LuxTrust Certification Practice Statement

Version number: 2.00

Publication Date: 10/08/2010

Effective Date: 25/08/2010

Document O.I.D: 1.3.171.1.1.1.1.0.*2(version).00(sub-version)*

Document Information

Document title:	LuxTrust Certification Practice Statement
Project Reference:	LuxTrust S.A.
Document Archival Code:	

Version History

Version	Who	Date	Reason of modification
1.7	PHI	14/04/2009	modifications to conform to EDP audit requirements
1.8	PHI	18/05/2009	modifications to conform to ETSI TS 101 456 following ILNAS audit findings
1.9	PHI	28/10/2009	insertion of ILNAS logo including accreditation reference and technical standards reference
1.95	PHI	15/12/2010	minor corrections
2.00	MSC	20/04/2011	Inclusion of “Mass Signature Service”, Annual review

Table of content

Intellectual Property Rights

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 1er 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 Time Stamping Policy. Document OID 1.3.171.1.1.3.1.0, latest version in force.

1 INTRODUCTION

1.1 Overview

1.1.1 The LuxTrust project

The LuxTrust project was created in the form of a Trusted Third Party (hereafter also "TTP"), with an international reach, aiming to establish a national expertise centre 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 [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.

1.1.2 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;
- Encryption facilities;
- Trusted Time Stamping;

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

1.1.3 LuxTrust PKI Hierarchy

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

- One Internationally recognised root : "GTE Cybertrust Global Root" which cross-signs the "LuxTrust Root CA"
- One "LuxTrust Root CA" root-signing all subordinates LuxTrust CAs
- One "LuxTrust Qualified CA" and one "LuxTrust Normalised CA". Each of these CAs is root-signed by the LuxTrust Root CA. The LuxTrust Qualified CA issues end-entity certificates. The LuxTrust Normalised CA does no more issue end-entity certificates.
- Additional CAs or CA hierarchies might be root-signed in the future under the LuxTrust Root CA

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 the LuxTrust Root CA, LuxTrust Normalised CA and LuxTrust Qualified CA. Additional CAs may be root-signed by the LuxTrust Root CA in the future.

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 certification services through any one of its CAs, as described in section 1.3.

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.

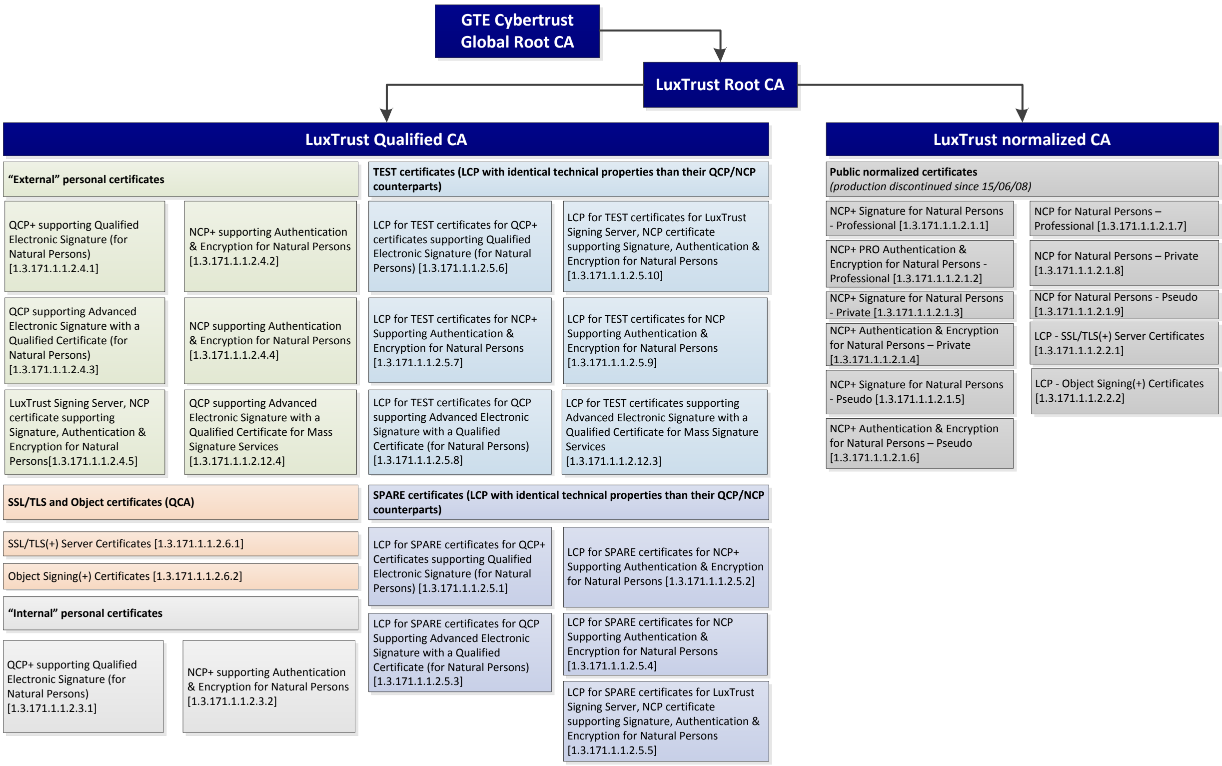

Figure 1 - LuxTrust PKI CA hierarchy, related CPS/CPs and contractural documents

1.1.4 The present document

The present document is the LuxTrust S.A. public statement of the practices followed by LuxTrust CAs when issuing certificates, and is therefore named the "LuxTrust Certification Practice Statement" or "LuxTrust CPS". Throughout this document, the use of the term "CPS" refers to the current document, unless otherwise specified.

The purpose of the present CPS Summary is to describe:

- Practices that are common to all certificate types (or policies) and that are relating to all certificate life cycle services (e.g., issuance, management, revocation, renewal or re-keying, etc.),
- Some details of the LuxTrust trustworthy systems and operations, as well as
- Some details concerning other business, legal and technical matters, common to all certificate types (or policies).

The LuxTrust CPS refers and encompasses several so-called Certificate Policies (CPs) that are "named sets of rules that indicate the applicability of a certificate to a particular community and/or class of applications with common security requirements". The purpose of each CP is to establish what Participants (CAs, and/or component services providers) within the LuxTrust PKI must do in the context of requesting, issuing, managing and using the specific type of certificates described in the related CP. The set of rules, requirements and definitions stated within a CP determines the level of security and assurance provided by this certificate type.

Figure 1 depicts the CA hierarchy as well as the relations between certificate policy documents. These CPs shall include by reference and be compliant to the applicable ETSI certificate policies as defined in the technical standards ETSI TS 101 456 [3] and ETSI TS 102 042 [4], accordingly. Issued LuxTrust certificates shall include the OIDs of the CPs or CPS to which they comply.

Note: as an example, a LuxTrust NCP+ Signature certificate for Natural Persons shall refer to the following documents, asserting the compliance of the associated requirements:

- the LuxTrust NCP+ Signature CP for Natural Persons, and
- the NCP+ ETSI TS CP 0.4.0.2042.1.2 related to the issuing of public key certificates requiring a secure user device as defined in the technical standard ETSI TS 102 042 [4].

The referred to applicable CP shall always refer and include by reference the present CPS.

The following table indicates and shortly describes the various types of certificates that are covered by different CPs under the present CPS:

CP identification	CP OID	Document OID	Short Description
"External" personal certificates			
QCP+ supporting Qualified Electronic Signature (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.4.1**	1.3.171.1.1.2.4.0 .x(version) .y(sub-version)	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, 1024-bit key size or 2048 bit key size and three (3) years validity or five (5) 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° 8/005 by the national registry of Accredited Certification Service Providers.
NCP+ supporting Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.4.2**	1.3.171.1.1.2.4.0 .x(version) .y(sub-version)	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, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[1] and key & data encryption. These Certificates are covered by the ILNAS accreditation as registered under the reference N° 8/005 by the national registry of Accredited Certification Service Providers.

[1] Please refer to section 1.4 of the related CP, for certificate usage restrictions.

CP identification	CP OID	Document OID	Short Description
QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.4.3**	1.3.171.1.1.2.4.0 .x(version) .y(sub-version)	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) 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 LTQCA**	**1.3.171.1.1.2.4.4**	1.3.171.1.1.2.4.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[2] and key & data encryption.
LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.4.5**	1.3.171.1.1.2.4.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate issued on a **non** SSCD centralized hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption.
QCP supporting Advanced Electronic Signature with a Qualified Certificate for Mass Signature Services **issued by LTQCA**	**1.3.171.1.1.2.12.4**	1.3.171.1.1.2.12.0 .x(version) .y(sub-version)	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for Mass Signature Services.
SSL/TLS and Object certificates (QCA)			
SSL/TLS(+) Server Certificates **issued by LTQCA**	**1.3.171.1.1.2.6.1**	1.3.171.1.1.2.6.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SCD, produced by QCA, with creation of the keys by the Subscriber, 1024 or 2048-bit key size, (1),(3) or (5) 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.

[2] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

CP identification	CP OID	Document OID	Short Description
Object Signing(+) Certificates **issued by LTQCA**	**1.3.171.1.1.2.6.2**	1.3.171.1.1.2.6.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SCD, produced by QCA, with creation of the keys by the Subscriber, 1024 or 2048-bit key size, (1),(3) or (5) years validity, and a key usage combining digital signature (dS bit), key and data encryption.
SPARE certificates (LCP with identical technical properties than their QCP/NCP counterparts)			
LCP for SPARE certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.5.1**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size or 2048 bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of electronic signature for SPARE purposes of QCP+ signature certificates.
LCP for SPARE certificates for NCP+ supporting Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.2**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[3] and key & data encryption for SPARE purposes of NCP+ authentication and encryption certificates.
LCP for SPARE certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.5.3**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for SPARE purposes of QCP signature certificates.
LCP for SPARE certificates for NCP supporting Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.4**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[4] and key & data encryption for SPARE purposes of NCP authentication and encryption certificates.

[3] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.
[4] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

CP identification	CP OID	Document OID	Short Description
LCP for SPARE certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.5**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a **non** SSCD centralised hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for SPARE purposes of NCP authentication, encryption and signature certificates.
TEST certificates (LCP with identical technical properties than their QCP/NCP counterparts)			
LCP for TEST certificates for QCP+ certificates supporting Qualified Electronic Signature (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.5.6**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SSCD, Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size or 2048 bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of electronic signature for TEST purposes of QCP+ signature certificates.
LCP for TEST certificates for NCP+ supporting Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.7**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate on SSCD Hardware token (e.g., LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[5] and key & data encryption for TEST purposes of NCP+ authentication and encryption certificates.
LCP for TEST certificates for QCP supporting Advanced Electronic Signature with a Qualified Certificate (for Natural Persons) **issued by LTQCA**	**1.3.171.1.1.2.5.8**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for TEST purposes of QCP signature certificates.

[5] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

CP identification	CP OID	Document OID	Short Description
LCP for TEST certificates for NCP supporting Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.9**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[6] and key & data encryption for TEST purposes of NCP authentication and encryption certificates.
LCP for TEST certificates for LuxTrust Signing Server, NCP certificate supporting Signature, Authentication & Encryption for Natural Persons **issued by LTQCA**	**1.3.171.1.1.2.5.10**	1.3.171.1.1.2.5.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant Certificate issued on a **non** SSCD centralised hardware token (i.e., LuxTrust Signing Server), with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to signature, authentication purpose and/or key & data encryption for TEST purposes of NCP authentication, encryption and signature certificates.
LCP for TEST certificates supporting Advanced Electronic Signature with a Qualified Certificate for Mass Signature Services **issued by LTQCA**	**1.3.171.1.1.2.12.3**	1.3.171.1.1.2.12.0 .x(version) .y(sub-version)	ETSI TS 101 456 QCP compliant Qualified Certificate not issued on SSCD Hardware token, with creation of the keys by the CSP, 1024-bit key size or 2048-bit key size and three (3) years validity or five (5) years validity, and with a key usage limited to the support of advanced electronic signature with a qualified certificate for Mass Signature Services.
Public normalised certificates (production discontinued since 15/06/08)			
NCP+ Signature for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.1**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PRO certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to electronic signature
NCP+ Authentication & Encryption for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.2**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PRO certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[7] and key & data encryption.

[6] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

[7] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

CP identification	CP OID	Document OID	Short Description
NCP+ Signature for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.3**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PRIVATE certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to electronic signature
NCP+ Authentication & Encryption for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.4**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PRIVATE certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[8] and key & data encryption.
NCP+ Signature for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.5**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PSEUDONYM certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to electronic signature
NCP+ Authentication & Encryption for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.6**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP+ compliant Normalised Certificate with PSEUDONYM certificate profile on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[9] and key & data encryption.
NCP for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.7**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate with PRO certificate profile on a “LuxTrust Server Signing” token (non-SSCD), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and a key usage combining digital signature (authentication and electronic signature purposes), key and data encryption.
NCP for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.8**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate with PRIVATE certificate profile on a “LuxTrust Server Signing” token (non-SSCD), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and a key usage combining digital signature (authentication and electronic signature purposes), key and data encryption.

[8] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

[9] Please refer to section 1.4 of the related CP, in order to take knowledge of the usage restriction of such a certificate.

