         P         Contain information usele to rational and European level, followed by the character ":"	Issuer			False						
organizationName         ✓         S         LuxTrust S.A.           Validity         ✓         False         D         Certificate generation process date/time.           NotAfter         ✓         D         Certificate generation process date/time + 24 Months           Subject         ✓         False         D         Certificate generation process date/time + 24 Months           CommonName         ✓         M         D         Shall contain the full registered name of the subject (legal person).           countryName         ✓         M         D         Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character lSO 3166 country code; hyphen-minus "." and identifier (according to country and identify type reference).           reference).         There initial characters shall have one of the following defined values:         1) "VAT" for identification based on an identifier from a national trade register. Or two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character 5 (lowed by "."), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain a least a			-							
Validity       ✓       False       ✓         Notafter       ✓       D       Certificate generation process date/time.         Subject       ✓       False       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       Shall contain the full registered name of the subject (legal person) is established (ISO3166)         countryName       ✓       M       D       Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character IsO 3166 country code; hyphen-minus "." and identifier (according to country and identify type reference). The three initial character shall have one of the following defined values:         (2.5.4.97)       ✓       M       D       D         M       D       Notaret registration authority, identification based on a national value added tax identification mither.         (2.5.4.97)       ✓       M       D       D         M       D       Notaret registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by the character sollowed by the character sollowed by the character sollowed by the character sollowed by the			-							
NotBefore       ✓       D       Certificate generation process date/time.         NotAfter       ✓       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       ✓       D       Certificate generation process date/time.       24 Months         Subject       ✓       False       ✓       M       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         organisationIdentifier       ✓       M       D       Shall contain information using the following structure in the presented order:         (2.5.4.97)       ✓       M       D       The three initial characters shall have one of the following defined values:         (2.5.4.97)       ✓       M       D       D       The three initial characters shall have one of the following defined values:         (2.5.4.97)       ✓       M       D       D       D       The three initial characters shall have one of the following defined values:         (2.5.4.97)       ✓       M       D       D       D       D       D         In three initial character eigister. Or Two characters according to local definition within the specified country and name registration authority, identifyi		organizationName	-	<b>F</b> -1		5	Lux I rust S.A.			
NotAfter       ✓       D       Certificate generation process date/time + 24 Months         Subject       ✓       False       ✓       M       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       Shall contain the full registered name of the subject (legal person) is established (ISO3166)         countryName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         organisationIdentifier       ✓       M       D       Shall contain information using the following structure in the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus *-* and identifier (according to country and identity type reference).         organisationIdentifier       ✓       M       D       D       Intertification number.       2) "NTR" for identification based on a national value added tax identification number.       2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character science is provided (two characters followed by *::), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a	validity	NetDefere		False						
Subject       ✓       False       ✓         commonName       ✓       M       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         commonName       ✓       M       D       Shall contain information using the following structure in the presented order: 3 character ISO 3166 country code; hyphen-minus "-" and identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identity type reference).         organisationIdentifier       ✓       M       D       Shall contain information using the following structure in the presented order: 3 character ISO 3166 country code; hyphen-minus "-" and identify type reference).         (2.5.4.97)       ✓       M       D       The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).         When a locally defined identify type reference is provided (two characters followed by ":"), the nameRegistration(IETF RFC 3739 [1]) shall be present and shall contain at least a			-							
commonName       ✓       M       D       Shall contain the full registered name of the subject (legal person).         countryName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         countryName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         commonName       ✓       M       D       the country in which the subject (legal person) is established (ISO3166)         commonName       ✓       M       D       Shall contain information using the following structure in the presented order:         a character legal person identity type reference;       2 character legal person identity type reference;       2 character legal person identity type reference;         corganisationIdentifier       ✓       M       D       The three initial characters shall have one of the following defined values:         (2.5.4.97)       ✓       M       D       D       WTM for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character "." (colon).         when character stollowed by the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a	Cubicat	NotAfter		Falaa		D	Certificate generation process date/time + 24 Months			
countryName       v       M       D       person).         countryName       v       M       D       the country in which the subject (legal person) is established (ISO3166)         Shall contain information using the following structure in the presented order:       Shall contain information using the following structure in the presented order:         GranisationIdentifier       v       M       D       Shall contain information using the following structure in the presented order:         (2.5.4.97)       v       M       D       Shall contain information using the following structure in the presented order:         (2.5.4.97)       v       M       D       Shall contain information using the following structure in the presented order:         (2.5.4.97)       v       M       D       Shall contain information using the following identifier form a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).       When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistration Authorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a	Subject	[	v	Faise			Chall contain the full registered name of the publicat (level			
Country Name       V       M       D       established (ISO3166)         Image: Shall contain information using the following structure in the presented order:       3 character legal person identity type reference;       2 character legal person identity type reference;         3 character legal person identity type reference;       2 character legal person identity type reference;       2 character legal person identity type reference;         4 character legal person identity type       3 character legal person identity type reference;       2 character legal person identity type         6 organisationIdentifier       M       M       D       The three initial characters shall have one of the following defined values:         1) "VAT" for identification based on a national value added tax identification number.       2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).         When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a		commonName	✓		М	D	person).			
organisationIdentifier (2.5.4.97)MDMDImage: Section 10 and 10		countryName	✓		М	D				
<sup>54</sup> IN = Included: Attribute / field included within the certify		(2.5.4.97)			М	D	the presented order: 3 character legal person identity type reference; 2 character ISO 3166 country code; hyphen-minus "-" and identifier (according to country and identity type reference). The three initial characters shall have one of the following defined values: 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon). When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceldentifier generalName. The two letter			

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

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

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



VERSION 1.28

organizationName       ✓       M       D       Shall contain the full registered name of the superson).         organizationalUnitName       ✓       O       D       Company/institution department or other information.	ubject (legal
	mation item
subjectPublicKeyInfo	
Algorithm ✓ Public Key: Key length: 2048bit up to 40	96bit (RSA);
subjectPublicKey ✓ M public exponent: Fermat-4 (=010001).	( )/
Extensions	
Authority	
Properties	
authorityKeyldentifier	
keyldentifier ✓ SHA-1 Hash of the LuxTrust Global Qualifien key	<b>∍d</b> CA public
authorityInfoAccess	
AccessMethod ✓ Id-ad-2	
accessLocation  Intp://ca.luxtrust.lu/LTGQCAx17.crt	
AccessMethod ✓ Id-ad-1	
accessLocation ✓ http://qca.ocsp.luxtrust.lu/ <sup>59</sup>	
cRLDistributionPoint ✓ False	
distributionPoint 🗸 S	
fullName ✓ http://crl.luxtrust.lu/LTGQCAx17.crl	
Subject Properties	
subjectKeyldentifier	
keyldentifier       ✓       Fixed       The Key Identifier comprises a four-bit field value, followed by the least significant 60 bits 1 hash of the value or subjectPublicKey bit st including the length and number of unused bit	of the SHA- tring (tag, not
Policy Policy	
Properties	
keyUsage V True	
digitalSignature   S False	
nonRepudiation   S True	
keyEncipherment	
dataEncipherment     ✓     S     False	
certificatePolicies     ✓     False	
Policyldentifier         ✓         1.3.171.1.10.3.25	
policyQualifierID ✓ S Id-qt-1 (CPS)	
qualifier	
policyQualifierID ✓ S Id-qt-2 (User Notice)	

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

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.26>.

