

LuxTrust Global Qualified PKI Disclosure Statements

Version number: 1.3

Publication Date: 26/03/2018

Effective Date: 09/04/2018



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

Document Information

Document title:	LuxTrust Global Qualified PKI Disclosure Statements
Project Reference:	LuxTrust S.A.
Document Archival Code:	

Version History

Version	Who	Date	Reason of modification
0.9	SealWeb	09/01/2017	First version
1.0	DEL/YNU	06/03/2017	Review
1.1	DEL	17/03/2017	Signing Server certificates added
1.2	DEL	05/02/2018	Advanced eSeal certificate added
1.3	DEL	22/03/2017	Corporate Certificate added

Table of content

DOCUMENT INFORMATION	2
VERSION HISTORY	2
TABLE OF CONTENT	3
INTELLECTUAL PROPERTY RIGHTS	3
REFERENCES.....	4
INTRODUCTION.....	5
1 TSP CONTACT INFO	5
2 CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE.....	5
3 RELIANCE LIMITS	12
4 OBLIGATIONS OF SUBSCRIBERS.....	13
5 CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES	13
6 LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY	14
6.1 DAMAGES COVERED AND DISCLAIMERS	14
6.2 LOSS LIMITATIONS	14
6.3 LIMITATIONS OF LIABILITY	15
7 APPLICABLE AGREEMENTS	15
8 PRIVACY POLICY.....	15
8.1 CONFIDENTIALITY OF BUSINESS INFORMATION	15
8.2 PROTECTION OF PERSONAL INFORMATION	15
8.3 RETENTION TIME	16
9 REFUND POLICY	16
10 APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION.....	16
11 TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT.....	16

Intellectual Property Rights

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

References

- [1] The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [2] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
- [3] ETSI TS 101 456 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- [4] ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- [5] ICAO (International Civil Aviation Organization) – Machine Readable Travel Documents – Technical Report – PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, October 01, 2004
- [6] ETSI TS 102 023 – Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- [7] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.
- [8] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.
- [9] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.
- [10] Règlement Grand-Ducal du 1^{er} juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».
- [11] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.
- [12] LuxTrust Global Root CA Certification Practice Statement – Document OID: 1.3.171.1.1.1.10.1.00
- [13] LuxTrust Global Root CA - Certificate Profiles latest version in force available on LuxTrust site
- [14] Règlement grand-ducal du 25 février 2015 modifiant le règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [15] Règlement grand-ducal du 18 juin 2014 relatif à la carte d'identité
- [16] 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
- [17] LuxTrust Global CA Practices Statements. Latest version in force available on LuxTrust site.

Introduction

The present document is the LuxTrust S.A. public “PKI Disclosure statement” (PDS) for the LuxTrust Global Qualified CA. Throughout this document, the use of the term “PDS” refers to the present document, unless otherwise specified.

The purpose of the PDS is to:

- summarise the key points of the CPs and CPS for the benefit of Subscribers and Relying Parties
- provide additional detail and further provisions that apply to the CPs.

1 TSP contact info

LuxTrust contact information	
Contact Person:	CSP Board Contact
Postal Address:	LuxTrust CSP Board LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen
Telephone number:	+352 26 68 15 - 1
Fax number:	+352 26 68 15 - 789
E-mail address:	cspboard@luxtrust.lu
Website:	www.luxtrust.lu

The form and/or procedure to be used for applying for the suspension, un-suspension and revocation of a certificate can be obtained from the following URL: <https://sra.luxtrust.lu> (French) or <https://www.luxtrust.lu/en/management/revocation> (English).

2 Certificate type, validation procedures and usage

The description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage is presented below:

CP identification	CP OID	Short Description
LuxTrust Global Qualified CA		
QCP+ supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.1	<p>ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature.</p> <p>ILNAS is the national supervisory body, which is responsible for undertaking supervision of LuxTrust currently under the regulation N°910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.</p>
NCP+ supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.2	<p>ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), 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 (to the exclusion of electronic signature) and key & data encryption.</p> <p>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.</p>
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	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, 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 advanced electronic signature with a qualified certificate.
NCP supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.4	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, 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 (to the exclusion of electronic signature) and key & data 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	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a non SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.
NCP+ supporting Advanced Electronic Mass Signature Services, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.6	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic Mass Signature Services.