CP identification	CP OID	Document OID	Short Description
NCP for Natural Persons **issued by LTNCA**	**1.3.171.1.1.2.1.7**	1.3.171.1.1.2.1.0 .x(version) .y(sub-version)	ETSI TS 102 042 NCP compliant Normalised Certificate with PSEUDONYM certificate profile on a “LuxTrust Server Signing” token (non-SSCD), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and a key usage combining digital signature (authentication and electronic signature purposes), key and data encryption.
SSL/TLS(+) Server Certificates **issued by LTNCA**	**1.3.171.1.1.2.2.1**	1.3.171.1.1.2.2.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SCD, with creation of the keys by the Subscriber, 1024 or 2048-bit key size, (1),(3) or (5) 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.
Object Signing(+) Certificates **issued by LTNCA**	**1.3.171.1.1.2.2.2**	1.3.171.1.1.2.2.0 .x(version) .y(sub-version)	ETSI TS 102 042 LCP compliant certificate, on SCD, with creation of the keys by the Subscriber, 1024 or 2048-bit key size, (1),(3) or (5) years validity, and a key usage combining digital signature (dS bit), key and data encryption.

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 (e.g., LRAO registering LuxTrust end-users), etc. (Document OID 1.3.171.1.1.2.3.0.x.y).

LuxTrust also issues certificates from a TEST QCA platform which are technically identical to production certificates but which are signed by a test QCA root certificate (Document OID 1.3.171.1.1.2.7.0.x.y.)

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), see section 1.3.5.6 of the present document. These services consist of the management of the infrastructure, and the provisioning of Time Stamp Tokens according to the LuxTrust Time Stamping Policy [12].

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 [1]. LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping policy [12].

The LuxTrust CSP Board acts as Policy Approval Authority (see section 1.5.1) for LuxTrust S.A.. In particular the CSP board manages the LuxTrust Certification Practice Statement (CPS) and all related CPs, covering the statements of the practices followed by LuxTrust S.A. acting as CSP in issuing CA and end-entities certificates as well as in issuing TSTs through its TSAs.
By means of the CPS and related CPs, LuxTrust S.A. acting as CSP indicates and guarantees that it complies with regulatory and standard texts applicable, and whether or not this guarantee is supported by an accreditation as well as the name and coordinates of the accreditation body.

1.2 Document name and identification

This document sets out and identifies the LuxTrust Certification Practice Statement (CPS). The present LuxTrust CPS can be identified by any party through the following OID:

1.3.171.1.1.1.1.0.x(version).y(sub-version)

This LuxTrust CPS (OID) shall be inserted by reference within each and every Certificate Policy ruled by the LuxTrust CPS.

1.3 PKI Participants

The LuxTrust PKI Participants are the legal entities or set of legal entities filling the role of participant within the LuxTrust PKI, that is either making use of or providing LuxTrust PKI (component) services that are used by LuxTrust S.A. acting as CSP to provide its LuxTrust certification services.

These PKI Participants within the LuxTrust PKI are identified as follows:

- Certification Authorities
- Central & Local Registration Authorities
- Subscribers
- Relying Parties
- And other Participants as:
- CA Factory Services Provider
    - (Secure) Signature Creation Device (SSCD) Providers
    - Certificate Revocation Status Services Provider
    - Suspension Revocation Authority
    - Dissemination (Publication) and Repository Services
    - Time Stamping Services
    - Root Signing Services Provider

The aforementioned parties are collectively called the PKI Participants. All PKI Participants implement practices, procedures and controls conforming to the requirements expressed within the LuxTrust CPS and the applicable CP. For clarification purposes, the following diagram illustrates the high level interrelationship between the LuxTrust PKI component services.

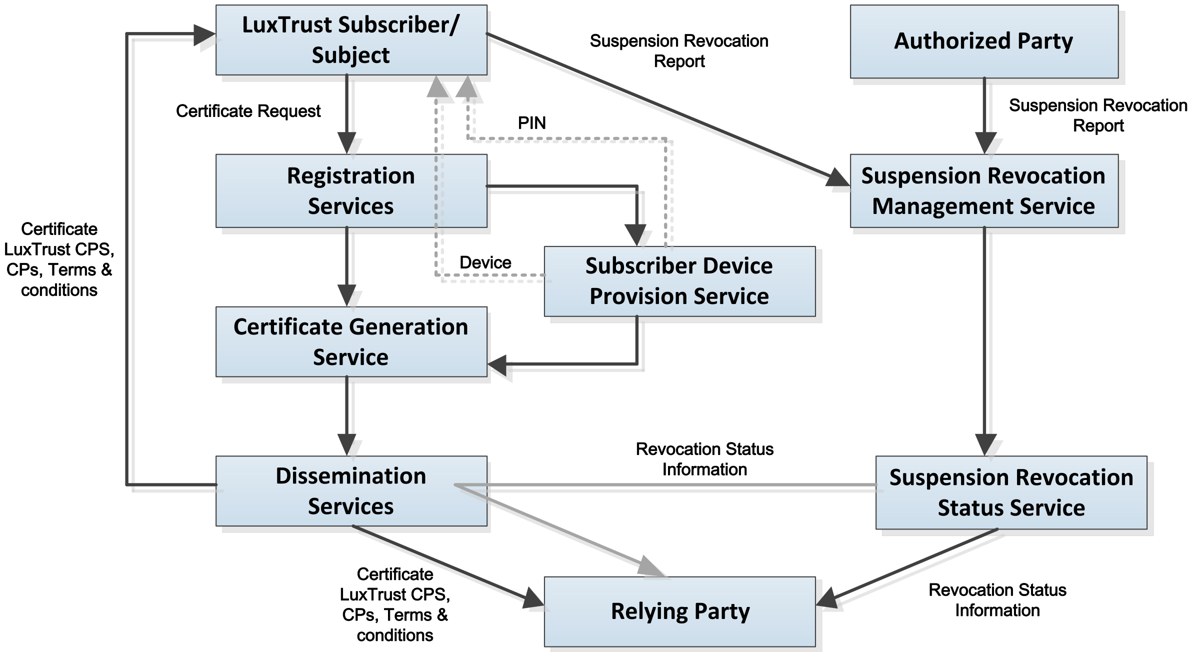

Figure 2 - Illustration of LuxTrust certification services

The next schema provides a high level view on the identified LuxTrust PKI Participants:

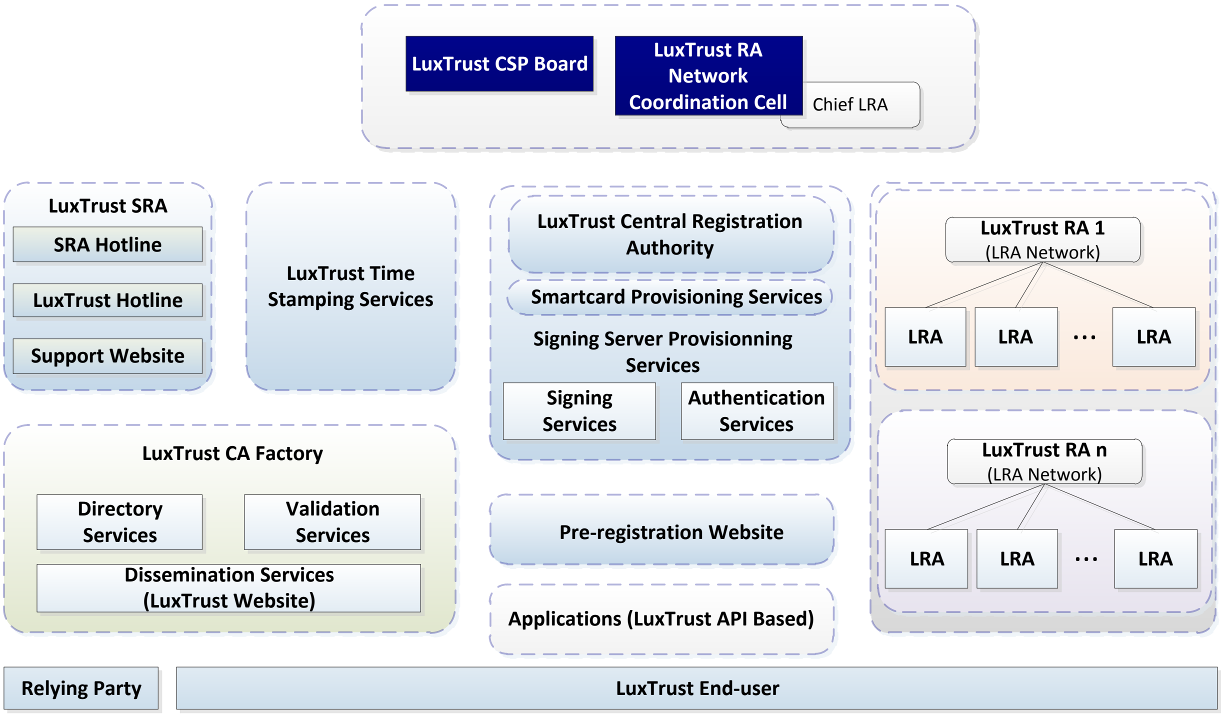

Figure 3 - LuxTrust PKI Components, PKI participants and relying parties

The complete (technical, logical, physical) description of the entire LuxTrust PKI, including the provision of Time Stamping Services is fully detailed in LuxTrust S.A. internal and sensitive documents.

1.3.1 Certification Authorities

As described in section 1.1.3, LuxTrust S.A. acting as CSP is using several Certification Authorities (CAs) to issue LuxTrust Certificates.

1.3.1.1.1 Three-level CA hierarchy

The top level root is the *GTE Cybertrust Global Root* managed by Verizon Business, which cross-signs the *LuxTrust ROOT CA*, the highest level of authority managed by LuxTrust. The LuxTrust PKI is formed using two additional subordinate, cross-signed CAs: The "*LuxTrust Normalised CA*" and the "*LuxTrust Qualified CA*". The legal person (organisation) responsible for these CAs is LuxTrust S.A. acting as CSP.

The "LuxTrust Normalised CA" (hereafter "LTNCA") and the "LuxTrust Qualified CA" (hereafter "LTQCA") operate within a grant of authority for issuing respectively *LuxTrust Normalised Certificates* and *LuxTrust Qualified Certificates* under the LuxTrust CPS and the applicable CP depending on the type of Certificate that is issued. This grant has been provided by the "LuxTrust Root CA" (hereafter "LTRCA") under the responsibility and authority of LuxTrust S.A. acting as CSP.

Note 1: *Unless explicitly otherwise indicated, "the CA", refers to both LTNCA and LTQCA granted to issue Certificates within their respective domain by the LuxTrust Root CA. 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.

The LTNCA and LTQCA, as well as all supporting component services, are accredited respectively against ETSI TS 102 042 [4] and ETSI TS 101 456 [3] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 august 2000 on electronic commerce as modified. ILNAS is the accreditation entity. For further details please refer to section 8 of the present CPS.

LuxTrust S.A. can be contacted, using the coordinates as provided in the section 1.5.1 of the present CPS. The technical management and operations of the LuxTrust LTRCA, LTNCA and LTQCA (including the Certificate generation services) are compliant with the present CPS and provided through a CA Factory Services provider (see section 1.3.5.1), within secure facilities with disaster recovery in Grand-Duchy of Luxembourg.

The LuxTrust PKI component services supporting the LuxTrust certification services are common to the LuxTrust CAs for their respective CA domains within the LuxTrust PKI.

1.3.2 Registration Authorities

The LuxTrust Registration Authority Network is made of a Central Registration Authority (CRA) and of a set of Registration Authorities (RAs), each of them composed of one or several Local Registration Authorities.

- The **Central Registration Authority** (CRA).
- The **Registration Authority** (RA).
- The **Local Registration Authority** (LRA): Its mission is to proceed to face-to-face registration of LuxTrust applicants, and to validate certificate un-suspension and revocation requests from certified users when physical presence of the user is requested.

All communications between LRAs, CRA, SRA, CAs, and other (e.g. SSCD) Service Providers regarding any phase of the life cycle of the Certificates are secured with PKI based encryption and signing techniques to ensure confidentiality, mutual authentication and secure logging/auditing.

1.3.2.1 Central Registration Authority - CRA

The CRA aims to share RA facilities for several LRAs and provide a central operational communication interface between the RAs and the rest of the LuxTrust PKI Participants (e.g., Certificate factory, LuxTrust token providers, Suspension and Revocation Authority - SRA), as well as performing re-key from subscribers. In particular, the task of certificate suspension, notification of changes in the information supporting the certification process of an end-user, password reset requests will be centralised in CRA activities.

The CRA is the entity that has final authority and decision upon the issuance, the suspension and revocation of a Certificate under all CPs covered by the present CPS.

The CRA interacts indirectly and/or directly with the Subscribers and directly with the CA to deliver public certification services to the Subscribers:

- By setting up a Suspension Revocation Hotline Service for immediate suspension of certificate (suspended status of the certificate will immediately be updated in the entries of the Certificate Suspension/Revocation Status Services) through a 24/7 hot line. Contact details of this SRA Hotline are available at https://sra.luxtrust.lu.
- By setting-up a LuxTrust Hotline and support website for help desk services, those are available at https://helpdesk.luxtrust.lu.
- By registering Subscribers for certification services
- By setting up facilities
    - For notification of changes in certified information or in information supporting certification. Note that any change to certified information shall lead to the suspension (minimum) or the revocation of the related certificate).
    - For collection and approval of requests related to the provision of a new password for Signing Server accounts

  Those facilities are available online at https://helpdesk.luxtrust.lu and https://sra.luxtrust.lu.