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

### <sup>59</sup> SINCE LTGQCA3

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

 $^{61}$  CE = Critical Extension.

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

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



	Lu	xTrus	t Smart	Card Q	CP-n-c	scd Certificate Profile
Attribute	Field	IN <sup>60</sup>	CE <sup>61</sup>	O/M <sup>62</sup>	CO 63	Value
Version		✓	False			
			. 0.00		S	Version 3 Value = "2"
SerialNum	ber	✓	False			
					FDV	Validated on duplicates.
signature		✓	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
	Algorithm				3	Encryption.
signature	/alue	✓	False			
-					D	Issuing CA Signature.
Issuer	a a constructivo de la construcción de la construcción de la construcción de la construcción de la construcción	$\checkmark$	False		S	
	countryName commonName	▼ ✓			S S	
		· ·				LuxTrust Global Qualified CA x <sup>64</sup>
Validity	organizationName	✓ ✓	False		S	LuxTrust S.A.
valuity	NotBefore	▼ ✓	Faise		D	Certificate generation process date/time.
	NotAfter	· ✓			D	Certificate generation process date/time + <b>36</b> Months
Subject	1100 1101	✓	False			
	serialNumber	✓		м	D	Serial Number as constructed by LRAO
		<u>↓ ·</u>	<u> </u>	101		,
	commonName	~		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	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		м	D	<b>PRO and PRIVATE products</b> : 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	¥		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	<b>PRO products only:</b> Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		м	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	v		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<ul> <li>PRO products:</li> <li>Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)</li> <li>PRIVATE products:</li> <li>If the holder is underage: "Mineur jusqu'à : " &amp; (Date of birth + 18 years).</li> </ul>
	organizationalUnit Name 2	×		0	D	<b>PRO products only</b> : Company/institution department or other information item
subjectPu	blicKeyInfo	<ul> <li>✓</li> </ul>	False			
	Algorithm	$\checkmark$				Public Key: Key length: 2048bit (RSA); public exponent:
Extensio	subjectPublicKey	, v		М		Fermat-4 (=010001).
ns						

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



VERSION 1.28

Attribute	Field	IN <sup>60</sup>				ascd Certificate Profile Value
Attribute	Field	IN	CE	O/M <sup>62</sup>	CO 63	Value
Authorit						
у						
Properti es						
	eyldentifier	√	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityIn		✓ ✓	False		-	
	AccessMethod accessLocation	✓ ✓				Id-ad-2
		· ✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt Id-ad-1
	AccessMethod accessLocation	✓ ✓				
a DI Diatrik	utionPoint	· ·	False			http://qca.ocsp.luxtrust.lu/ <sup>65</sup>
CREDISTIN	distributionPoint	▼ ✓	Faise		S	
	fullName	· •			5	http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject						
Properti						
es						
subjectAlt		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKe		$\checkmark$	False		Fixed	The Key Identifier comprises a feyr bit field with a 0400
	keyldentifier	v			Fixeu	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	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
certificate	dataEncipherment	✓ ✓	False		S	False
certificater	Policyldentifier	v √	False			1.3.171.1.1.10.3.26
	policyQualifierI	· •			S	Id-qt-1 (CPS)
	D				Ũ	
	qualifier	~			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.104440.4.0
						0.4.0.194112.1.2
QualifiedC	ertificateStat	~	False			
	QcCompliance	✓		М	S	True
	(0.4.0.1862.1.1)					
	QcSSCD			М	S	True
	(0.4.0.1862.1.4)	,		L		
	QcPDS	~		М	S	https://www.luxtrust.lu/upload/data/repository/PD
	(0.4.0.1862.1.5)					S.pdf
	0.01.000	✓		NA NA	<u> </u>	id atai gat asign
		v		М	S	id-etsi-qct-esign
	(0.4.0.1862.1.6)					

### 1.12.33 LuxTrust Smart Card NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.27>.

### LuxTrust Smart Card NCP+ Certificate Profile

<sup>65</sup> SINCE LTGQCA3



Attribute	Field	IN 66	CE <sup>67</sup>	O/M <sup>68</sup>	CO <sub>69</sub>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNum	ber	$\checkmark$	False			
	1		E-l		FDV	Validated on duplicates.
signature	Algorithm	✓	False		S	OID = "1.2.840.113549.1.1.11" - SHA256 with
	Aigonain				5	RSA Encryption.
signature\	/alue	✓	False			
			E-l		D	Issuing CA Signature.
Issuer	countryName	$\checkmark$	False		S S	LU
	commonName	• ✓			S	LuxTrust Global Qualified CA x <sup>70</sup>
	organizationName	· ✓			S	LuxTrust S.A.
Validity	organizationivanie	· ✓	False		5	Euxiliust S.A.
valially	NotBefore	✓	1 0.00		D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 36
						Months
Subject		✓	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		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	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card
	surname	~		М	D	<b>PRO and PRIVATE products</b> : 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	*		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	<b>PRO products only:</b> Name of company/institution as in articles of association or equivalent documents, including the legal form.
	localityName	~		М	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnit Name 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	<ul> <li>PRO products:</li> <li>Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)</li> <li>PRIVATE products:</li> <li>If the holder is underage: "Mineur jusqu'à : " &amp; (Date of birth + 18 years).</li> </ul>

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

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

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

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

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



VERSION 1.28

		Lux1	rust Sn		NCP+ Cer	tificate Profile
Attribute	Field	IN 66	CE <sup>67</sup>	O/M <sup>68</sup>	CO <sub>69</sub>	Value
	organizationalUnit Name 2	~		0	D	<b>PRO products only</b> : Company/institution department or other information item
subjectPut	olicKeyInfo	✓	False			
	Algorithm	√	1 0100			Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensio ns						
Authorit y Properti es						
authorityK	eyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityIn		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/71
cRLDistrib		✓	False			
	distributionPoint	✓			S	
	fullName	$\checkmark$				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properti es						
subjectAlt	Name	✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKey		✓	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 Properti es						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	<ul> <li>✓</li> </ul>			S	False
certificate		✓	False			
	PolicyIdentifier	✓ ✓				1.3.171.1.10.3.27
	policyQualifierID qualifier	v v			S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	policyQualifierID	▼ ✓			S S	
	PolicyIdentifier	✓ ✓			5	Id-qt-2 (User Notice) 0.4.0.2042.1.2

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

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

These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.0.3.28>.