CP identification	CP OID	Short Description
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	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by LuxTrust, 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.
LCP for INTEGRATION certificates LCP+ supporting Authentication & Encryption, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.8	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by LuxTrust, 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.
LCP for INTEGRATION certificates for NCP+ supporting Authentication & Encryption, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.9	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 LuxTrust, 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.
QCP+ supporting Qualified Electronic Signature with Qualified Certificate issued on SSCD for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.10	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by 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.
NCP+ supporting Authentication & Encryption for Natural Persons for LRAO Purposes, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.11	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by LuxTrust, 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.
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	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by LuxTrust, 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.
QCP+ supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.13	ETSI TS 101 456 QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g., Luxemburgish 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.
NCP+ supporting Authentication & Encryption for Natural Persons, issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.14	ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g., Luxemburgish 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 (to the exclusion of electronic signature) and key & data encryption.

CP identification	CP OID	Short Description
NCP+ Advanced Electronic Seal Signature Services , issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.15	ETSI TS 102 042 NCP+ compliant Normalised Certificate on Secure User Device (HSM), with creation of the keys by LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to the support of advanced electronic 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	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by LuxTrust, 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.
LCP for INTEGRATION certificates LCP supporting Authentication & Encryption issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.17	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., Luxemburgish eID Smart Card), with creation of the keys by LuxTrust, 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.
Normalized Certificate Policy for LuxTrust Qualified Timestamping	1.3.171.1.1.10.3.18	<p>LuxTrust Qualified Timestamping Certificates are issued by the LuxTrust Qualified CA with keys located on HSM devices, with generation by LuxTrust 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.</p> <p>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.</p> <p>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.</p>
Qualified Certificate Policy for LuxTrust Qualified Timestamping	1.3.171.1.1.10.3.19	<p>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.</p> <p>This profile complies to the requirements of the standard ETSI EN 319 411-2 describing the Requirements for trust service providers issuing EU qualified certificates.</p> <p>No certificates are issued at the current stage.</p>

CP identification	CP OID	Short Description
LuxTrust SPARE Signing Server LCP Certificate Profile	1.3.171.1.1.10.3.20	<p>LuxTrust Signing Server LCP Certificates are Lightweight Certificates not issued on SSCD Hardware token with creation of the keys by LuxTrust 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.</p> <p>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). The usage purpose of these Certificates is only authentication <OID 1.3.171.1.1.10.3.20>.</p> <p>The LuxTrust SPARE Signing Server LCP Certificate Profile includes the corresponding SPARE Signing Server LCP Certificate, i.e., <1.3.171.1.1.10.3.20>.</p>
Qualified eSeal Product		
LuxTrust Qualified eSeal Certificate Profile supporting digital signature	1.3.171.1.1.10.3.21	<p>LuxTrust Certificates for Qualified Seal Signature Services. 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.</p> <p>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 QCP-I-qscd certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., <OID 1.3.171.1.1.10.3.21>.</p>
LuxTrust Advanced eSeal - Certificate Profile supporting authentication	1.3.171.1.1.10.3.22	<p>LuxTrust Certificates for Advanced Seal Signature Services. 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.</p> <p>This profile aims at issuing advanced electronic eSeals as per Regulation (EU) No 910/2014. The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of advanced eSeals supported by Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy. These Certificates include the corresponding LuxTrust OID, i.e., <OID 1.3.171.1.1.10.3.22>.</p>
Advanced eSeal Product		
LuxTrust Advanced eSeal - Certificate Profile supporting signature	1.3.171.1.1.10.3.23	<p>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.</p> <p>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.</p>