All LRAs and RAs are connected to the LuxTrust CA Factory via the Central Registration Authority (CRA), for electronic processing of certificate requests. The CRA is the central instance that performs much of the interfacing from Local Registration Authorities and Registration Authorities towards the CA, the Smart Card Issuing Authority, or the Server Signing service provisioning entities.

The purpose of the CRA is to perform routing operations for information flows within the infrastructure and includes strong tracing and audit capabilities. This provides Registration Authorities with the ability to trace back data changes and manipulations, as well as to enforce accountability for registration authority operations.

The LuxTrust CSP Board directly controls the “LuxTrust RA Network Coordination Cell” in charge of the global coordination of the LuxTrust Registration Authority (RA) Network including the Central Registration Authority (CRA) and the Local Registration Authorities organised in several groups known as LRA Networks.

The LuxTrust RA Network Coordination Cell is in charge of the initialisation and registration of LuxTrust PKI specific end-entities, such as CRA Officers, LRA Officers, PKI Participants other than Subscribers and Relying Parties (e.g., Time Stamping Authority, (S)SCD services providers) . Punctually and exceptionally, the cell may also perform LuxTrust end-user registration.

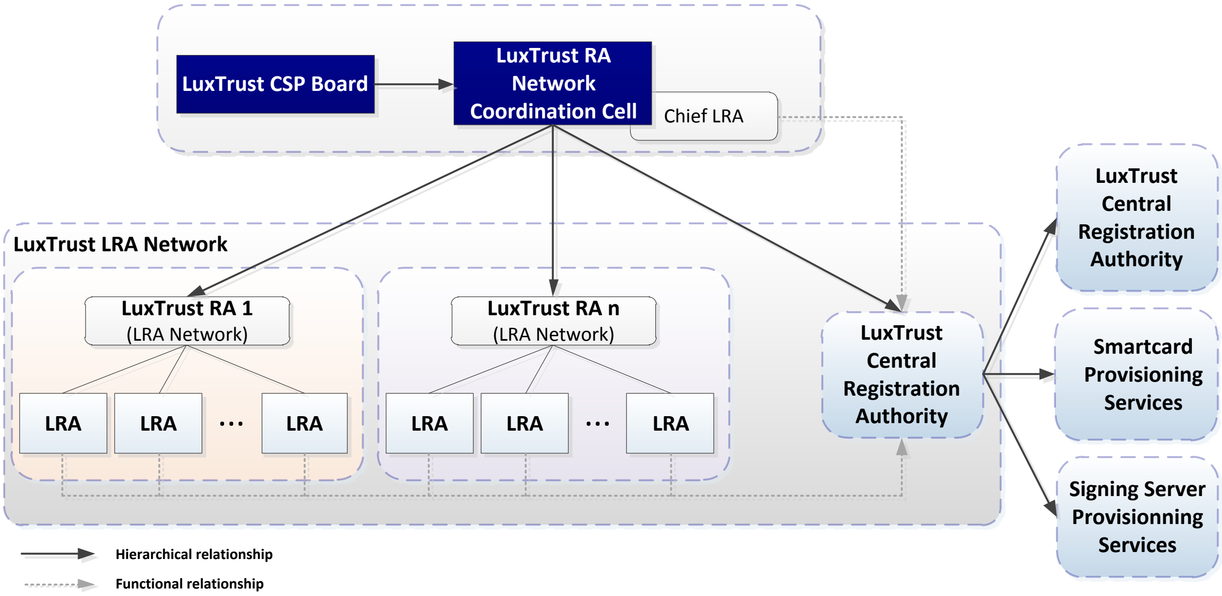

Figure 4 - LuxTrust Registration Authorities

The LuxTrust CSP Board will translate the general registration services dispositions from the LuxTrust CPS and Certificate Policy(ies) into specific procedural instructions for the different RAs. These procedures will be communicated and enforced through the LuxTrust RA Network Coordination Cell.

The provision of Central Registration Services is ensured by U-Trust[10] consortium under a signed contractual agreement with LuxTrust S.A. acting as CSP, under the present CPS and in compliance with the related LuxTrust CPs.

1.3.2.2 Registration Authority - RA

The **Registration Authorities** (RA) aim to operate one or several LRAs and may proceed, under strictly determined and controlled conditions, to the validation of LuxTrust specific face-to-face or remote registration.

1.3.2.3 Local Registration Authorities

The mission of the Local Registration Authorities (LRA) is to proceed to the registration of the LuxTrust new users (Subscribers) and to validate the certificate suspension, un-suspension and revocation requests from the certified Subscribers when their physical presence is requested. With regards to registration, LRAs may have direct contact with the Subscribers and must have direct contact with their RA, but have no direct contacts with the CA.

Within the CA domain, a Local Registration Authority registers and verifies Subscriber's application data on behalf of the CRA. With regards to registration, LRAs may have direct contact with the Subscribers and must have direct contact with the CRA, but have no direct contacts with the CA.

Following tasks are performed by Local Registration Authorities:

- Registration of end-users subscription to LuxTrust certification services
- Suspension, un-suspension or revocation of Subscribers' certificates
- Specific customer oriented tasks (while these will be centralised to a maximum, e.g. notification of changes in certified information or in information supporting certification, request for information, etc.)

[10] The U-Trust consortium is constituted by legal persons, see Glossary

The provision of Local Registration Services under the present CPS, in compliance with the related LuxTrust CP is enforced through signed contractual agreement with LuxTrust S.A. acting as CSP. An official and exhaustive list of legal entities authorized to act as LRAs is available on the LuxTrust website under the following URL: https://ra.luxtrust.lu.

See the related CP for further details.

1.3.3 Subscribers

The Subscribers of the CA services in the LTNCA and LTQCA domains are either:

- physical persons identified as private persons, or
- physical persons identified as private persons entitled to represent a legal person or qualified by professional attributes (e.g., self-employed, employee), or
- physical persons either identified as private persons, or identified as private persons entitled to represent a legal person or qualified by professional attributes (e.g., self-employed, employee) and registering a non-physical entity as Subject of a LuxTrust Certificate (e.g., (web) server, object signing entity, etc.).

In the first two cases listed above the Subscriber is the Subject of the issued LuxTrust Certificate.

In order to be eligible for receiving CA services, the Subscriber shall comply with the requirements related to the Certificate application procedures and to the Subscriber's obligations and liabilities as stated in the present CPS and in the relevant sections of the applicable CP. See the applicable CP for further details and/or restrictions on Subscriber's eligibility to receive CA services.

1.3.4 Relying Parties

Relying Parties are entities including physical or legal persons who rely on a Certificate and/or a security operation verifiable with reference to a public key listed in a Certificate. Prior to relying on digital certificates for security operations, Relying Parties must always ensure:

- The validity of the certificate through CA Certificate Revocation Status Services (e.g., OCSP, CRL, …)
- The context in which the certificate is used against the Certificate Policy.

Relying Parties shall also comply with the Relying Parties obligations and liabilities as stated in the present CPS and in the relevant sections of the applicable CP.

Note: Relying Parties are entities that are not necessarily Subscribers.

1.3.5 Other Participants

1.3.5.1 CA Factory Services Provider

The provision of CA Factory Services under the present CPS, in compliance with the relevant LuxTrust CPs is ensured by U-Trust under a signed contractual agreement with LuxTrust S.A. acting as CSP.

1.3.5.2 (Secure) Signature Creation Device Provider

The provision of physical end-user (Secure) Signature Creation Device ((S)SCD) Services, namely the LuxTrust Smart Card and other smart token provisioning facilities services under the present CPS, in compliance with the relevant LuxTrust CPs is ensured by U-Trust under a signed contractual agreement with LuxTrust S.A. acting as CSP.

The provision of LuxTrust Signing Server facilities, under the present CPS, and in compliance with the relevant LuxTrust CPs is ensured by U-Trust under a signed contractual agreement with LuxTrust S.A. acting as CSP.

1.3.5.3 Certificate revocation status Services Provider

The provision of Certificate Revocation Status Services under the present CPS, in compliance with the relevant LuxTrust CPs is ensured by U-Trust under a signed contractual agreement with LuxTrust S.A. acting as CSP.

1.3.6 Suspension Revocation Authority

The provision of Suspension Revocation Authority Services under the present CPS, in compliance with the relevant LuxTrust CPs is ensured by U-Trust under a signed contractual agreement with LuxTrust S.A. acting as CSP.

1.3.7 Dissemination (Publication) and Repository Services

The Dissemination Services (publication of CPS, CP's, General Terms and Conditions, and other public LuxTrust CSP related documents if any) are available from the official LuxTrust CSP Web Site. This interface also allow access to former versions of official documents (CPS, CP's, GTC, PO's), CRLs, CA certificates, certificates download, certificates status. Dissemination and Repository Services are provided as described in section 2 of the present CPS.

1.3.8 Time Stamping Services

The LuxTrust Time Stamping Services support assertions of proofs that an electronic record existed before a particular time. These services can be used in support to non-repudiation services, to prove that an electronic signature was generated during the validity period of a public key certificate, to support electronic long term archiving, etc.

The LuxTrust Time Stamping services are provided under the authority of LuxTrust S.A. acting as Time Stamping Services Provider, according to

- IETF RFC 3161 and 3628,
- ETSI TS 102 023 and 101 861
- ISO/IEC 18014 (1-2-3) technical standards,
- LuxTrust Time Stamping Policy [11]

Time Stamp tokens are signed by a LuxTrust S.A. certified key. See the LuxTrust Time Stamping Policy for further details [12].

The LuxTrust Time Stamping Services are accredited by ILNAS against ETSI TS 102 023 [6] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic. For further details please refer to the LuxTrust Time Stamping Policy [12].

1.3.9 Root Signing Services

The Root Signing Services Provider ensures that LTRCA remains trusted by widely used applications and notifies LuxTrust S.A. of any event affecting trust to its own root. The entity providing Root Signing Services to the LTRCA is GTE Cybertrust Global Root in compliance with the LuxTrust CPS and under a contractual agreement signed with LuxTrust S.A. acting as CSP.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Appropriate certificate uses of Certificates issued under a specific CP covered by the present CPS are described in this applicable specific CP.

The applications for which the Certificate is deemed to be trustworthy must be decided by the Relying Parties themselves on the basis of the nature and purpose (incl. key usage) of the Certificate, including any applicable limitation as written in the Certificate. Complementarily, the relying party must also consider the level of security of the procedures followed for issuance of the Certificate as described in the applicable CP and in the present LuxTrust CPS.

[11] The LuxTrust Time Stamping Practice Statement is made of the combination of the LuxTrust Time Stamping Policy [12] and of the LuxTrust CPS in which practice statements include statement related to the management of the Time Stamping services as part of the LuxTrust PKI.

Key usage and the applicability of the Certificates are certified (see the description of the Certificate content in Section 7 of the applicable CP).

Normalised Certificates issued by the LTNCA or by the LTQCA under this CPS comply with ETSI TS 102 042 [4], according to the NCP+, NCP or LCP requirements respectively and additionally to the applicable requirements from ETSI 101 456 when issued by the LTQCA.

Qualified Certificates issued by the LTQCA under this CPS comply with ETSI TS 101 456 [3], according to the QCP+ or QCP requirements respectively.

1.4.2 Prohibited certificate uses

Usage of Certificates that are issued in the LuxTrust Project, other than to support applications identified in Section 1.4.1 of the present CPS or in the applicable CP is prohibited.

Relying Parties are strongly recommended to make use of the LuxTrust Certificate Policy Notice and OID as identified in the Certificate (see section 1.2 of the applicable CP) to appropriately accept or reject a Certificate usage.

1.5 Policy administration

1.5.1 Organisation administering the document

The Organisation administering the present CPS document is LuxTrust S.A. acting as Certification Service Provider (CSP) via its LuxTrust CSP Board, acting as Policy Approval Authority.

The CSP Board, acting as Policy Approval Authority, is composed of the senior management of LuxTrust S.A.. The procedure used to add or remove members of the CSP Board is determined and ruled by internal documents.

The Policy Approval Authority within LuxTrust S.A. is called the LuxTrust CSP Board. It is the high level management body with final authority and responsibility for:

- Specifying and approving the LuxTrust infrastructure and practices.
- Approving the LuxTrust Certification Practice Statement(s), LuxTrust Certificate Policies and LuxTrust Time Stamping Policies.
- Defining the review process for practices and policies including responsibilities for maintaining the Certification / TSA Practice Statements and Certificate / Time Stamping Policies.
- Defining the review process that ensures that the LuxTrust CAs and TSAs properly implements the above practices.
- Defining the review process that ensures that the Certificate / Time Stamping Policies are supported by the LuxTrust Practice Statement(s).
- Publication to the Subscribers and Relying Parties of the Certificates / Time Stamping Policies and Certification / Time Stamping Practice Statements and their revisions.
- Specifying cross-certification procedures and handling cross-certification requests.

Prior to becoming applicable, modifications to the CPS are announced in the repository as available on https://repository.luxtrust.lu.

The CSP board can be contacted using the following coordinates:

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*

1.5.2 Contact person

The contact person, designated by LuxTrust S.A., via its LuxTrust CSP Board acting as Policy Approval Authority, is a LuxTrust CSP Board member. See section 1.5.1 for contact details.

1.5.3 Entity determining suitability between CPS and covered CPs

The Entity determining suitability between CPS and CPs is LuxTrust S.A. acting as CSP, via its LuxTrust CSP Board acting as Policy Approval Authority. See section 1.5.1 for contact details.