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

<sup>71</sup> SINCE LTGQCA3



	LuxTrust Sr	nart C	ard LOF		+ - Signa	ature Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile						
Version		√	False		<u> </u>	$\lambda$ (arrian 2) (also $-$ "2"
SerialNumb	er	$\checkmark$	False		S	Version 3 Value = "2"
Senainumb		•	I dise		FDV	Validated on duplicates.
signatureAl	aorithm	✓	False		1.51	
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA
						Encryption.
signatureVa	lue	✓	False			
locuor		✓	False		D S	Issuing CA Signature.
Issuer	countryName	✓ ✓	Faise		S	LU
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	~			S	LuxTrust S.A.
Validity	•. gaa	✓	False		Ū	
<b>,</b>	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(s) as on ID card without indication
	Surname	~		М	D	"épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"LuxTrust RA Officer"
	organizationName	~		М	D	Constructed by LuxTrust
	localityName	~		М	D	Country of RA
	organizationalUnitNam e 1	~		М	D	RA code Constructed by LuxTrust
	organizationalUnitNam e 2	~		М	D	RAO code Constructed by LuxTrust
subjectPubl		✓	False			
	Algorithm	$\checkmark$				Public Key: Key length: 2048bit (RSA); public
Extension s	subjectPublicKey	~		M		exponent: Fermat-4 (=010001).
Authority						
Properties authorityKe	vldentifier	√	False			
aunontyre	keyldentifier	<b>√</b>	1 0150			SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<b>√</b>				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		✓	False			
	distributionPoint	$\checkmark$			S	1
	fullName	×				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltN		✓	False			
	Rfc822Name	<ul> <li>✓</li> </ul>		0	D	Certificate Holder's email address
subjectKeyl	dentifier	✓	False			



VERSION 1.28

	LuxTrust S	mart C	ard LOF		+ - Signa	ature Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	keyldentifier	<b>_</b>			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		$\checkmark$	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePo	olicies	✓	False			
	Policyldentifier	✓				1.3.171.1.1.10.3.28
	policyQualifierID	✓			S	Id-gt-1 (CPS)
	Qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	√			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.2042.1.2

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

LuxTrust Normalised Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose for LRAO Purposes. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.29>.

	LuxTrust Sn	hart Ca	rd LOR	A NCP+	- authen	tication Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumb	ber	✓	False			
					FDV	Validated on duplicates.
signatureAl	lgorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	alue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Global Qualified CA x <sup>17</sup>
	organizationName	√			S	LuxTrust S.A.
Validity		√	False			
-	NotBefore	√			D	Certificate generation process date/time.
	NotAfter	√			D	Certificate generation process date/time + 36 Months
Subject		√	False			
	serialNumber	~		М	D	Serial Number as constructed by LRAO
	commonName	~		м	D	Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character.
	givenName	~		М	D	Given name(s) as on ID card
	Surname	~		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



VERSION 1.28

	LuxTrust Sma	rt Ca	rd LOR	A NCP+	- authen	tication Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	<b>CO</b> <sup>16</sup>	Value
	localityName	✓		М	D	Country of RA
	organizationalUnitNam	~		м	D	RA code Constructed by LuxTrust
	e 1	•		IVI	D	TA Code Constructed by Eux Trust
	organizationalUnitNam	~			_	
	e 2	~		М	D	RAO code Constructed by LuxTrust
subjectPubl	icKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public
	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extension						
S						
Authority Properties						
authorityKe	yldentifier	✓	False			
,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,,	keyldentifier	✓				SHA-1 Hash of the LuxTrust Global Qualified CA
	-					public key
authorityInfo		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		✓	False			
	distributionPoint	$\checkmark$			S	17
	fullName	~				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properties						
subjectAltNa		✓	False			• ····
	Rfc822Name	<ul> <li>✓</li> </ul>	E de s	0	D	Certificate Holder's email address
subjectKeyl		✓ ✓	False		Fixed	The Key Identifier comprises a feur hit field with a
	keyldentifier	v			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of
						the SHA-1 hash of the value or subjectPublicKey bit
						string (tag, not including the length and number of
						unused bit-string bits).
Policy						
Properties keyUsage		✓	True			
Reyusaye	digitalSignature	▼ ✓	Thue		S	True
	nonRepudiation	· ✓	1		S	False
	keyEncipherment	✓	1	1	S	True
	dataEncipherment	✓			S	False
certificatePo		✓	False			
	Policyldentifier	√				1.3.171.1.1.10.3.29
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	Qualifier	✓ ✓			S	https://repository.luxtrust.lu
	policyQualifierID PolicyIdentifier	$\checkmark$			S	Id-qt-2 (User Notice)
	Folicyldentitier	v				0.4.0.2042.1.2
						0.7.0.2072.1.2

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

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



VERSION 1.28

	LuxTrus	st eID \$	Smart C	ard Q(	CP-n-qs	cd Certificate Profile
Attribute	Field	IN <sup>72</sup>	CE <sup>73</sup>	O/M 74	CO <sup>75</sup>	Value
Base Profile						
Version	•	✓	False			
					S	Version 3 Value = "2"
SerialNumb	er	✓	False			
					FDV	Validated on duplicates.
signatureAlg	gorithm	✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureVa	lue	✓	False			
					D	Issuing CA Signature.
Issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓		1	S	LuxTrust Global Qualified CA x <sup>76</sup>
	organizationName	~			S	LuxTrust S.A.
Validity	organizationName	▼ ✓	False		3	
valiulty	NotBefore	✓ ✓	Faise		D	Cartificate generation process data /time
	NotAfter	<i>✓</i>			D	Certificate generation process date/time. Certificate generation process date/time + maximum 120 Months; Certificate generation process date/time + 1 day for
						PSEUDONYM Certificate
Subject	serialNumber	✓ ✓	False	M	D	Serial Number as constructed by LRAO
					_	
	commonName	~		М	D	Concatenation of given name(s) and surname(s) separated by the space character
	givenName	~		М	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	~		М	D	LU
	emailAddress	~		0	D	Subject's email address
	Title	✓		М	D	"Private Person"
	organizationalUnitName 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
subjectPubli		✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA);
Extension	subjectPublicKey	✓		M		public exponent: Fermat-4 (=010001).
S Authority Properties						
Properties authorityKey	Identifier	✓	Folco			
aumontyney	keyldentifier	▼ ✓	False	-		SHA-1 Hash of the LuxTrust Global Qualified CA x
and the second second			5-1			SHA-1 Hash of the LuxTrust Global Qualified CA x public key
authorityInfo		<ul> <li>✓</li> </ul>	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	$\checkmark$				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribut		✓	False			
	distributionPoint	▼ ✓	1 aise		S	
	fullName	▼ ✓			3	17
	TUITINATTIE	*				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl

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

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

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

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

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



VERSION 1.28

SubjectKeyldentifier         keylde         Policy         Properties         keyUsage         digital         nonRe         keyEn         dataE         certificatePolicies         Policy         pol         pol         pol         dataE         certificatePolicies         pol         pol	Field	72	LuxTrust eID Smart Card QCP-n-qscd Certificate Profile										
Properties subjectAltName Rfc82 subjectKeyldentifier keylde Policy Properties keyUsage digital nonRe keyEn dataE certificatePolicies Policy pol		IN <sup>72</sup>	CE <sup>73</sup>	O/M 74	CO <sup>75</sup>	Value							
Rfc82 SubjectKeyldentifier keylde Policy Properties keyUsage digital nonRe keyEn dataE certificatePolicies Policy pol													
subjectKeyldentifier         keylde         Policy         Properties         keyUsage         digital         nonRe         keyEn         dataE         certificatePolicies         Policy         pol         pol         pol         dataE         certificatePolicies         Policy         pol		✓	False										
Policy Properties keyUsage digital nonRe keyEn dataE certificatePolicies Policy pol	2Name	✓		0	D	Subject email address							
Policy Properties keyUsage digital nonRe keyEn dataE certificatePolicies Policy pol		✓	False										
Properties keyUsage digital nonRe keyEn dataE certificatePolicies Policy pol	entifier	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).							
digital nonRe keyEn dataE certificatePolicies Policy pol													
nonRe keyEn dataE certificatePolicies Policy pol		✓	True										
keyEn dataE certificatePolicies Policy pol	Signature	$\checkmark$			S	False							
dataE certificatePolicies Policy pol	epudiation	✓			S	True							
certificatePolicies Policy pol	cipherment	✓			S	False							
Policy	ncipherment	$\checkmark$			S	False							
pol		✓	False										
	Identifier	✓				1.3.171.1.1.10.3.30							
(	icyQualifierID	✓			S	ld-qt-1 (CPS)							
	Qualifier	✓			S	https://repository.luxtrust.lu							
policy	/QualifierID	✓			S	Id-qt-2 (User Notice)							
Policy	Identifier	~				0.4.0.194112.1.2							
QualifiedCertificate	Stat	✓	False										
	mpliance ).1862.1.1)	~		М	S	True							
QcSS		~		М	S	True							
QcPE		~		М	S	https://www.luxtrust.lu/upload/data/repository/PD S.pdf							
QcTy (0.4.0	pe ).1862.1.6)	~		М	S	id-etsi-qct-esign							

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

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburguish eID Smart Card), with creation of the keys by LuxTrust, 2048-bit key size and sixty-one (61) months validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.31>.

LuxTrust eID Smart card NCP+ Certificate Profile									
Attribute	Field	IN''	CE <sup>78</sup>	O/M 79	CO <sub>80</sub>	Value			
Base Profile									
Version		✓	False						
					S	Version 3 Value = "2"			
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	signatureValue		False						
-					D	Issuing CA Signature.			
Issuer		✓	False		S				
	countryName	✓			S	LU			

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

 $<sup>^{78}</sup>$  CE = Critical Extension.

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

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



VERSION 1.28

	LuxTru	st eid	Smart o	card N	CP <u>+ Ce</u>	rtificate Profile
Attribute	Field	IN″	CE <sup>78</sup>	O/M 79	CO <sup>80</sup>	Value
	commonName	√			S	LuxTrust Global Qualified CA x <sup>81</sup>
	organizationName	√			S	LuxTrust S.A.
Validity	organizationName	√ 	False		5	
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + maximun
						120 Months; Certificate generation process date/time + 1 day fo PSEUDONYM Certificate
Subject		√	False			
	serialNumber	$\checkmark$		Μ	D	Serial Number as constructed by LRAO
	commonName	~		М	D	Concatenation of given name(s) and surname(s separated by the space character
	givenName	~		м	D	Given name(s) as on ID card or as provided by the RNCID
	Surname	~		М	D	Surname(s) as on ID card without indication "épouse" "ép." or similar and the subsequent name(s) or as provided by the RNCID
	countryName	~		М	D	LU
	emailAddress	~		0	D	Subject's email address
	Title	~		М	D	"Private Person"
	organizationalUnitNam e 1	~		0	D	If the holder is underage: "Mineur jusqu'à : " & (Date c birth + 18 years).
subjectPubli	icKeyInfo	~	False			
	Algorithm	✓				Public Key: Key length: 2048bit up to 4096bit (RSA)
_	subjectPublicKey	~		М		public exponent: Fermat-4 (=010001).
Extension						
s Authority Properties						
authorityKey	/Identifier	√	False			
	keyldentifier	<b>√</b>				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authorityInfo		✓ ✓	False			
	AccessMethod accessLocation	✓ ✓				Id-ad-2
						http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓ ✓				Id-ad-1
	accessLocation					http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribut	tionPoint distributionPoint	✓ ✓	False		S	
	fullName	▼ ✓			3	17
Subject Properties	TullName	•				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
subjectAltNa	ame	√	False			
-	Rfc822Name	√		0	D	Subject email address
subjectKeylo		√	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage		√	True			
,	digitalSignature	√			S	True
	nonRepudiation	~			S	False
l. I		✓		T	S	True
	keyEncipherment					
certificatePo	dataEncipherment	✓ ✓ ✓	False		S	False

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



VERSION 1.28

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

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

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

	LuxTru					I Certificate Profile	
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>1</sup> 5	CO <sup>16</sup>	Value	
Base							
Profile							
Version	1	~	False			$\lambda$ (arbian $2\lambda$ ) (also $=$ " $2$ "	
SerialNumb	or	✓	False		S	Version 3 Value = "2"	
Senainum		•	Faise		FDV	Validated on duplicates.	
signatureA	lgorithm	✓	False		100		
orginatarora	algorithm		1 0.00		S		
						OID = "1.2.840.113549.1.1.11" - if SHA256 with RSA Encryption.	
signatureVa	alue	✓	False				
					D	Issuing CA Signature.	
Issuer		√	False		S		
	countryName	√			S	LU	
	commonName	~			S	LuxTrust Global Qualified CA x <sup>17</sup>	
	organizationName	✓			S	LuxTrust S.A.	
Validity	1	✓	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	<b>PRO and PRIVATE products</b> : Concatenation o given name(s) and surname(s) as on ID carc separated by a "Space" character	
	givenName	~		М	D	<b>PRO and PRIVATE products</b> : Given name(s) as on ID card	
	surname	~		М	D	<b>PRO and PRIVATE products</b> : Surname(s) as or 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	
	title	~		М	D	PRIVATE products:         Fixed value: "Private Person"         PRO products:         "Professional Person" (default) o.         "Professional Administrator"         (Other titles possible for special purpose certificates)	
	organizationName	~		М	D	<b>PRO products only:</b> Name of company/institution as in articles of association or equivalent documents, including the legal form.	