CP identification	CP OID	Short Description
LuxTrust Advanced eSeal - Certificate Profile supporting authentication	1.3.171.1.1.10.3.24	<p>LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy.</p> <p>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.</p>
Advanced Automated eSeal		
LuxTrust Advanced Automated eSeal Certificate Profile supporting digital signature	1.3.171.1.1.10.3.25	<p>LuxTrust Certificates for Advanced automated Seal Signature Services are Advanced Certificates compliant with ETSI EN 319 411-1 NCP+ Normalized certificate policy certified as generated on secure user device (HSM), with creation of the keys by LuxTrust, with 2048-bit key size and 2 years validity from issuing start date.</p>
Qualified Smart Cards		
LuxTrust Smart Card QCP-n-qscd Certificate Profile	1.3.171.1.1.10.3.26	<p>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.</p>
LuxTrust Smart Card NCP+ Certificate Profile	1.3.171.1.1.10.3.27	<p>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.</p>
LuxTrust Smart Card LORA NCP+ (compliant with ETSI EN 319 411-1) supporting Advanced Electronic Signature with Normalized Certificate issued for Natural Persons for LRAO purposes, issued by LuxTrust Global Qualified CA.	1.3.171.1.1.10.3.28	<p>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 the support of advanced electronic signature for LRAO purposes.</p>
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	<p>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.</p>
QCP-n-qscd supporting Qualified Electronic Signature (for Natural Persons), issued by LuxTrust Global Qualified CA	1.3.171.1.1.10.3.30	<p>LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy (e.g., Luxemburgish 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.</p>

CP identification	CP OID	Short Description
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	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy (e.g., Luxemburgish 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.
Signing Server Qualified certificates		
LuxTrust Signing Server QCP-n-qscd certificate profile (for natural persons)	1.3.171.1.1.10.3.32	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 limited to the support of qualified electronic signature.
LuxTrust Signing Server QCP-l-qscd certificate profile (for legal persons)	1.3.171.1.1.10.3.33	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-l-qscd certificate policy with creation of the keys by LuxTrust, up to 4096 bit key size and with a key usage limited to the support of qualified electronic eSeals.
LuxTrust Signing Stick QCP-n-qscd certificate profile	1.3.171.1.1.10.3.34	LuxTrust Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the LuxTrust, 2048 bit key size and three (3) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.34>.
LuxTrust Signing Stick NCP+ Certificate Profile	1.3.171.1.1.10.3.35	LuxTrust Normalized Certificate compliant with ETSI EN 319 411-1 NCP+ certificate policy, with creation of the keys by the LuxTrust, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.35>.
LuxTrust Signing Server Advanced Automated eSeal Certificate Profile	1.3.171.1.1.10.3.36	LuxTrust Lightweight Certificate Policy Certificate compliant with ETSI EN 319 411-1 LCPcertificate policy, with creation of the keys by the LuxTrust, 4096 -bit key size and two (2) years validity, and with a key usage limited to authentication purpose. These Certificates include the corresponding LuxTrust OID, i.e., < OID 1.3.171.1.1.10.3.36>.
LuxTrust SSL CA		
SSL/TLS(+) Standard Server Certificates, issued by LuxTrust SSL CA	1.3.171.1.1.10.5.1	ETSI TS 102 042 LCP compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.

CP identification	CP OID	Short Description
SSL/TLS(+) Extended Validation Server Certificates - EVCP, issued by LuxTrust SSL CA	1.3.171.1.1.10.5.2	ETSI TS 102 042 EVCP compliant certificate, produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail.
SSL/TLS(+) Extended Validation Server Certificates – EVCP+, issued by LuxTrust SSL CA	1.3.171.1.1.10.5.3	ETSI TS 102 042 EVCP+ compliant certificate, on Secure User Device, produced by SSL CA, 2048-bit key size, (1) or (2) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for server and client authentication and secure e-mail. This profile is anticipated for future usage.
Object Signing(+) Certificates, issued by LuxTrust SSL CA	1.3.171.1.1.10.5.4	ETSI TS 102 042 LCP compliant certificate produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption. Not currently supported.
LuxTrust SSL/TLS Certificate for Client Authentication issued by LuxTrust SSL CA	1.3.171.1.1.10.5.5	ETSI TS 102 042 LCP compliant certificate produced by SSL CA, with creation of the keys by the Subscriber, 2048-bit key size, (1), (2) or (3) years validity, and a key usage combining digital signature (dS bit), key and data encryption as well as extended key usage for client authentication and secure e-mail.
SSL/TLS QCP-w Extended Validation Server Certificates	1.3.171.1.1.10.5.6	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.
LuxTrust Global Corporate CA		
LuxTrust Corporate LCP Certificate Profile	1.3.171.1.1.10.4.1	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.
LuxTrust Global Timestamping CA		
LuxTrust Timestamping certificate	1.3.171.1.1.10.8.1	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.