1.5.4 CPS and covered CPs Approval Procedure

The Entity approving the present CPS and the covered CPs is LuxTrust S.A. acting as CSP, via its LuxTrust CSP Board acting as Policy Approval Authority. See section 1.5.1 for contact details. The procedure used to approve documents is determined and ruled by internal documents.

1.6 Definitions and acronyms

1.6.1 Definition

Name	Definition
Advanced Electronic Signature [1]	Refers to Electronic Signature meeting the following requirements: – It is uniquely linked to the signatory; – It is capable of identifying the signatory; – It is created using means that the signatory can maintain under his sole control; and – It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Certification Authority (CA) [2]	Authority trusted by one or more users to create and assign certificates. A certification authority may optionally create the users' keys.

Certificate [2]	Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.
Certificate Identifier	A unique identifier of a Certificate consisting of the name of the CA and of the certificate serial number assigned by the CA.
Certificate Policy (CP) [2]	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement [2]	Statement of the practices which a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Certificate Validity Period	The time interval during which the CA warrants that it will maintain information about the status of the certificate. (Time interval between start validity date and time and final validity date and time).
Certificate Revocation List (CRL) [2]	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certification Path [3]	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Service Provider [1]	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Commitment Type	A signer-selected indication of the exact intent of an electronic signature.
CRL Distribution Point	A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.
Data To Be Signed (DTBS)	The complete electronic data to be signed (including both Signer's Document and Signature Attributes).
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient
End Entity	A certificate subject that uses its public key for purposes other than signing certificates
Electronic Signature	– European Directive [1]: means data in electronic form that are attached to or logically associated with other electronic data. – 14/08/2000 Luxembourg Law [7]: Art. 6. « Signature » - Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé : "La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte. Elle peut être manuscrite ou électronique. La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article."

Hash Function	Cryptographic function that maps a variable length string of bits to fixed-length strings of bits, satisfying the following two properties: − It is computationally unfeasible to find for a given output an input which maps to this output; − It is computationally unfeasible to find for a given input a second input which maps to the same output.
Key Pair	Public Key and the corresponding Private Key.
Mass Signature Services (MSS)	LuxTrust service providing advanced signature based on Qualified Certificates following QCP Public, whose certificates are covered by this CP. Signature Creation Devices remains within LuxTrust premises and Subjects are provided with secure access through the public internet.
De-centralized Mass Signature Service (D-MSS)	LuxTrust service providing advanced signature based on Qualified Certificates following QCP Public, whose certificates are covered by this CP. Signature Creation Devices are located within the Subjects' premises and Subjects are provided with secure access to the devices through their networks.
Object Identifier (OID)	Sequence of numbers that uniquely and permanently references an object.
Online Certificate Status Protocol (OCSP) Provider	Online trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the OSCP server (which contains the certificate status) and the client application (which is informed of that status).
Public Key	Key of an entity's asymmetric key pair that can be made public.
Private Key	Key of an entity's asymmetric key pair that should only be used by that entity.
Qualified Certificate [1]	Certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive [1].
Secure User Device [4]	Device which holds the user's private key and protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signature Attributes	Additional information that is signed together with the Signer's Document.
Signature Creation Data [1]	Refers to unique data, such as codes or private cryptographic keys used by the signatory to create an electronic signature.
Signature Creation Device [1]	Refers to configured software or hardware used to implement the signature creation data.
Signature Policy	Set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.
Signature Policy Identifier	Object Identifier that unambiguously identifies a Signature Policy.
Signature Policy Issuer	Organization creating, maintaining and publishing a signature policy.
Signature Policy Issuer Name	Name of a Signature Policy Issuer.
Signature Verification	Process performed by a verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.

Signature-Verification-Data [1]	Data, such as codes or public cryptographic keys used for the purpose of verifying an electronic signature.
Signature-Verification Device [1]	Configured software or hardware used to implement the signature verification-data.
Signatory [1]	A person who holds a signature creation device and acts either on his own behalf or on behalf of the natural legal person or entity he represents.
Signer	Entity that creates an (electronic) signature.
Signer's Identity	Registered name of the signer (i.e. as registered by the CSP supplying the signer's certificate).
Signer's Document	Electronic data to which the electronic signature is attached to or logically associated with.
Subject	Entity to which a Certificate is issued.
Subscriber	Entity that requests and subscribes to a Certificate and for which it is either the Subject or not.
Trusted Third Party (TTP)	Authority trusted (and widely recognised, possibly accredited) by one or more users to provide Trusted Services such as Timestamping, Certification …
Time Stamp	Proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.
Time Stamping Authority	Authority trusted by one or more users to provide a Time Stamping Service.
Time Stamping Service	Service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.
U-Trust	Entities that are subcontracting part of the maintenance of LuxTrust activities. U-Trust encompasses: – CETREL S.A.; – Clearstream Services;
Validation Data	Additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.
Verifier	Entity that validates or verifies an electronic signature. This may be either a relying party or a third party interested in the validity of an electronic signature.
What Is Presented is What Is Signed (WIPIWIS)	Description of the required qualities of the interface able to unambiguously present the signer's document to the verifier according to the content format of the signer's document.
What You See Is What You Sign (WYSIWYS)	Description of the required qualities of the interface able to unambiguously present to the signer the document to be signed according to the content and format.

1.6.2 Acronyms:

Acronym	Definition
AES	Advanced Electronic Signature
ARL	Authority Revocation List
B2B	Business to Business
CA	Certification Authority
CME	Cryptographic Module Engineering
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
KYC	Know Your Customer
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NCP	Normalised Certificate Policy
NCP+	Normalised Certificate Policy +
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKCS	Public Key Certificates Standard
PSF	Professionnel du Secteur Financier (FSP – Financial Sector Professional)
QES	Qualified Electronic Signature
QCP	Qualified Certificate Policy
RA	Registration Authority
RAO	Registration Authority Officer
RFC	Request for Comments
RSA	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SCD	Signature Creation Device

SRA	Suspension and Revocation Authority
SRAO	Suspension and Revocation Authority Officer
SSCD	Secure Signature Creation Device
TSP	Time Stamping Policy
TSSP	Time Stamping Service Provider
TSU	Time Stamping Unit
URL	Uniform Resource Locator
UTC	Coordinated Universal Time

1.7 Relationship with the European Directive on Electronic Signatures

The LTNCA and LTQCA are accredited respectively against ETSI TS 102 042 [4] and ETSI TS 101 456 [3] in application of Article 30 of the Grand-Duchy of Luxembourg modified law of 14 August 2000 on electronic commerce. This law is based on European Directive on electronic signatures 1999/93/EC and lays out the legal framework of electronic signatures in the Grand-Duchy of Luxembourg. ILNAS is the accreditation entity.

Electronic signatures supported by a certificate covered by the "**LuxTrust NCP supporting Signature, Authentication and Encryption**" Certificate Policy and issued by the LTQCA, or by the **"LuxTrust NCP+ Signature"** Certificate Policy and issued by the LTNCA, are Advanced Electronic signatures as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

Electronic signatures supported by the "**LuxTrust QCP+ supporting Qualified Electronic Signature**" Certificate are Qualified Electronic Signatures as long as they are generated from **Secure Signature Creation Devices**, and that they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

Electronic signatures supported by a certificate covered by the "**LuxTrust QCP supporting Advanced Electronic Signature with a Qualified Certificate**" Certificate Policy are Advanced Electronic signatures (supported by a Qualified Certificate) as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

See the section 1.4 for further details on authorised and prohibited usages of these certificates.

2 Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

LuxTrust S.A. acting as CSP, via its LuxTrust CSP Board acting as Policy Approval Authority, is the ultimate entity responsible for the operation of online and publicly available repository(ies). LuxTrust S.A. is also responsible for the publication of the following documents and information:

- The present CPS
- The covered CPs
- The related subscriber contractual agreements (e.g., Purchase Orders, General Terms and Conditions, etc.)
- The Certification Authority Certificates, Certification Paths and related ARLs
- The Certificates Public Registry
- The Certificate Revocation Lists (CRLs)
- The LuxTrust Time Stamping Policy [12].

The aforementioned documents and information are available from online publicly available website accessible as described here after. Note: published documents and information can be physically available and managed on repositories that are technically operated by U-Trust consortium.

2.2 Publication of Certification Information

LuxTrust S.A. acting as CSP, via its LuxTrust CSP Board acting as Policy Approval Authority, is the ultimate responsible for the publication of the certification information as listed in section 2.1.

The LuxTrust CPS covering the practices used by the CA for Certificates issuance under the applicable CP is available online on https://repository.luxtrust.lu. This repository shall also contain any other public documents where LuxTrust S.A. acting as CSP makes certain disclosures about its practices, procedures and the content of certain of its policies, including the present CPS, and the covered CPs. It reserves right to make available and publish information on its policies by any means it sees fit.

Unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Subscriber does not agree to the publication of the Certificate in the LuxTrust Public Repository of Certificates immediately on creation. The Subscriber is made aware by the CSP that refusal to publish his Certificates may lead to usage difficulties if his counterpart expects to get the Subscriber's Certificates from the certificate publishing services of LuxTrust.

The LTQCA publishes the digital Certificates that have been accepted to be published by Subscribers and information about these certificates in (an) online publicly available repositories(y). LuxTrust S.A., acting as CSP, reserves right to publish Certificate status information on third party repositories. The Subscribers are notified that the LTQCA shall only publish information they submit as the information to be certified in the Certificate.

The CA publishes CRL's at regular intervals at https://crl.luxtrust.lu as indicated in section 4.9 of the present CPS.

The CA makes available an OCSP responder server at http://ocsp.luxtrust.lu that provides notice on the status of a Certificate issued by the CA, upon request from a Relying Party, in compliance with the IETF RFC 2560. The status information of any Certificate as delivered by the OCSP server shall be consistent with the information listed in the CRL in force, and vice versa.

The CA maintains the CRL distribution point and the information on this URL until the expiration date of all Certificates containing the CRL distribution point.

A web interface for Certificate status checking services is available from https://test.luxtrust.lu and allows a user to obtain status information on a Certificate. See section 2.4 for access restriction.

2.3 Time of Frequency of Publication

2.3.1 Frequency of Publication of Certificates

Certificates are published following certificate issuance as specified in section 4.3 and 4.4.2 of the present LuxTrust CPS and of the applicable CP.

2.3.2 Frequency of Publication of Revocation information

The CRLs are published following to the CRL issuance as specified in section 4.9 of the present LuxTrust CPS and of the applicable CP.

2.3.3 Frequency of Publication of Terms & Conditions

An update of all relevant Terms & Conditions (including the LuxTrust CPS, the General Terms and Conditions and the Purchase Order) is published whenever a change occurs.

2.4 Access Control on Repositories

All repositories as listed in 2.1 are available in public anonymous read-only access. Only Trusted Staff functions, as specified in section 5 of the present CPS have write and change access on these repositories, with strong PKI Credentials based access control. State-of-the-art security measures protect these repositories.

While the primary objective of the CA and of LuxTrust S.A. is to keep access to its public repositories free of charge, it reserves right to charge for publication services such as the publication of Certificate status information (e.g., high volume/bandwidth connections, third party databases, private directories, etc.) and/or to restrict access to value added Certificate status information services or restrict automated access to CRL.

The CA may take reasonable measures to protect and prevent against abuse of the OCSP, Web interface status verification and CRL download services.

3 IDENTIFICATION AND AUTHENTICATION

1.1. Naming

3.1.1 Types of names

Naming and identification rules for physical (private) persons are the same as legal rules applied for naming and identification of physical persons on citizen identity cards, passports or Luxembourg residency cards.

Subject names are either identical to names used within identity documents (in case of registration at a non-PSF RA) or such as to comply with KYC procedures as these procedures are mandatory for PSF companies or institutions (in case of registration at a PSF RA).

Naming and identification rules for professional attributes of physical persons are the same as the legal rules applied to naming and identification of professional attributes in the Grand-Duchy of Luxembourg and of equivalent international professional attributes.

See the applicable CP for more detailed naming rules (in particular for non-physical entities) and for detailed structure of the Certificates subject attributes (section 7.1 of the applicable CP, including X.500 distinguished names and RFC-822 names).

The LuxTrust CSP is only authorised to issue the following names in the CA Certificates it issues:

For the LuxTrust Root CA Certificates:

Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust root CA

For the LuxTrust Normalised CA Certificates (self-signed & issued by the LuxTrust Root CA):

Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust Normalised CA

For the LuxTrust Qualified CA Certificates (self-signed & issued by the LuxTrust Root CA):

Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust Qualified CA

3.1.2 Need for names to be meaningful

Unless pseudonyms are used, the names used under this CPS and the applicable CP shall be meaningful as identifying certificate Subjects (physical persons, optional professional attributes, non-physical entities).

RFC 822 names may not be meaningful.

3.1.3 Anonymity or pseudonymity of subscribers

Unless otherwise specified in the applicable CP, Subscribers, as physical persons, may choose to receive a Certificate certifying their identity as a pseudonym. The Certificate clearly identifies this choice through the mention “Pseudonym:” together with the allocated **pseudonymUniqueIdentifier** in the appropriate subject attributes as specified in section 7.1 of the applicable CP.