	LuxTrust	Signir	ng Serve	er QCP	-n-ascd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>1</sup>	CO <sup>16</sup>	Value
				5		
	localityName	~		м	D	<b>PRO products only</b> : Company/institution country of HQ (as in articles of association)
	organizationalUnitNa me 1	V		M for PRO prod ., cond i- tiona I (O) for PRI V prod .)	D	<b>PRO products</b> : Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier) <b>PRIVATE products:</b> If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).
	organizationalUnitNa me 2	~		0	D	<b>PRO products only</b> : Company/institution department or other information item
subjectPub		✓ ✓	False			Public Key: Key length: up to 4096 bit (RSA);
	algorithm subjectPublicKey	✓ ✓		М		public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extension s						
Authority Properties						
authorityKe		✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust <b>Global Qualified</b> CA public key
authorityInf	oAccess AccessMethod	$\checkmark$	False			ld-ad-2
	accessLocation	· ✓		ł – –		http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				ld-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu	itionPoint distributionPoint	✓ ✓	False		<u> </u>	
	fullName	▼ ✓			S	http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
Subject Properties						
subjectAltN		✓	False			
subjectKey	Rfc822Name	✓ ✓	False	0	D	Certificate Holder's email address
Subjectively	keyldentifier	×			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Properties						
keyUsage	digitalSignature	✓ ✓	True		S	True
	nonRepudiation	<b>*</b>			S S	True True
	keyEncipherment	~			S	True
	dataEncipherment	· ✓			S	False
certificateP	olicies	✓	False		-	
	Policyldentifier	<b>~</b>				1.3.171.1.1.10.3.32
	policyQualifierID gualifier	✓ ✓			S S	Id-qt-1 (CPS) https://repository.luxtrust.lu
	quaimer	×			3	
	Policyldentifier	~				0.4.0.194112.1.2
QualifiedCe	rtificateStat	$\checkmark$	False			



VERSION 1.28

	LuxTrust Signing Server QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>1</sup> ₅	CO <sup>16</sup>	Value					
	QcCompliance (0.4.0.1862.1.1)	×		М	S	True					
	QcSSCD (0.4.0.1862.1.4)	~		М	S	True					
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS. pdf					
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-esign (0.4.0.1862.1.6.1)					

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

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

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



	LuxTrus	st Sigr	ning Ser	ver QCF	P-I-qscd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value
Aunoute	organisationIdentif ier (2.5.4.97)	N ✓		М	D	<ul> <li>Shall contain information using the following structure in the presented order: <ul> <li>3 character legal person identity type reference;</li> <li>2 character ISO 3166 country code;</li> <li>hyphen-minus "-" and</li> <li>identifier (according to country and identity type reference).</li> </ul> </li> <li>The three initial characters shall have one of the following defined values: <ul> <li>1) "VAT" for identification based on a national value added tax identification number.</li> <li>2) "NTR" for identification based on an identifier from a national trade register. Or Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).</li> <li>When a locally defined identity type reference is provided (two characters followed by ":"), the nameRegistrationAuthorities element of SemanticsInformation (IETF RFC 3739 [1]) shall be present and shall contain at least a uniformResourceIdentifier generalName. The two letter identity type reference following the ":" character shall be unique within the specified uniformResourceIdentifier.</li> </ul></li></ul>
	organizationName	~		М	D	Shall contain the full registered name of the subject (legal person).
	organizationalUnitNa me 1	~		о	D	Company/institution department or other information item
	organizationalUnitNa me 2	~		0	D	Company/institution department or other information item
subjectPub	licKeyInfo algorithm	$\checkmark$	False			Public Kov Kov longth: up to 4006 bit (DCA)
	subjectPublicKey	✓ ✓		М		Public Key: Key length: up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
Extensio ns	SubjectrubileRey	• 				
Authority Propertie s	uldontific-		Fels.			
authorityKe		$\checkmark$	False			SHA-1 Hash of the LuxTrust Global Qualified CA
outh or its days	keyldentifier	✓ ✓	Folco			public key
authorityInf	AccessMethod	✓ ✓	False			ld-ad-2
	accessLocation	✓ ✓				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				Id-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/ <sup>18</sup>
cRLDistribu		~	False			
	distributionPoint	✓ ✓	1 0150		S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
			L		l	



VERSION 1.28

	LuxTru	ıst Sigr	ning Ser	ver QCI	P-I-qscd	Certificate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Subject Propertie s						
subjectKey		✓	False			
	keyldentifier	✓			Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).
Policy Propertie s						
keyUsage		~	True			
	digitalSignature	~			S	True
	nonRepudiation				S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificateP	Policies	✓	False			
	Policyldentifier	~				1.3.171.1.1.10.3.33
	policyQualifierID	√			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	Policyldentifier	~				0.4.0.194112.1.3
Qualifie	edCertificateStat	✓	False	1		
L	QcCompliance (0.4.0.1862.1.1)	~		М	S	True
	QcSSCD (0.4.0.1862.1.4)	✓		М	S	True
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS. pdf
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-eseal (0.4.0.1862.1.6.2)

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

LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.34>.

	LuxTrust Signing Stick QCP-n-qscd Certificate Profile										
Attribute	Field	IN <sup>82</sup>	CE <sup>83</sup>	O/M <sup>84</sup>	CO 85	Value					
Base Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	ber	✓	False								
					FDV	Validated on duplicates.					
signatureA	lgorithm	✓	False								
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.					
signature	/alue	✓	False								
					D	Issuing CA Signature.					
Issuer		√	False		S						
	countryName	✓			S	LU					

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

<sup>&</sup>lt;sup>83</sup> CE = Critical Extension.

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

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



	Lux				CP-n-o	qscd Certificate Profile
Attribute	Field	IN <sup>82</sup>	CE <sup>83</sup>	O/M <sup>84</sup>	CO 85	Value
	commonName	✓			S	Lux Trust Clobal Qualified CA v <sup>86</sup>
		· •				LuxTrust Global Qualified CA x <sup>86</sup>
Validity	organizationName	✓ ✓	False		S	LuxTrust S.A.
Validity	NotBefore	▼ ✓	Faise		D	Certificate generation process date/time.
	NotAfter	▼ ✓			D	Certificate generation process date/time + 36 Months
Subject	NOLAILEI	✓ ✓	False		D	Certificate generation process date/time + 30 Months
Subject			1 0130		_	
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	commonName	~		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	<b>PRO and PRIVATE products</b> : Given name(s) as on IL card
	surname	~		м	D	<b>PRO and PRIVATE products</b> : Surname(s) as on IL card without indication "épouse", "ép." or similar and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
	title	¥		М	D	PRIVATE products: Fixed value: "Private Person" PRO products: "Professional Person" (default) or "Professional Administrator" (Other titles possible for special purpose certificates)
	organizationName	~		М	D	<b>PRO products only:</b> 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 HC (as in articles of association)
	organizationalUnit Name 1	v		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	~		0	D	<b>PRO products only:</b> Company/institution department or other information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓				Public Key: Key length: 2048bit (RSA); public exponent
	subjectPublicKey	✓		М		Fermat-4 (=010001).
Extensio ns						
Authorit y Properti es						
authorityK	eyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA publi key
authoritylr	foAccess	✓	False			
autorityli	AccessMethod	· ✓	1 0.00			Id-ad-2
	accessLocation	· ·				
						http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	<ul> <li>✓</li> </ul>				Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/ <sup>87</sup>