3 Reliance limits

LuxTrust does not set reliance limits for certificates issued under this policy. Reliance limits may be set by other policies, application controls, applicable law or by agreement. See Limitation of Liability, below.

For the usage limitations (digital signatures, seals, authentication...), see previous section.

LuxTrust S.A. acting as CSP keeps internal records or ensures the archival, in a trustworthy manner, of the following items:

- All certificates for a period of a minimum of 10 years after the expiration of that certificate;
- Audit trails on the issuance of certificates for a period of a minimum of 10 years after issuance of a certificate;
- Audit trail of the revocation of a certificate for a period of a minimum of 10 years after revocation of a certificate;
- Registration related information combined by LRAO once registration of a Subscriber is performed (including certificate re-key). LRAO securely stores and archives the Subscriber's application related information in an appropriate secure location according to the requirements laid down in relevant sections of the CPS and the applicable CP. This archiving is done on paper-based and/or electronically collected information for a minimum of 10 years following registration.
- CRLs for a minimum of 10 years after publishing;
- The very last back up of a CA archive for 10 years following the issuance of the last certificate by this CA.

4 Obligations of subscribers

The Subscriber accepts the Certification Practice Statement (CPS) currently in effect, as provided by LuxTrust S.A. acting as CSP and setting out the procedures used for providing the Certificates.

The Subscriber agrees to the CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the CPS and the applicable CP (<https://www.luxtrust.lu/en/simple/591>). (S)he is also committed to comply with the rules of General Conditions of sale (<https://www.luxtrust.lu/en/simple/556>).

In particular, the Subscriber is liable towards Relying Parties for any use that is made of his / her secure cryptographic device, including the keys or Certificate(s), unless (s)he can prove that (s)he has taken all the necessary measures for a timely revocation of his / her Certificate(s) when required.

The certificates and private keys should be made inaccessible to others and used only for the usage purpose defined in Section 2.

5 Certificate status checking obligations of relying parties

The following statements must be considered and complied with by any Relying Party:

- Receive notice and adhere to the conditions of the applicable CP and of the LuxTrust CPS and associated conditions for Relying Parties.
- Decision to rely on a certificate must always be a *conscious* one and can only be taken by *the Relying Party itself based on RFC 5280*.
- Therefore, *before deciding to rely on a certificate, one must be assured of its validity*. If the Relying Party is not certain that its software performs such checks automatically, the Relying Party has to open the Certificate by clicking on it and checking that the Certificate is **NOT** either
 - *expired* – by looking at the “valid from ___ to ___” notice; *or*
 - *suspended or revoked* – by following the link to the Certificate Revocation List (CRL) and making sure that the certificate is not listed there, using the OCSP validation services or the web based interface allowing to check the status of a Certificate.
- **Never rely on expired or revoked certificates.**
- Without prejudice to the warranties provided in the present CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it. LuxTrust S.A. acting as CSP accepts liability up to an aggregate limit as specified in the general terms and conditions for the concerned service for direct losses, due to non-compliance with this LuxTrust CPS, towards a Relying Party reasonably relying on a Certificate.
- Without prejudice to the warranties provided in the applicable CP or in the LuxTrust CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- If a Relying Party relies on a Certificate without following the above rules, LuxTrust S.A. will not accept liability for any consequences.

- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt.
- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify LuxTrust S.A. acting as CSP.

Relying Parties must use online resources that the CA makes available through its repository to check the status of a Certificate before relying on it. The CA updates OCSP, CRLs and the Web based interface Certificate revocation status service accordingly at the following URLs:

- CRLs are available from <http://crl.luxtrust.lu/>
- OCSP service is available from <http://ltgroot.ocsp.luxtrust.lu>, <http://qca.ocsp.luxtrust.lu/>, <http://ssl.ocsp.luxtrust.lu/>
- Web interface for Certificate status checking services is available from <https://status.luxtrust.lu/> and allows a user to obtain status information regarding his own Certificate.