Unless chosen by the subscriber or otherwise specified in the applicable CP, the **pseudonymUniqueIdentifier** is uniquely determined at registration by the Local Registration Authority according to the following scheme:

The uniqueIdentifier used in the syntax of the commonName for pseudonym users is deemed to be unique.

In case the Subscriber chooses to receive a Certificate certifying his identity as a pseudonym, the LRAO registering the Subscriber retains full identification of the Subscriber with regards to his/her allocated **pseudonymUniqueIdentifier**.

This information is retained as confidential and shall never be disclosed to third parties unless as foreseen by law (to the notable exception of the *paper*-based registration files that must be communicated to LuxTrust S.A., as ruled by its PSF status).

3.1.4 Rules for interpreting various name forms

RFC-822 names may be used as Alternate Subject Names by indicating the e-mail address of the Certificate Subject.

3.1.5 Uniqueness of names

The full combination of the Subject Attributes (Distinguished name) has to be unique. Specific CP covered by the present CPS may foresee other means to ensure the uniqueness of the full combination of the Subject Attributes (Distinguished name).

3.1.6 Recognition, authentication, and role of trademarks

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 retrieval systems, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission of LuxTrust S.A.

3.2 Initial identity validation

Initial identity validation procedures for PKI Participants or organisation of PKI Participants other than Subscribers, comply with provisions of the present CPS (and in particular with section 5.2.1) and are fully detailed in LuxTrust S.A. internal documents.

Procedures for initial subscriber identity validation are governed by the rules expressed in the following subsections, and detailed in the applicable CP. At expiration of the Certificates, the same procedures as for the initial identity validation (i.e. revalidation) are followed, unless online re-key is authorised and performed under the applicable CP (see section 4.6 to 4.9 of the present CPS and of the applicable CP).

3.2.1 Method to prove possession of private key

Unless otherwise specified in the applicable CP, the key generation process is ensured by the CSP in compliance with the applicable ETSI TS 102 042 [4] or ETSI TS 101 456 [3] technical standard, respectively for Certificates issued under the LTNCA, or the LTQCA. In that case, the private key activation data may be sent to the Certificate Subject by postal mail or delivered to the Certificate Subject according to a physical presentation based procedure, strictly followed by the LRAO registering the Subscriber (Certificate Subject). This procedure is provided by LuxTrust S.A. as an internal and auditable document, and is in line with the applicable CP.

Key generation process ensured by the Subscriber is only allowed for Certificates issued under the LTNCA (discontinued) or LTQCA with LCP policies, and complies with requirements stated in the applicable CP and with the ETSI TS 102 042 technical standard.

3.2.2 Authentication of organisation identity

Rules for identification of the Subscriber’s organisation are compliant with the legal rules applied to naming and identification of organisations in the Grand-Duchy of Luxembourg.

The following documents are required for the identification of Subscriber's organisation (legal person) and/or to validate the relationship of a physical person within a legal person:

1. Recent constitutive act, or recent extract of the commercial register (or the foreign equivalent for foreign companies registered under foreign law;
2. A recent official document or a recent original and certified mandate stating the split of responsibilities or disposition powers within the organs of the legal person (board of directors, delegated administrator, CEO, manager, etc.);
3. When the legal person runs financial sector activities involving third party funds management, the copy of the required authorisation or the mention that such authorisation is not required;
4. A copy of the identity evidence (identity card, passport or Luxembourg residency card) of one of the physical persons who is a legal representative of the legal person; in case this person cannot be physically present at the LRA, the copy must be certified by a competent authority (embassy, consulate, notary, municipality, police office, bank from the first order) and be accompanied by a legalisation of the signature of this authority.
5. The information about their legal address, civil state, and profession;
6. In case a company established in a non-Luxembourg jurisdiction is found as founder or administrator or signatory in the LuxTrust registration process, LuxTrust S.A. reserves right to ask for constitutive documents of this company (points 1 & 2 above), the declaration of the commercial beneficiary and the origin of the funds of the company, as well as an explanatory description of structure of the proposed company.
7. In case the relationship of a physical person within a legal person is to be validated and certified in the Certificate, the person identified in (4) shall sign the appropriate guarantee as provided in the applicable Certificate application form (Purchase Order).

In case of foreign law companies, an additional banking reference can be required and LuxTrust S.A. reserves right to reject the application of such companies.

3.2.3 Authentication of individual identity

For a registration authority, identification is performed through a face-to-face identification following PSF rules set by the CSSF. Face to face registration of an individual Subscriber (or Subject if it differs from the subscriber) for issuance of a certificate, include the following:

- The Subscriber must be present in person in front of a LuxTrust LRAO during registration process, or the Subscriber initial registration process must guarantee that it includes an equivalent face-to-face identification and authentication process whose results are securely[12] transmitted to a LuxTrust LRAO;
- The Subscriber must provide for verification a valid and authentic identity card or identity passport or Luxembourg residency card;
- The LRAO must verify the authenticity and validity of the provided identity proof according to (legal) procedures provided by LuxTrust S.A. and against stolen identity proof lists.

For remote registration, the Subscriber must provide copies of a valid and authentic identity card or identity passport or Luxembourg residency card for verification. Specific requirements may be required by the applicable CP.

Identification and authentication requirements for an individual Subscriber aiming to have its professional attributes certified must provide evidence of the applicability of such professional attributes. When these professional attributes are related to an organisation, the Subscriber must comply with the provision stated in section 3.2.2 of the present CPS.

[12] Transmission shall ensure data origin authentication, data integrity, non-repudiation of signing, and confidentiality.

3.2.4 Non-verified subscriber information

Subscriber's e-mail address of natural persons is non-verified Subscriber information. Subscriber provided Subject serialNumber (for SSL/Object certificates only) is non-verified Subscriber information. The Subscriber is entirely responsible of providing up-to-date, accurate and correct information during registration process.

3.2.5 Validation of authority

Not applicable.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key & update requests

3.3.1 Identification and authentication for routine re-key & update

See sections 4.7 and 4.8.

3.3.2 Identification and authentication for re-key after revocation

The same process as for initial identity validation is used.

3.4 Identification and authentication for revocation request

Identification and authentication procedures for revocation requests related to PKI Participants or organisation of PKI Participants other than Subscribers comply with provisions of the present CPS and are fully detailed in LuxTrust S.A. internal documents, including applicable CP for PKI Participants other than Subscribers.

The whole processes associated to suspension, revocation and un-suspension are detailed in section 4.9.

The Subscriber, and if applicable the legal representative (or his duly appointed delegate) of the company/organisation from which the Subscriber is a member of, the LRA, the CRA or LuxTrust S.A. may apply for suspension or un-suspension following suspension of the Certificate. The Subscriber (or the Subject, when different) is notified by email upon certificate status change.

The CA makes information relating to the status of the suspension or revocation of a Certificate available to all parties at all times, as indicated in Sections 4.9 and 4.10 of the present CPS.

Information and online facilities for the suspension / un-suspension following suspension of the Certificate can be obtained on the LuxTrust website https://suspend.luxtrust.lu respectively on https://activate.luxtrust.lu.

Applications and reports relating to a suspension, un-suspension following suspension are processed on receipt, and are authenticated as described in section 4.9.15, 4.9.16 and 4.9.3 respectively.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

For all PKI Participants within the CA domain, including the Relying Parties, there is a continuous obligation to inform directly or indirectly the CA:

- of all changes in both the information that is certified within a Certificate and in the information that has been used to support the Certificate issuing process, during the operational period of such Certificate, or
- of all any other fact that may affect the validity of a Certificate

The CA shall then take appropriate measures to make sure that the situation is corrected (including revocation of the Certificate if applicable).

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Unless otherwise specified by law, LuxTrust applicable standards, or the applicable CP, any physical person can submit a Certificate application. The CA issues, suspends or revokes Certificates only at authenticated request of the CRA, or LuxTrust S.A. acting as CSP, to the exclusion of any other entity, unless explicitly instructed so by the CSP.

4.1.2 Enrolment process and responsibilities

For provision of services, the CA and LuxTrust S.A. may rely on third party agents under appropriate (sub-) contracting agreements. Towards any party, LuxTrust S.A. acting as CSP assumes full responsibility and accountability for acts or omissions of all third party agents it uses to deliver certification services.

Within the context of new Subscriber registration, the LRA and CRA responsibility is to verify that the Subscriber is indeed the person (s) he claims to be and to validate the information that is requested to be certified by the CA as well as the information supporting this certification. This shall be done in compliance with the rules and practices as stated by the applicable CP, the LuxTrust CPS and by strictly following the LuxTrust registration procedures.

The Subscriber will have to proceed to a valid initial identification and authentication as described in section 3.2. In case the professional quality has to be certified, the Subscriber must also prove his/her professional quality, together with any information supporting his/her registration.

At time of registration, the LRA (and CRA when remote registrations are concerned) guarantees the accuracy of all information contained in the certificate request sent to the Central Registration Authority (to the CA when CRA remotely registered certification requests are concerned). It also guarantees that the certificates Subscriber as well as the certificate Subject (in case the Subject and the Subscriber of the certificate are different entities) have been duly registered and that all required verifications have been performed prior to successful registration leading to Certificate issuance.

Upon successful validation of the Subscriber through face-to-face registration, the LRAO combines and securely archives all the submitted documents and uses the RA Graphical User Interface to send the certificate request (and in case the key generation is done by the CSP, the request for the LuxTrust (S)SCD) to the CRA. The CRA then performs a final validity check, on receipt of the Subscriber's registration information received from the LRAO. In case the request is accepted by the CRA, the CRA requests the (S)SCD Issuing Authority for the generation of the key-pair(s) (only in case the key generation is done by the CSP), and/or Certificate(s) by the Certificate Factory (CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber (via his/her LRAO in case of pseudonym Subscriber) and set out the grounds for this rejection.

Upon successful validation of the Subscriber remote electronic registration, the CRAO combines and securely archives all the submitted documents, performs a final validity check on receipt of the paper-based Subscriber's registration information when applicable. In case the request is accepted by the CRA, the CRA requests the Certificate(s) to the Certificate Factory (CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber and set out the grounds for this rejection.

In case of SSCD delivery (e.g., LuxTrust Smart Card Subscribers), the Certificates are generated in a suspended mode by the LuxTrust CA (Factory). This suspension notification is immediately available via the LuxTrust Revocation Status Services.

4.1.2.1 Subscriber enrolment process

The enrolment process for the Subscriber to submit Certificate application is described in details in the applicable CP. This process shall be compliant with the applicable technical standard ETSI TS 101 456 [3] or ETSI TS 102 042 [4], respectively for Certificates issued by the LTQCA or the LTNCA.

4.1.2.1.1 Registration Preparation

As a general provision, the Subscriber must obtain the Order Form and the General Terms and Conditions for the Certificate (hereafter referred to as "the Order Form" and "the General Terms and Conditions") from LuxTrust S.A. acting as CSP. These, together with the present CP and the LuxTrust Certification Practices Statements (CPS), constitute the Subscriber Agreement between the Subscriber and LuxTrust S.A. (the CSP). The Subscriber may also ask the CSP to send him/her copies of the documents in question by postal mail or to obtain the documents from an LRA approved by the CSP for the applicable CP. The correct versions of these documents are available on: https://repository.luxtrust.lu.

The Subscriber must duly complete and sign the Order Form. The Order Form may falls into two parts:

a. The "Subscriber Part" must be duly completed and signed by the Subscriber.
b. If applicable (optional): The "Subscriber Organisation Part" must be duly filled in and signed by a legal representative (or his/her duly appointed proxy) of the organisation to which the Subscriber belongs.

By signing the Order Form, the Subscriber and, if applicable, the Subscriber's organisation accept the General Terms and Conditions, the CP and the CPS.

4.1.2.1.2 Online Registration Preparation

In order to ease Subscriber registration preparation and to reduce the amount of errors, an end-user web-based registration preparation interface is provided to the Subscriber. This interface presents the Subscriber with a convenient & intelligent electronic form to collect information needed for registration. This form will dynamically present appropriate fields in function of the choices of the Subscriber: type of requested certificate, type of identity (e.g., physical private person or physical person with professional attributes), type of requested Signature Creation Device (e.g., server signing account, or smart card), etc. Once the Subscriber's registration information filled-in, the intelligent form will provide the Subscriber with a printer friendly version of the LuxTrust Subscriber Order Form and will remind him/her the supporting registration documents that the Subscriber must collect and bring to the LRA in order to validate his/her registration.

In addition to, or in replacement of, this registration preparation facility, it is possible for the LuxTrust CSP (through the LuxTrust CRA or RA Network) to organise so-called "Certification Invite Processes". Such processes enable CRA or (L)RA network(s) to perform certification invitation mailings towards pre-established end-users lists and can be used to initiate the certification process of a specific community as LuxTrust end-users.

4.1.2.1.3 Supporting registration documents

The Subscriber applying for LuxTrust Certificate(s) requiring face-to-face registration may present himself, in person, to one of the LRAs authorised under the applicable CP. If physical presence is required, the Subscriber may arrange a meeting with an LRA Officer (LRAO) and go there in person, bringing with him/her the documents required by the applicable CP. Remotely requested certificates do not require face-to-face registration and can be requested online or remotely as specified in the applicable CP.

The next steps in the Subscriber enrolment process will depend on the applicable CP in function of the choice of the Subscriber to apply for a specific certificate type. These next steps cover:

- The identification and authentication of the Subscriber and his request,
- The communication of the request to the CRA, and,
- The communication with the (S)SCD Issuing Authority (if applicable), and
- The communication with the CA for certificate generation, immediate suspension (if applicable), publication (if applicable), certificate, (S)SCD and related activation data delivery (if applicable) to the Subscriber.