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



VERSION 1.28

	Lux	Frust \$	Signing	Stick Q	CP-n-c	qscd Certificate Profile
Attribute	Field	IN <sup>82</sup>	CE <sup>83</sup>	0/M <sup>84</sup>	CO 85	Value
cRLDistrib	cRLDistributionPoint		False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properti es						
subjectAlt		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKe		✓	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 Properti es						
keyUsage		✓	True			
	digitalSignature	✓			S	False
	nonRepudiation	✓			S	True
	keyEncipherment	✓			S	False
	dataEncipherment	✓ ✓			S	False
certificate		✓ ✓	False			
	Policyldentifier policyQualifierI D	✓ ✓			S	1.3.171.1.10.3.34 Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	Policyldentifier	~				0.4.0.194112.1.2
QualifiedC	ertificateStat	✓	False			
	QcCompliance (0.4.0.1862.1.1)	~		М	S	True
	QcSSCD (0.4.0.1862.1.4)			М	S	True
	QcPDS (0.4.0.1862.1.5)	~		М	S	https://www.luxtrust.lu/upload/data/repository/PDS.pdf
	QcType (0.4.0.1862.1.6)	~		М	S	id-etsi-qct-esign

### 1.12.41 LuxTrust Signing Stick NCP+ Certificate Profile

LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.35>.

	LuxTrust Signing Stick NCP+ Certificate Profile										
Attribute	Field	IN 88	CE <sub>89</sub>	O/M <sup>90</sup>	CO <sup>91</sup>	Value					
Base											
Profile											
Version		✓	False								
					S	Version 3 Value = "2"					
SerialNum	SerialNumber V False										

## <sup>87</sup> SINCE LTGQCA3

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

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

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

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



			rust Sig			
Attribute	Field	IN 88	CE89	O/M <sup>90</sup>	CO <sup>91</sup>	Value
					FDV	Validated on duplicates.
signature		✓	False			
	Algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signature\	Value	✓	False			
Issuer		✓	False		DS	Issuing CA Signature.
133061	countryName	· ·	1 0130		S	LU
	commonName	·			S	LuxTrust Global Qualified CA x <sup>92</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity	organizationitanie	<ul> <li>✓</li> </ul>	False		0	
·	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	~			D	Certificate generation process date/time + 3 Months
Subject		✓	False			
	serialNumber	✓		М	D	Serial Number as constructed by LRAO
	Seriainumber			IVI	D	PRO and PRIVATE products: Concatenation of
	commonName	~		М	D	given name(s) and surname(s) as on ID car separated by a "Space" character.
	givenName	~		М	D	<b>PRO and PRIVATE products</b> : Given name(s) a on ID card
	surname	~		м	D	<b>PRO and PRIVATE products</b> : Surname(s) as ou ID card without indication "épouse", "ép." or simila and the subsequent name(s)
	countryName	~		М	D	Nationality of holder (ISO3166)
	emailAddress	~		0	D	Subject's email address
						PRIVATE products:
	title	*		М	D	Fixed value: "Private Person" PRO products: "Professional Person" (default) of "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	<b>PRO products only</b> : Company/institution countr of HQ (as in articles of association)
	organizationalUnit Name 1	~		M for PRO prod., condi- tional (O) for PRIV prod.)	D	PRO products:         Company/Institution VAT number (or if no VA 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	~		о	D	<b>PRO products only</b> : Company/institution department or othe information item
subjectPu	blicKeyInfo	✓	False			
	Algorithm	✓	ļ			Public Key: Key length: 2048bit (RSA); publi
Futar -!-	subjectPublicKey	✓		М		exponent: Fermat-4 (=010001).
Extensio						

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



VERSION 1.28

	L	.uxTı		ning Sticl		ertificate Profile
Attribute	Field	IN 88	CE <sup>89</sup>	O/M <sup>90</sup>	CO <sup>91</sup>	Value
Authorit y						
Properti es						
authorityK	eyldentifier	✓	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA public key
authoritylr	nfoAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	✓				ld-ad-1
	accessLocation	✓				http://qca.ocsp.luxtrust.lu/93
cRLDistrib	outionPoint	✓	False			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx <sup>17</sup> .crl
Subject Properti es						
subjectAlt		✓	False			
	Rfc822Name	✓		0	D	Certificate Holder's email address
subjectKe		✓	False			
	keyldentifier	~			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	$\checkmark$			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓	L		S	False
certificate		✓	False			
	Policyldentifier	✓ ✓				1.3.171.1.1.10.3.35
	policyQualifierID	✓ ✓			S	Id-qt-1 (CPS)
	qualifier	$\checkmark$			S	https://repository.luxtrust.lu
	policyQualifierID	$\checkmark$			S	Id-qt-2 (User Notice)
	Policyldentifier	V				0.4.0.2042.1.2

### 1.12.42 LuxTrust Signing Server Advanced Automated eSeal Certificate Profile

LuxTrust Lightweight Certificate Policy Certificate compliant with ETSI EN 319 411-1 LCPcertificate policy, with creation of the keys by the LuxTrust, 4096 -bit key size and two (2) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.3.36>.

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

<sup>93</sup> SINCE LTGQCA3



	Advanced eSeal - LCP Certificate Profile										
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value					
	algorithm				S	OID = "1.2.840.113549.1.1.11" - if SHA256 with					
						RSA Encryption.					
signatureVa	alue	~	False								
					D	Issuing CA Signature.					
Issuer		~	False		S						
	countryName	$\checkmark$			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 + 12, 24					
						Months					
subject		~	False								
	serialNumber	~		М	D	Serial Number as constructed by LRAO					
	commonName	~		М	D	Shall contain the full registered name of the subject (legal person).					
	countryName	~		М	D	the country in which the subject (legal person) is established (ISO3166)					