6 Limited warranty and disclaimer/Limitation of liability

6.1 Damages covered and disclaimers

Except as expressly provided elsewhere in the CPS, the applicable CP and in the applicable legislation, LuxTrust S.A. acting as CSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. LuxTrust S.A. does not warrant "non repudiation" of any Certificate or message. LuxTrust S.A. does not warrant any software.

6.2 Loss limitations

To the extent permitted by law, LuxTrust S.A. makes the following exclusions or limitations of liability:

- In no event shall LuxTrust S.A. be liable for any indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, digital signatures, or other transactions or services offered or contemplated by the CPS even if LuxTrust S.A. has been advised of the possibility of such damages.
- In no event shall LuxTrust S.A. be liable for any direct, indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use or the reliance of a suspended, revoked or expired Certificate.
- The limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages, incurred by any person, including without limitation a Subscriber, an applicant, a recipient, or a Relying Party, that are caused by reliance on or use of a Certificate LuxTrust S.A. issues, manages, uses, suspends or revokes, or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim.
- By accepting a Certificate, the Subscriber agrees to indemnify and hold LuxTrust S.A. and his agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that LuxTrust S.A. and its agents and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:
 - Falsehood or misrepresentation of fact by the Subscriber;
 - Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive LuxTrust or any person receiving or relying on the Certificate;

- Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key.

6.3 Limitations of liability

The liability of LuxTrust S.A. acting as CSP towards the Subscriber or a Relying Party is limited according to other sections of the CPS (e.g., but not limited to section 9) and to the extent permitted by law.

In addition, within the limit set by the Grand Duchy of Luxembourg law, in no event (except for fraud or wilful misconduct) will LuxTrust S.A. be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or digital signatures;
- Any other damages.

The certificate generation and revocation management is independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, is free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

7 Applicable agreements

LuxTrust publishes at the following repository [CP-CPS](#) the certificate policy and certificate practice statements.

8 Privacy policy

Personal data is managed by the TSP and its information systems according to the Luxembourg and European regulations, in particular, the EU Data Protection Act.

Registration information is, among others, personal data.

8.1 Confidentiality of business information

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and in particular relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions are provided within the CPS.

LuxTrust S.A. acting as a CSP guarantees the confidentiality of any data not published in the Certificates, according to the applicable laws on privacy, as well as according to the Luxembourg laws on the financial sector, specifically with regard to banking secrecy.

8.2 Protection of personal information

LuxTrust S.A. acting as a CSP operates within the boundaries of the Luxembourg law of 02/08/2002 on Privacy Protection in relation to the processing of personal data implementing the European Union Directive 95/46/EC On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data. LuxTrust also acknowledges Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector.

Personal data communicated to LuxTrust S.A. by the applicant are entered into a file held by the LuxTrust LRA exclusively.

8.3 Retention time

See above for the retention time of registration information.

9 Refund policy

A refund request can be requested by subscribers if the obligations that have to be fulfilled by LuxTrust are not met.

10 Applicable law, complaints and dispute resolution

The CPS and provision of LuxTrust PKI Services are compliant to relevant and applicable laws of Grand Duchy of Luxembourg.

Prior to litigation, the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters is ruled by the "LuxTrust Dispute Resolution Procedure" as publicly available from <https://repository.luxtrust.lu>.

The courts of the judicial district of Luxembourg-city have exclusive competence for any dispute arising from, or in connection with, the CPS.

11 TSP and repository licenses, trust marks, and audit

With regards to the provision of LuxTrust Normalised Certificates and qualified certificates LuxTrust S.A. acting as CSP through its LuxTrust CAs operates:

- According to [Regulation \(EU\) N°910/2014](#) on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)

LuxTrust S.A. acting as CSP accepts compliance audit for its LuxTrust CAs and all its supporting certification services to ensure they meet the ILNAS requirements for the voluntary "Supervision of Certification Service Providers issuing certificates or providing other services related to electronic signatures" as described and available on the official ILNAS website, www.ilnas.lu.

ILNAS is the national supervisory body, which is responsible for undertaking supervision of LuxTrust under the regulation N°910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market ([supervision procedure](#)).

LuxTrust is certified by LSTI acting as certification accredited body. This certificate is publicly available on the LSTI website: http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.

The Luxembourg's Trusted List is available at the following URL: [Trusted list](#).