If applicable, certificate un-suspension process is also be described.

Archival of registration related information is the final task of the LRAO or CRAO upon completion of Subscriber registration. The LRAO or CRAO must securely store and archive the Subscriber's application related information in an appropriate secure location according to the requirements laid down in relevant sections of the present CPS and the applicable CP. This archiving is done on both paper-based and electronically collected information.

4.1.2.2 Other PKI Participants enrolment process

The enrolment process for PKI Participants other than Subscribers is described within internal LuxTrust documentation.
Related processes are compliant with the NCP+ policy requirements stated in the technical standard ETSI TS 102 042 [4].

4.1.2.2.1 RA enrolment process

When not specified in the following text, "RA" shall collectively designate the CRA, SRA, LRA and their respective Officers, "CRA" shall collectively designate the CRA and its respective Officers, and similarly for "LRA".

LuxTrust RA networks outside the LuxTrust S.A. legal entity are formally (i.e. contractually) bound with LuxTrust S.A. (CSP). Before being officially entitled and operational, all LuxTrust RA Officers are trained and subject to regular audit either done by LuxTrust S.A. or done in the context of a wider scope, e.g., ILNAS accreditation of (Qualified and) Normalised Certification Service Providers.

The RA contractual agreement with LuxTrust S.A. (CSP) implies the RA to fully endorse obligations in terms of:

- Material and human resources adapted to the RA task;
- Confidential and private treatment of data;
- Protection of RA(O) credentials information allowing to be authenticated as RA(O) and access to RA(O) applications;
- Insurance;
- Reporting;
- Working timetable and availability of services;
- Data archiving;
- Audit and controls.

Subsequently, the RA and its Officers (RAOs) will be subject to:

- Pass certification process for being operational;
- Once operational, strictly respect the RA procedures and guidelines provided by LuxTrust S.A;
- And in particular, perform correct identification and authentication of the clients :
    - Scrupulous verification of the customer data, proofs, identity validation
    - Ask correct information to customer
- Take ad-hoc measures regarding logical and physical security of the information and of the software.

To be issued an RAO certification, being either employed by LuxTrust S.A. or by a contracting RA organisation, an RAO candidate must:

- Be part of an organisation that contracted with LuxTrust S.A. (CSP) as RA, SRA or LRA Network;

- Complete the RAO Agreement, attesting to the truth of his or her assertions regarding professional experience and legally commit to adhere to the RAO Obligations and Code of Ethics;
- Attend the preparation training. This is usually a one or two days training covering the RAO knowledge domains:
  - Basic principles in cryptography and PKI systems
  - Related laws and regulations
  - RA software practices
  - RA(O) guidelines and procedures
  - Telecommunication and Internet security basics
- Accept for being selected for audit or controls;
- Continuing education is required to maintain an RAO's certification in good standing.

4.1.2.3 PKI Participants responsibilities related to enrolment process

4.1.2.3.1 Subscribers' responsibilities

By signing the Subscriber Agreement (Order Form), the Subscriber agrees with and accepts the associated General Terms and Conditions, the applicable CP, and the LuxTrust CPS. Specifically, the Subscriber hereby gives his/her acceptance to the following responsibilities related to the enrolment process:

- The information submitted during enrolment process by the Subscriber must be valid, up-to-date, accurate, and complete. Additionally, this information must meet the requirements for the type of Certificate requested, the applicable CP and in particular with the corresponding enrolment (registration) procedures. The Subscriber is responsible for the accuracy of the data provided during enrolment process.
- The Subscriber must agree to the retention - for a period of [10] years from the date of expiry of the last Subscriber Certificate - by the CSP and LRA of all information used for the purposes of registration, for the provision of a (S)SCD or for the suspension or revocation of the Certificate, and, in the event that the CSP ceases its activities, the Subscriber must also consent for this information to be transmitted to third parties under the same terms and conditions as those laid down in this CPS, and in the applicable CP.
- The Subscriber hereby acknowledges the rights, obligations and responsibilities of the CSP, and other PKI Participants. These are set out in the present LuxTrust CPS, in the Order Form and in the General Terms and Conditions relating thereto, and in the applicable CP.

4.1.2.3.2 LRA – CRA responsibilities

When face-to-face registration is required, the LRA and CRA (here after referred to as L/C-RA) are under a contractual obligation to comply scrupulously with the registration procedures described in related LuxTrust internal LRA procedures and the LuxTrust internal CRA procedures.

The L/C-RA guarantees that:

- Subscribers are properly identified and authenticated both with regard to the personal identity of the Subscriber as a natural private person and with regards to any optional information about optional professional status.
- Any application for Certificates submitted to the CA is complete, accurate, valid and duly authorised, in particular for Certificate Subject related information when the Subject and the Subscriber of the requested Certificate are different entities.
- The L/C-RA Officer (L/C-RAO) informs the Subscriber of the terms and conditions for the use of the Certificate. These are set out in the Order Form and the General Terms and Conditions to be signed by the Subscriber (in paper or notarised electronic form).
- The L/C-RAO checks the identity of the Subscriber on the basis of valid identity documents recognised under Grand-Duchy of Luxembourg law. These identity documents must indicate the full name (last name and first names), date and place of birth.

- The L/C-RAO also verifies any optional information relating to the Subscriber's professional status for the purposes of certification, as indicated in Section 7.1 of the applicable CP.
- If the Subscriber is an affiliate of a legal person, the L/C-RAO validates the documentation supplied as proof of the existence of this relationship.
- The L/C-RAO ensures the storage of at least one copy of the information provided by the Subscriber during enrolment process, in particular:
    - A copy of all information used to check the identity of the Subscriber and any references to his/her professional status, including any reference numbers on documentation used for this verification as well as any limitations on its validity.
    - A copy of the contractual agreement signed by the Subscriber, including the latter's agreement to all obligations incumbent on him/her.

  This information is retained by the L/C-RA for a period of ten (10) years from the date of expiry of the last Certificate linked to the Subscriber's registration by the L/C-RA.
- The L/C-RAO ensures compliance with the requirements relating to the processing of personal data and the protection of privacy with respect to the Subscriber enrolment process.
- The L/C-RA ensure the application of clear and appropriate measures with respect to:
    - Physical security of the information provided by the Subscriber during enrolment process and, where appropriate, of the systems concerned;
    - Confidentiality regulations, specifically also those regarding banking secrecy, if applicable;
    - Logical access to any software;
    - L/C-RAOs dealing with Subscriber enrolment process.
- The classification of and responsibility for this data are treated as of crucial importance, i.e.,
    - the data itself (registration data, guidelines and procedures, etc.) in paper form and, where applicable, in electronic form;
    - The software applications used and their configuration;
    - The equipment (hardware, telecommunications tools, etc.) and their configuration;
    - Physical access to the data (buildings, safes, access controls and conditional access to software, etc.).

  The L/C-RA guarantees that these items are managed and stored in such a way as to avoid any repercussions as a result of a loss of confidentiality, integrity as well as availability of this data.

4.1.2.3.3 CA – LuxTrust S.A. acting as CSP responsibilities

Please refer to section 9.6.1 of the present CPS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Unless the Certificate Subscriber has already been identified, by the RA Network, as described in section 3.2 of the present CPS, validation of Certificate requests will require the Certificate Subscriber to present himself to a Local Registration Authority (LRA). The LRA performs the Subscribers identification and authentication and guarantees the accuracy at the time of registration of all information contained in the certificate request as sent to the Central Registration Authority. The LRA also guarantees that the Subscriber of the certificate (as well as the Subject of the Certificate in case these entities are different) has (have) been duly registered and that all required verifications have been performed prior to his successful registration leading to the Certificate issuance.

When remote registration is applicable, the CRA performs the Subscribers identification and authentication and guarantees the accuracy, at the time of registration, of all information contained in the certificate request as sent to the CA, and that the Subscriber of the certificate (as well as the Subject of the Certificate in case these entities are different) has (have) been duly registered and that all required verifications have been performed prior to his successful registration leading to the Certificate issuance.

4.2.2 Approval or rejection of certificate applications

Upon successful validation of the face-to-face Subscriber registration, the LRAO sends the Certificate request to the Central Registration Authority (CRA). The CRA then performs a final technical validity check, on receipt of the Subscriber's registration information as received from the LRAO. In case the request is accepted by the CRA, the CRA requests the (S)SCD Issuing Authority for the creation of the key-pair(s) (only in case the key generation is done by the CSP), and/or Certificate(s) by the Certificate Factory (CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber (via his/her LRAO in case of pseudonym Subscriber) and set out the grounds for this rejection.

Upon successful validation of the remote Subscriber registration, the CRAO performs a final technical validity check on receipt of the paper-based Subscriber's registration information as received from the Subscriber. In case the request is accepted by the CRA, the CRA requests the creation of the Certificate(s) by the Certificate Factory (CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber and set out the grounds for this rejection.

4.2.3 Time to process certificate applications

Not applicable.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Actions performed by the CA during the issuance of the Certificate are described within and ruled by the present LuxTrust CPS, and in the applicable CP.

The CA validates and ensures the uniqueness of each certificate it issues using the certificateSerialNumber field of each certificate. According to the certificate profile described in the applicable CP (section 7.1), the CA may performs additional specific checks and/or validations on the content, format or other specificities of the certificate requests. See the applicable CP for further details.

The CA authenticates the signed certificate requests and only accepts requests sent by the LuxTrust CRA, unless explicitly instructed otherwise by LuxTrust S.A. acting as CSP and as fully documented (e.g., initial registration procedure for PKI Officers as Chief LRAO, etc.).

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

The notification to Subscriber of issuance of Certificate is described in the Subscriber's enrolment process in section 4.1.2.1 of the present CPS and of the applicable CP.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

The Certificate is deemed to be accepted by the Subscriber, as the case may be, on the eighth day after its publication in the LuxTrust CSP Public Repository of Certificates or its first use by the Subscriber, whichever occurs first. In the intervening period, the Subscriber is responsible for ensuring the accuracy of the content of the Certificate. The Subscriber must immediately notify LuxTrust S.A. acting as CSP of any inconsistency the Subscriber has noted between the information in the Subscriber Agreement and the content of the Certificate.

Objections to accepting an issued Certificate are notified via the LRA, or SRA to the CRA in order to request the CA to revoke the Certificate and take the appropriate measures to enable the reissuing of a Certificate. The procedure used for this purpose is described in Section 4.9 of the present CPS. This is the sole recourse available to the Subscriber in the event of non-acceptance on Subscriber's part.

4.4.2 Publication of the Certificate by the CA

Once the Certificate has been issued by the CA, unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Certificate is not published in the LuxTrust Public Repository of Certificates (Directory). This repository is in the public domain and is accessible at all times as stated in Section 2 of the present CPS.

Unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Subscriber does not agree to the publication of the Certificate in the LuxTrust Public Repository of Certificates immediately on creation. The Subscriber is made aware by the CSP that refusal to publish his Certificates may lead to usage difficulties if his counterpart expects to get the Subscriber's Certificates from the certificate publishing services of LuxTrust.

4.4.3 Notification of Certificate issuance by the CA to other entities

If the Subscriber has agreed to the publication of his certificate, the certificate issuance is notified by the CA to other entities through the publication of the Certificate in the LuxTrust Public Repository of Certificates (Directory), available in the public domain and accessible at all times as stated in Section 2 of the present CPS.

4.5 Key pair and certificate usage

The responsibilities relating to the use of keys and Certificates are defined in the next sections.

4.5.1 Subscriber private key and certificate usage

By signing the Subscriber Agreement, the Subscriber gives his/her acceptance to the following responsibilities related to the Subscriber private key and Certificate usage:

- In using the Key Pair, the Subscriber must comply with any limitations indicated in the Certificate, in the applicable CP or in applicable contractual agreements.
- In accordance with the LuxTrust CPS and with the applicable CP, the Subscriber must protect the Private Key and its Activation Data at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. Once the Private and Public key pair has been delivered to the Subscriber, the Subscriber is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Subscriber is the sole user of the Private Key. The Private Key Activation Data (e.g., 5 digit Activation Code, PIN-code or password(s)) used to prevent unauthorised use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without adequate protection. The Subscriber must never leave the Private Key or the Private Key Activation Data unsupervised when it is not locked (e.g., leave it unsupervised in a work station when the PIN code or password has been entered).
- The Subscriber has sole liability for the use of the Private Key. The CA or LuxTrust S.A. acting as CSP is not liable for the use made of the Key Pair belonging to the Subscriber or for any damage resulting from misuse of the Key Pair.
- The Subscriber shall refrain from tampering with a Certificate.
- The Subscriber shall only use Private Key and Certificate for legal and authorised purposes in accordance with the applicable CP, the Subscriber Agreement and the LuxTrust CPS, and as it may be reasonable under the circumstances.
- The Subscriber must ask the CSP to revoke the Certificate as required pursuant to the applicable CP and the LuxTrust CPS, and in particular if:
    - The Private Key of the Subscriber is lost, stolen or potentially compromised; or,

- The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data (e.g. PIN code) has been compromised or for any other reason[13]; and/or,
- The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part)

The Certificate revocation process is then started immediately. The suspension and revocation process and procedures are set out in Section 4.9 of the present CPS, and of the applicable CP.