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



	Adv	/ance	d eSea	nl - LCP	Certif	icate Profile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
	organizationalUnitNam	$\checkmark$				
	e 2	v		0	D	Company/institution department or other
						information item
subjectPubl	icKeyInfo	~	False			
	algorithm	$\checkmark$				Public Key: Key length: up to 4096 bit (RSA);
	subjectPublicKey	√		М		public exponent: Fermat-4 (=010001).
Extension						
S						
Authority						
Properties						
authorityKey	/Identifier	~	False			
	keyldentifier	~				SHA-1 Hash of the LuxTrust Global Qualified CA
						public key
authorityInfo	Access	~	False			
	AccessMethod	~				ld-ad-2
	accessLocation	~				http://ca.luxtrust.lu/LTGQCAx <sup>17</sup> .crt
	AccessMethod	~				ld-ad-1
	accessLocation	√				http://qca.ocsp.luxtrust.lu/18
cRLDistribut	tionPoint	√	False			
	distributionPoint	√			S	
	fullName	√				http://crl.luxtrust.lu/LTGQCA <sup>17</sup> .crl
Subject						
Properties						
subjectKeyl	dentifier	√	False			
	keyldentifier	~			Fixed	The Key Identifier comprises a four-bit field with a
						0100 value, followed by the least significant 60 bits
						of the SHA-1 hash of the value or
						subjectPublicKey bit string (tag, not including the
						length and number of unused bit-string bits).
Policy						
Properties						
keyUsage	1	~	True			
	digitalSignature	$\checkmark$			S	True
	nonRepudiation	~			S	False
	keyEncipherment	<b>v</b>			S	False
	dataEncipherment	~			S	False
certificatePo	blicies	~	False			
	PolicyIdentifier	$\checkmark$				
						1.3.171.1.1.10.3.36
		~				
	policyQualifierID	· ~			S	Id-qt-1 (CPS)
	qualifier	•			S	https://repository.luxtrust.lu



VERSION 1.28

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

### 1.12.43 LuxTrust Corporate LCP Certificate Profile

LuxTrust Lightweight Certificate Policy Certificate compliant with ETSI EN 319 411-1 LCP certificate policy, with creation of the keys by the LuxTrust, 4096 -bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.10.4.1>.

LuxTrust Corporate LCP Certificate Profile – Corporate CA									
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value			
Base Profile									
Version		~	False						
					S	Version 3 Value = "2"			
SerialNumber		~	False						
					FDV	Sequential CSN			
signatureAlgorit	hm	~	False						
	Algorithm				S	OID = "1.2.840.113549.1.1.11"-SHA256 with RSA Encryption.			
signatureValue		~	False						
					D	Issuing CA Signature.			
lssuer		~	False		S				
	countryName	~			S	LU			
	commonName	~			S	LuxTrust Corporate CA x			
	organizationName	~			S	LuxTrust S.A.			
Validity	1	~	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			



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



VERSION 1.28

	LuxTrus	t Corpor	ate LCP (	Certificate F	Profile – Co	prporate CA
Attribute	Field	IN <sup>18</sup>	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value
subjectAltName		~	False			
	Rfc822Name	~		0	D	N/A
subjectKeyIdent	ifier	~	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	V			S	False
	keyEncipherment	~			S	False
	dataEncipherment	~			S	False
certificatePolicie	98	~	False			
	PolicyIdentifier	~				1.3.171.1.1.10.4.1
	policyQualifierID	~			S	Id-qt-1 (CPS)
	Qualifier	~			S	https://repository.luxtrust.lu
	PolicyIdentifier	~				0.4.0.2042.1.3

## 1.13 Timestamping Certificate Profile

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

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



	LuxTru			ing Certi		rofile
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	<b>O/M</b> <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile Version			False			
Version		-	1 0130		S	Version 3 Value = "2"
SerialNumbe	er en en en en en en en en en en en en en	✓	False			
			False		FDV	Validated on duplicates.
signatureAlg	algorithm	~	False		S	OID = "1.2.840.113549.1.1.11" - SHA25
	algoriani				Ũ	with RSA Encryption.
signatureVal	ue	✓	False		-	
loover		✓	False		D S	Issuing CA Signature.
issuer	countryName	▼ ✓	Faise		S	LU
	commonName	~			S	LuxTrust Global Timestamping CA x <sup>17</sup>
	organizationName	✓			S	LuxTrust S.A.
Validity		✓	False			
	NotBefore NotAfter	✓ ✓			D D	Certificate generation process date/time.
	NotAiter	v			D	Certificate generation process date/time - 60 Months
subject	I	✓	False			
	commonName	~		М	D	tts.luxtrust.lu
	localityName	✓		м	D	Capellen
						,
	organizationName	~		М	D	LuxTrust S.A.
	organizationalUnitName 1	✓		М	D	PKI Entity
	countryName	✓		0	D	LU
subjectPubli		✓	False	<u> </u>		
Subjecti ubil	algorithm	· ·	I alse			Public Key: Key length: 2048 bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions					-	
Authority Properties						
authorityKey	l /Identifier	✓	False			
	keyldentifier	✓				SHA-1 Hash of the LuxTrus
		✓	E e le c			Timestamping CA public key
authorityInfo	Access	▼ ✓	False			ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGTSACAx <sup>17</sup> .crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistribut		✓ ✓	False		6	
	distributionPoint fullName	✓ ✓			S	http://crl.luxtrust.lu/LTGTSACAx <sup>17</sup> .crl
Subject						
Properties						
subjectAltNa		<ul> <li>✓</li> </ul>	False			
subjectKeylo	Rfc822Name	✓ ✓	False	0	D	info@luxtrust.lu
Subjectivelyic	keyldentifier	✓ ✓	raise		Fixed	The Key Identifier comprises a four-b
					. incu	field with a 0100 value, followed by the
						least significant 60 bits of the SHA-1 has
						of the value or subjectPublicKey bit strin (tag, not including the length and number
						of unused bit-string bits).
Policy						
Properties			-			
keyUsage	digitalSignature	✓ ✓	True		6	True
	digitalSignature nonRepudiation	✓ ✓			S S	True False
	keyEncipherment	✓ ✓			S	False
	dataEncipherment	✓			S	False
Extended Ke	y Usage	✓	False			
	TimeStamping	✓	1	1	S	Set



VERSION 1.28

	LuxTrust Timestamping Certificate Profile									
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value				
Private Key	Usage Period	√	False							
	Usage period (2.5.29.16)	~		М	D	Certificate generation process date/time + 12 Months				
certificatePc	olicies	✓	False							
	Policyldentifier	√				1.3.171.1.1.10.8.1				
	policyQualifierID	√			S	Id-qt-1 (CPS)				
	qualifier	✓			S	https://repository.luxtrust.lu				
	policyQualifierID	√			S	Id-qt-2 (User Notice)				
	noticeNumbers									
	DisplayText	~				LuxTrust LCP certificate compliant with ETSI TS 102 042. Sole authorised usage: Signature of LuxTrust Trusted Time Stamp tokens generated by LuxTrust time- stamping authority.				
	Policyldentifier	✓				0.4.0.2042.1.3				