- The Subscriber must inform the CSP of any changes to data not included in the Certificate but submitted during the enrolment process. The CSP then rectifies the registered data.
- The Subscriber having received a LuxTrust SSCD (e.g., LuxTrust Smart Card) shall ensure the destruction of the SSCD or give his SSCD back to a LuxTrust LRA for destruction once all Certificates on the SSCD are either revoked or expired.
- The LuxTrust Signing Server Account Subscriber accepts that his certified private key shall be destroyed once expired or revoked.

4.5.2 Relying Party public key and Certificate usage

Relying Parties providing services or directly relying on Certificates issued in accordance with the applicable CP and the present CPS must perform the following and assume the responsibility for having performed the following:

- Successfully perform public key operations as a condition of relying on a Certificate.
- Validate a Certificate by using the CA's Certificate Revocation Lists (CRLs) OCSP or web based Certificate status services in accordance with the Certificate path validation procedure (see also section 4.9.6),
- Un-trust a Certificate if it expired, has been suspended or revoked.
- Rely on a Certificate only for appropriate applications (and context) as set forth in the applicable CP, taking into account all the limitations on the use of the Certificate specified in the Certificate, the applicable contractual documents and the applicable CP (in particular in its section 1.4).
- Take all other precautions with regard to the use of the Certificate as set out in the applicable CP or elsewhere, and rely on a Certificate as may be reasonable under the circumstances.
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on a Certificate.

4.6 Certificate renewal

Not applicable

4.7 Certificate re-key

For Certificates having been registered through a remote (online) registration process, Certificate re-key process shall be identical to the original initial certification process.

For face-to-face registered Certificates, the following apply:

Certificate online re-key is authorised under the following conditions:

- Subscriber key generation is done by the CSP;
- The initial Certificate is still valid (not suspended, not revoked and not expired);
- The certified information is still valid;
- The Subscriber electronically signs an electronic certificate on-line re-key contract with the CSP for processing the request.

[13] Loss of the Private Key Activation Data shall lead to the revocation of the concerned Certificates and Certificates re-key can be applied (see section 4.9 and 4.7 respectively).

The CSP shall take care of the re-key process:

- Either on a new physical (S)SCD and of the secure delivery of this new (S)SCD (e.g., LuxTrust Smart Card) and associated Activation Data (via two separate channels);
- Or on a new LuxTrust Signing Server SCD Account and of the secure delivery of the associated LuxTrust Signing Server Account Activation Data and the SCD (Token).

Certificate re-key may also occur once the initial Certificate is expired for reasons (e.g., key compromise) other than the exclusion of the Subscriber from the LuxTrust services. In that case, the same requirements, processing rules and responsibilities apply as for initial certification request.

The only data which can be updated by the subject is (are) the email address(es). Other subject data must contain the same values as the certificate on which the re-key is based on. As a result, the subject serial number or LuxTrust serial number, located within the certificate subject, remains the same. This provides application providers with a technical and "unique" identifier over time.

In case of Certificates (online) re-key on LuxTrust (S)SCD, and when Subscriber key generation is done by the CSP, a new (S)SCD is issued while the revoked or expired (S)SCD or the (S)SCD that contains only revoked Certificates shall be destroyed according to the present CPS. In case of Certificates re-key on LuxTrust Signing Server Account, old keys related to revoked Certificates shall be destroyed according to the present CPS.

In all other cases, Certificate re-key is not allowed.

See applicable CP for possible further details.

4.8 Certificate modification

The Subscriber must immediately inform the CSP Certification Service of any changes to the data on the Certificate, or when the certified data has become inaccurate or has changed in any way. Through the SRA, the Subscriber must ask the CSP to revoke the Certificate. The Certificate revocation process is then started immediately. The suspension and revocation procedures are set out in Section 4.9 of the present CPS.

In case the Subscriber wants to change the certified information, or has requested the revocation of his/her Certificate due to circumstances mentioned in the previous paragraph, and wishes to be issued a new Certificate, the Subscriber shall process to a full Certificate application as following the initial certification process (see section 4.1 of the present CPS).

4.9 Certificate revocation and suspension

The suspension, un-suspension and revocation processes are managed by the Suspension and Revocation Authority (SRA), through the CRA towards the CA who technically suspends or revokes a Certificate. In any case, CRA, LRA and SRA functions shall be functionally separated to ensure segregation of duties.

LRAs shall in any case intervene in the process of un-suspension of Certificates, and in revocation of Subscriber's Certificate(s) when the physical presence of the requestor is demanded. CRAs shall in any case intervene in the process of un-suspension (rehabilitation after suspension) and in revocation of subscriber remotely requested certificates when the physical presence of the certificate status change requestor is not required. These processes can be either:

- On the initiative of the Subscriber itself, or
- On the initiative of a duly authorised person.

It is important to note that CRA may initiate a suspension or revocation process in case of doubt on the *sanity* of an end-user (as well as any other LuxTrust PKI Participant when applicable and as stated in the present CPS). It is an obligation for all entities subject to FSP (PSF)[14] regulation. The CRA is FSP (PSF) and will thus be in possession of specific blacklists. As a consequence, it is an obligation for CRA to initiate suspension and/or revocation whenever necessary.

For the sake of clarity, a Certificate status can be either valid, or suspended or revoked. Suspension is a temporary and reversible state. A Certificate can be un-suspended to become valid again. The revocation process is irreversible. Once revoked, the Certificate cannot be un-revoked.

Upon expiration or revocation of a LuxTrust Certificate, the corresponding private key must be destroyed in accordance with the present CPS. Once all LuxTrust Certificates within a LuxTrust (S)SCD (e.g., Smart Card) are either expired or revoked, this LuxTrust (S)SCD shall be destroyed by the Certificate Subscriber himself or brought back by the Subscriber to a LuxTrust LRA for destroying in accordance with the present CPS.

The Subscriber, and if applicable the legal representative (or his duly appointed delegate) of the Subscriber's organisation, the LRA, the CRA or LuxTrust S.A. may apply for suspension, un-suspension, or revocation of the Certificate. The Subscriber and, where applicable, the legal representative (or his duly appointed delegate) of the Subscriber's organisation is notified of the suspension, un-suspension or revocation of the Certificate.

Additional specific procedures and/or requirements may be described in the applicable CP, however in all cases; the requirements stated in the next sub-sections (4.9.x) shall be implemented as a minimum.

4.9.1 Circumstances for revocation

The Subscriber and, when applicable, the organisation for which the Subscriber (or Subject when Subject and Subscriber are different entities) is certified (as stated in the Certificate), must ask the CSP to revoke the Certificate as required pursuant to the LuxTrust CPS, and in particular if:

- The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
- The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data (e.g. PIN code) has been compromised or for any other reason; or,
- The certified data is not reflecting the certificate request as verified by the Subscriber in the acceptance period following the issuance (see section 4.4.1 of the present CPS); or,
- The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part).

The CRA directly or the LRA and SRA (via the CRA) will request the suspension of a Certificate (or a pair of Certificates, e.g., in case of LuxTrust Smart Card Subscriber) after having received notice by the Subscriber, or when applicable, by the Subscriber's organisation.

In addition to the cases above, the CRA revokes any Certificate that has been suspended for more than a period of 30 days (60 days for initial suspension of LuxTrust Certificates).

4.9.2 Who can request revocation

Revocation can be requested to the CRA by the Subscriber, by the Subscriber's organisation if applicable, by the LRA, by the SRA, and by the CRA under the circumstances and conditions as set forth in the applicable CP and the present CPS.

Under specific circumstances, LuxTrust S.A. acting as CSP may request revocation to the CRA of any Certificate in accordance with the present CPS. E.g. specific circumstances may be that a LuxTrust Certificate Subscriber appears in a Blacklist as defined by and in accordance with the PSF rules.

[14] Financial Sector Professional – Professionnel du Secteur Financier

The CA revokes a Certificate immediately only upon revocation request coming from the CRA and having been approved by the CRA.

4.9.3 Procedure for revocation request

The form and/or procedure to be used for applying for the (suspension, un-suspension or) revocation of a Certificate can be obtained from the LuxTrust SRA webpage available at the following URL: https://sra.luxtrust.lu.

Applications and reports relating to a revocation are processed on receipt, and are authenticated and confirmed in the following manner:

4.9.3.1.1 Revocation of an existing LuxTrust Subscriber: process overview

The revocation of a certificate may be requested using one of the following possibilities:

a) If the requestor is still in possession of the certificate (and the related private key) to revoke and if that certificate is still valid, the requestor can revoke the certificate 24/7 over the LuxTrust website under https://revoke.luxtrust.lu. The requestor must authenticate to the online revocation service using the certificate that is to be revoked. Additionally, the requestor must provide a valid revocation challenge (located on his LuxTrust Codes document) and sign the request with the certificate. Upon successful completion of the process, the revocation is executed immediately.

b) Contact the LuxTrust SRA hotline: The revocation requestor contacts LuxTrust SRA to revoke a Certificate. When the SRA 24/7 Hotline receives the request, it will register the details and authenticate the revocation requestor through the various personal data.
   - If the personal secret information (personal data, question/answer, product ordering information, …) are correct, the SRA Hotline will revoke the Certificate.
   - If the personal secret information (personal data, question/answer, product ordering information, …) are not correct, the SRA performs no change on the validity status of the Certificate.

c) Go to an RA (or CRA or LRA): The revocation requestor may present himself physical to the RA (or CRA, or LRA) with and request a Certificate revocation. When the RA (or CRA, or LRA) receives the request, it will register the details of the revocation requestor and authenticate the requestor through identity documents. The revocation requestor will need to fill a revocation request form and sign it. The requestor may also download this request form from the LuxTrust website https://sra.luxtrust.lu.
   - If the revocation requestor can be properly identified and the revocation request form is properly filled out and signed, the RA will revoke the Certificate.
   - If the revocation requestor cannot be properly identified or the revocation request form is not properly filled out or signed, the RA performs no change on the validity status of the Certificate.

d) For professional products, LuxTrust offers the option to order a PRO certificate with the subject title “Professional administrator”. This type of product allows the product owner to manage (revoke or suspend) any professional certificate issued to the same company or institution. In order to have a third person’s certificate revoked, the holder of a “Professional administrator” certificate has to provide LuxTrust with a digitally signed document (e-mail, MS-Word, ...), within which he indicates the references of the certificate to be suspended or revoked. LuxTrust will validate the request through the following:
   - If requestors signature is valid;
   - If the requestor does have the “Professional administrator” status;
   - If the company or institution indicated in the requestors certificate does match the company or institution indicated in the certificate to be revoked.

Upon successful validation, the revocation request(s) is(are) executed.

Note : Un-suspension and suspension cases are detailed respectively in section 4.9.16 and 4.9.15 of the present CPS).

In case of face-to-face registered certificates, if the revocation requestor:

- Is not the Certificate Subscriber or Subject (e.g., employer of the Subscriber, another company legal representative for a dismissed CEO, etc.) and
- Does not know the Subscriber's secret information (suspension/revocation password, challenge questions, …) and
- Does not possess a valid LuxTrust signature Certificate certifying its power of representation versus the Subscriber Certificate to be revoked (in which case he can electronically sign an appropriate web-based form)

The revocation requestor must physically present himself to a LRA to proceed to the authentication of his request.

The revocation of a Certificate is definitive.

Note: For a revocation request, if the revocation requestor is requested to physically present himself to a LRA, any LRA approved by LuxTrust CSP may be used (according to the applicable CP), however,

- *For pseudonym subscribers*: Unless the pseudonym Subscriber proceeds through online revocation, the revocation requestor must present himself to the original LRA where the Subscriber initially performed the registration. Only this LRA is able to link the physical person identity with the certified pseudonym.
- In case the selected LRA is not part of the same LRA network as the initial LRA and/or this LRA network do not allow affiliated LRAs to access to a digitalised version of the end-user registration file, the revocation requestor shall be required to perform a full validation of his request using a process that is similar to the initial enrolment (registration) process to provide all the required proofs.

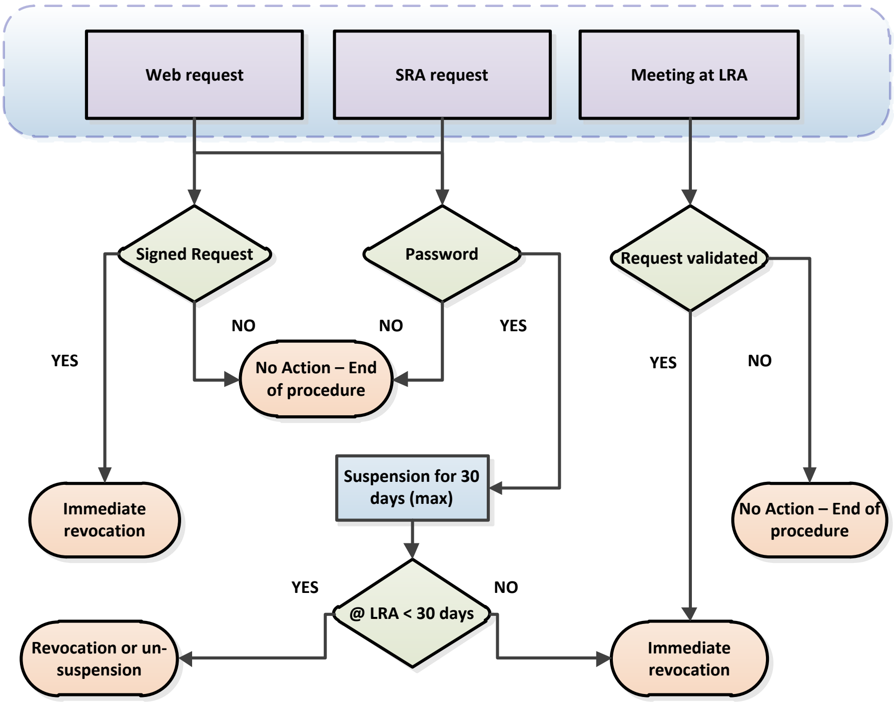

Figure 5 - Revocation for face to face registered certificates

The Figure 5summarises the process flow related to the revocation of a face-to-face registered Certificate. The Figure 6 summarises the process flow related to the revocation of a remotely registered Certificate.