#### 1.13.1 Normalized Certificate Policy for LuxTrust Qualified Timestamping

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

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

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

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

	Normalized	Certific	cate Poli	cy for Lι	uxTrust	Qualified Timestamping
Attribute	Field	IN <sup>13</sup>	CE <sup>14</sup>	O/M <sup>15</sup>	CO <sup>16</sup>	Value
Base						
Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumbe	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 + 60 Months
subject		✓	False			
	organisationIdentifier (2.5.4.97)	~		М	D	VATLU-20976985
	commonName	✓		Μ	D	LuxTrust Qualified Timestamping
	organizationName	✓		Μ	D	LuxTrust S.A.
	countryName	✓		Μ	D	LU
subjectPubli	icKeyInfo	✓	False			
	algorithm	✓				Public Key: Key length: up to 4096 bit (RSA)
	subjectPublicKey	✓		М		public exponent: Fermat-4 (=010001).
Extensions						
Authority						
Properties						
authorityKey	yldentifier	✓	False			
	keyldentifier	✓				SHA-1 hash of the LuxTrust Global Qualified CA
authorityInfo	DAccess	✓	False			
	AccessMethod	✓				ld-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt



VERSION 1.28

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

#### 1.13.2 Qualified Timestamping Certificate Profile

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

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

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

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

	Qualified Certificate Policy for for LuxTrust Qualified Timestamping									
Attribute	Field	IN1 3	CE1 4	O/M1 5	CO1 6	Value				
Base Profile										
Version		~	Fals e							
					S	Version 3 Value = "2"				
SerialNumb	per	~	Fals e							
					FDV	Validated on duplicates.				
signatureAl	gorithm	~	Fals e							
	algorithm				S	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.				
signatureVa	alue	~	Fals e							
					D	Issuing CA Signature.				



	Qualifie	d Certi	ficate P	olicy for	for Lux	Trust Qualified Timestamping
Attribute	Field	IN1	CE1	O/M1	CO1	Value
		3	4	5	6	
issuer		✓	Fals		S	
	a a un trutto ma	<ul> <li>✓</li> </ul>	е	-	<u> </u>	
	countryName commonName	v √			S S	LU LuxTrust Global Qualified CA x
	organizationName	▼ ✓			S	LuxTrust Global Qualified CA x
Validity	organizationivanie	· ·	Fals		5	
valiaity			e			
	NotBefore	$\checkmark$			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + 60 Months
subject		✓	Fals			
	organisationIdentifi		е			
	er					VATLU-20976985
	•	✓		М	D	
	(2.5.4.97)					
	commonName	~		м	D	
						LuxTrust Qualified Timestamping
	organizationName	$\checkmark$		M	D	LuxTrust S.A.
subjectPub	countryName	✓ ✓	<b>F</b> ala	М	D	LU
SubjectPub	alerteyiino	ľ	Fals e			
	algorithm	<ul> <li>✓</li> </ul>	U			Public Key: Key length: up to 3072 bit (RSA)
	subjectPublicKey	$\checkmark$		М		public exponent: Fermat-4 (=010001).
Extension	,					
S						
Authority						
Propertie						
S	d daw CC an	<ul> <li>✓</li> </ul>	E al a			
authorityKe	eyidentifier	v	Fals e			
	keyldentifier	✓	C		1	
	hoyhaonninoi					SHA-1 hash of the LuxTrust Global Qualified CA
authorityInf	foAccess	✓	Fals			
-			е			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTGQCAx.crt
	AccessMethod	✓			-	Id-ad-1
	accessLocation	~				http://qca.ocsp.luxtrust.lu/
cRLDistribu	utionPoint	✓	Fals			
UNED IOU ID			e			
	distributionPoint	✓			S	
	fullName	✓				http://crl.luxtrust.lu/LTGQCAx.crl
Subject						
Propertie s						
subjectAltN	lame	✓	Fals			
			e			
	Rfc822Name	✓		0	D	info@luxtrust.lu
subjectKey	Identifier	✓	Fals			
			е			
	keyldentifier	~			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						
Propertie						
s						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
				1	S	False
Extended	dataEncipherment	✓ ✓	True			
Extended K	dataEncipherment Key Usage	$\checkmark$	True			
Extended K	dataEncipherment Key Usage TimeStamping		True		S	Set
	dataEncipherment Key Usage	$\checkmark$	True Fals			



VERSION 1.28

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

#### 1.13.3 TimeStamp Request and Response Format

#### 1.13.3.1 TimeStamp Request Format

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

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

\*no extension is required to be supported

#### 1.13.3.2 TimeStamp Response Format

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

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



VERSION 1.28

LuxTrust Time Stamp Response					
Field	Value / comment				
	Object Identifier (OID) defining the digest algorithm used to compute the message imprint. If the original data instead of the hash value is provided, the library will automatically calculate the hash value using the algorithm defined by this OID. The developer must ensure that the specified algorithm is supported by the library and the TTS.				
Serial Number	Serial Number of the current TSU certificate (unique, up to 160 bits)				
Policy OID	1.3.171.1.1.10.3.18.1 / 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 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.				
Accuracy	1 second				
TSA Certificate Information	Current TSU Certificate				
Request Extensions	Value *				
None	None				

\*no extension is required to be generated, no extension shall be critical

## 1.14 Certificate extensions

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

## 1.15 Algorithm object identifiers

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

### 1.16 Name forms

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

### 1.17 Name constraints

Name constraints are supported as per RFC 5280.

### 1.18 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

### 1.19 Usage of Policy Constraints extension

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



VERSION 1.28

### 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.

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

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	<creation +="" 100="" ca="" days="" for="" global="" root="" time=""> <creation (4="" +="" 30="" 4,5="" and="" for="" hours="" minutes)="" subordinate<br="" time="">Qualified &gt;</creation></creation>						
	<pre><creation (8="" +="" 30="" 8,5="" and="" for="" hours="" minutes)="" pre="" subordinate<="" time=""></creation></pre>						
	SSL CAs>						
	<creation +="" 24="" cas="" for="" hours="" other="" 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>						
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 http://crl.luxtrust.lu.

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.



VERSION 1.28

## 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				
VEISION			Faise		S	Version 3 Value = "2"	
SerialNumbe	er en en en en en en en en en en en en en		False		3		
ochaittainbt			1 0100		FDV	Validated on duplicates.	
signatureAlg	aorithm		False		1.51		
	algorithm		. 0.00		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			М	D	LuxTrust S.A. OCSP Server 2	
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 LTGR x CA public key	
id-ocsp-noc	heck		False				
					S	NULL	
Subject Properties							
subjectKeylo	dentifier		False				
Policy	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	
certificatePolicies			False				
<b>F</b>	Policyldentifier			1	1	1.3.171.1.1.1.0.1.0	
	policyQualifierID			1	S	Id-qt-1 (CPS)	
	qualifier		1	1	S	https://repository.luxtrust.lu	
			1	1	, U		



VERSION 1.28

LuxTrust OCSP Certificate Profile							
Attribute	Field	IN18	CE19	O/M20	CO21	Value	
	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.	
	PolicyIdentifier					0.4.0.2042.1.3	
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)).