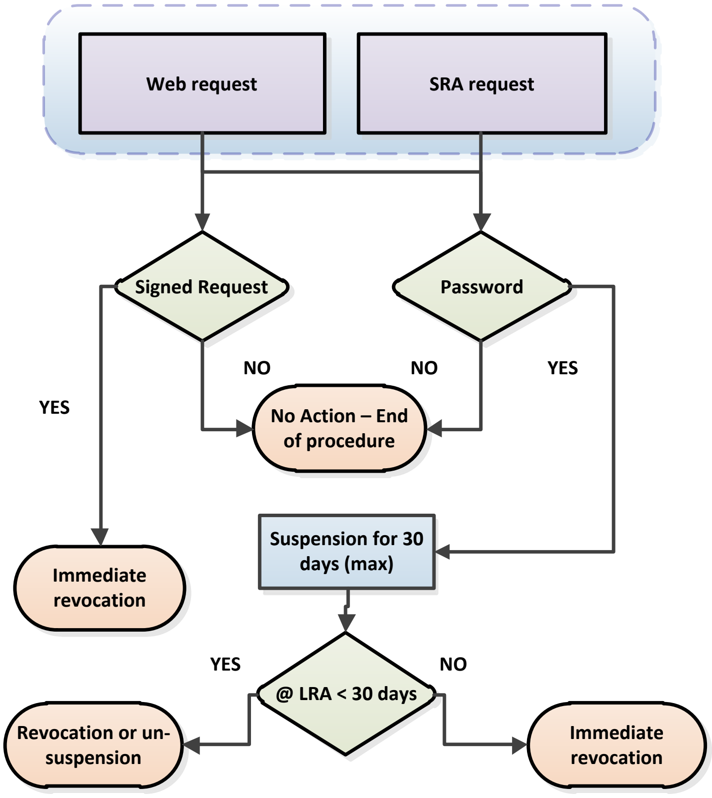

Figure 6 - Revocation process overview for remotely registered certificates

4.9.4 Revocation request grace period

LuxTrust S.A. acting as CSP performs revocation on a best effort basis, to ensure that the time needed to process the revocation request and to publish the revocation notification (updated CRL) is be as reduced as possible and does not exceed 24 hours.

4.9.5 Time within which CA must process the revocation request

While an LRA opening hours are limited, the SRA Hotline and web-based interface are available for at least as prompt as possible suspension (prior revocation) requests 24 hours a day, 7 days a week. Upon authentication and validation of the request, the SRA Hotline requests revocations or suspensions via the CRA towards the CA.

In case suspension is requested as a prior step towards revocation, the SRA informs the CRA who will contact the Subscriber (or its LRAO in case of pseudonym Subscriber) to invite him to present himself at a LRA in order to proceed to the revocation of the suspended Certificate.

4.9.6 Revocation checking requirement for Relying Parties

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.

4.9.7 CRL issuance frequency / OCSP response validity period

4.9.7.1.1 CRLs

A CRL is issued every four hours and thirty minutes (04.30h), at an agreed time. CRLs are signed and time-marked by the CA response (see section 7.2 of the present document).

Every CRL is stored, archived and is available for retrieval for 10 years upon request. Recovery of CRLs older than 12 months may be subject to retrieval and administration fees as stated in section 9.1 of the present CPS.

4.9.7.1.2 OCSP

OCSP service is available for certificate status validation. The fields "this update" and "next update" reflect the validity period of an OCSP (see section 7.3 of the present document). Information regarding requests and responses is retained for a period of 10 years.

4.9.8 Maximum latency for CRLs

Not applicable.

4.9.9 On-line revocation/status checking availability

The CA makes available Certificate status checking services including CRLs, OCSP and appropriate web interfaces.
While the primary objective of the CA is to provide access to its public repositories free of charge, LuxTrust S.A. reserves the right to charge for publication services such as the publication of Certificate status information (e.g., high volume/bandwidth connections, third party databases, private directories, etc.) and/or to restrict access to value added Certificate status information services or restrict automated access to CRLs.

The CA makes available Certificate status checking services including CRLs, OCSP and appropriate web interfaces.

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

Certificate revocation status services are available 24 hours per day, 7 days per week. Outside system maintenance windows, system failure or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that the uptime of these services exceeds 99,0%.

4.9.10 On-line revocation checking requirements

See section 4.9.6 of the present document.

4.9.11 Other forms of revocation advertisements available

Alternative, out-of-band, revocation advertisements available for the advertising of revocation, especially in case of revocation of the CA Signature Certificate are stipulated in the LuxTrust CPS (see section 5.7.3 of the present document).

4.9.12 Special requirements regarding key compromise

Not applicable.

4.9.13 Circumstances for suspension

In case of LuxTrust (S)SCD Subscribers, that is Subscribers for which LuxTrust S.A. is providing the (S)SCD and is performing the key generation for the Subscribers, Certificates are generated in a suspended mode by the CA. This suspension notification is immediately available via the LuxTrust revocation status services. In order to collect his/her (S)SCD and to un-suspend his/her Certificates the LuxTrust Subscriber may be requested to present himself (herself) to the LRA where his/her identity will be checked prior to (S)SCD delivery and activation of Certificates. If the (S)SCD is sent to the Certificate Subscriber by postal mail, or in case of LuxTrust Signing Server Account users, the activation and testing of the Certificates can be performed online through https://cmt.luxtrust.lu. Initial suspension has a maximum duration of 60 days. In case no un-suspension occurs within this period, the initially suspended Certificate(s) are revoked automatically. Un-suspension procedure is described in section 4.9.16 of the present CPS.

Otherwise, circumstances for suspension are limited to the occurring suspicion of any event that may lead to a revocation, such as specified in section 4.9.1 of the present CPS.

4.9.14 Who can request suspension

Persons or entities who can request suspension are limited to the persons or entities who can request a revocation, as specified under section 4.9.2 of the present CPS.

4.9.15 Procedure for suspension and un-suspension requests

The form and/or procedure to be used for applying for the suspension of a Certificate can be obtained from the LuxTrust SRA web pages available at: https://sra.luxtrust.lu.

Two types of suspensions are to be considered within LuxTrust;

- The initial suspension that is always performed by LuxTrust S.A. for the LuxTrust (S)SCD associated certificates, (certificates are kept suspended until hand-over of the (S)SCD to the Subscriber).
- Requested suspension by an authorised party (see also section 4.9.14).

4.9.15.1.1 Initial Suspension of LuxTrust (S)SCD Certificates

The initial suspension leads to a **60 days** suspension period at a maximum. Two cases are possible:

a. The SSCD Subscriber activates his Certificates before the end of the 60 days period, and then the Certificates are un-suspended.
b. If the Subscriber does not activate his Certificates before the end of the 60 days period, the Certificates are automatically revoked.

4.9.15.1.2 Suspension of an existing LuxTrust Certificate: process overview

A requested suspension leads to a **30 days** suspension period at a maximum.

The suspension requestor has two means to initiate the procedure:

a) **Contact the SRA Hotline:**
The suspension requestor contacts the SRA as indicated on https://sra.luxtrust.lu with the request to suspend a Certificate. When the SRA 24/7 Hotline receives the request, it will register the details of the suspension requestor and will validate his identity through his suspension/revocation password (Challenge).

- If the password (Challenge) is correct, the SRA Hotline will suspend the Certificate for a maximum period of 30 days, and inform the LuxTrust CRA of the event.
- If password (Challenge) is incorrect, the SRA performs no change on the validity status of the Certificate but raises an “alarm” towards the CRA.

b) **SRA Website based procedure:**
The suspension requestor proceeds via web-site:

- The suspension requestor electronically signs a suspension form-based request. If the signature is validated, the certificate is promptly suspended for a period of 30 days and the SRA will inform the LuxTrust CRA of the event.
- The suspension requestor does not electronically sign his request, but provides a correct Suspension/Revocation Password (Challenge), then the certificate is promptly suspended by the SRA for a period of 30 days maximum and the SRA will inform the LuxTrust CRA of the event.

- If the password (Challenge) or the electronic signature is incorrect or cannot be validated, the SRA performs no change on the validity status of the Certificate but raises an "alarm" towards the CRA.

For both a) and b) cases, LuxTrust CRA may inform the suspension requestor and the Subscriber that within the 30 days suspension period the Certificate can either be un-suspended or revoked before automatic revocation at expiration of the 30 days period. For this purpose the requestor or the Subscriber must either send a un-suspension or revocation confirmation to the CRA (in case of remotely registered Certificate), or go to an LRA and proceed to a full validation of the request (for face-to-face registered Certificate):

- When no valid un-suspension is performed within the 30 days suspension period, the Certificate is automatically revoked.

- When an authorised requestor presents himself at a LRA or when a valid un-suspension / revocation confirmation is sent to the CRA, before the end of the 30 days suspension period:
  (a) If the authorised requestor requests the un-suspension (respectively the revocation) of the Certificate, then, once the authorised requestor and his/her request are authenticated and validated, the un-suspension (respectively revocation) request is sent to the CA through/by the CRA
  (b) If the claimed authorised requestor is not correctly authenticated at the LRA, the LRA/CRA, no change on the validity status of the Certificate is done but an "alarm" is raised towards/by the CRA.

When the suspension requestor is or is not the Certificate Subscriber or Subject (e.g., employer of the Subscriber, another company legal representative for a dismissed CEO, etc.) and does not know the Subscriber's Suspension/Revocation Password and does not possess a valid LuxTrust signature Certificate certifying its power of representation versus the Subscriber or Subject Certificate to be revoked (in which case he can electronically sign an appropriate web-based form):

- Face-to-face registered Certificates: the suspension requestor must present himself to an LRA to proceed to the authentication of his request,
- Remotely registered Certificates: the suspension requestor must mail by post to the CRA the same documents and authentication proofs as for the initial registration (see applicable CP).

4.9.15.1.3 Un-suspension of a suspended existing face-to-face registered Certificate: process overview

1. The un-suspension requestor may present him(her)-self to an LRA to proceed to confirmation of his/her un-suspension request (i.e., within 30 days from a suspension or a revocation request, or within 60 days from (S)SCD associated Certificate creation). Assuming that the concerned Certificate is not a pseudonym Certificate, the requestor may choose any LRA approved by LuxTrust CSP, otherwise the requestor must go to the LRA that has proceeded to the initial registration. For both pseudonym and non-pseudonym Certificates, un-suspension may also occur through the Website based procedure.
2. The LRAO fully identifies and authenticates the requestor and fully validates the un-suspension request (as for initial registration).
3. Once the request is validated and if the requestor confirms at LRAO that (s)he wants to un-suspend the certificate, the LRAO sends the un-suspension validated request to the CRA (using LRA software).
4. The CRA then transmits the un-suspension request to the CA for immediate treatment.

4.9.15.1.4 Un-suspension of an existing remotely registered subscriber certificate: process overview

1. The un-suspension requestor must proceed to confirmation of his/her un-suspension request (i.e., within 30 days from a suspension or a revocation request).
2. The CRAO fully identifies and authenticates the requestor and fully validates the un-suspension request (as for initial registration).
3. Once the request is validated and if the requestor confirms that (s)he wants to un-suspend the Certificate, CRA then transmits the un-suspension request to the CA for prompt treatment.

To un-suspend his/her remotely registered certificate after previous suspension, the un-suspension requestor must provide the CRA Officer with an un-suspension request confirmation. This confirmation consists in:

- If the requestor is the Subscriber or an Administrator or Legal representative of the organisation or company having subscribed for the certificate, a signed copy recto-verso of the requestor identity card or passport or Luxembourg residency card is sufficient since the CRA is able to establish the authenticity of the request and in particular the non-ambiguous link between the requestor and the organisation or company thanks to the registration file, provided it corresponds to the persons authenticated in the initial registration file.

- If the requestor is not the Subscriber nor an Administrator or Legal representative of the organisation or company owning the certificate, a full validation of his request using a process that is similar to the initial enrolment (registration) process to provide all the required proofs; all the document required for the registration process (see applicable CP in Annex I.3) are required in order to enable the CRA to establish the non-ambiguous link between the requestor and the organisation or company

This confirmation can be sent per fax and/or per postal mail to the LuxTrust CRA. When no valid un-suspension is performed within the 30 days, the Certificate is automatically revoked.

When the un-suspension requestor is or is not the Certificate Subscriber or Subject (e.g., employer of the Subscriber, another company legal representative for a dismissed CEO, etc.) and does not know the Subscriber's Suspension/Revocation Password and does not possess a valid LuxTrust signature Certificate certifying its power of representation versus the Subscriber or Subject Certificate to be un-suspended (in which case he can electronically sign an appropriate web-based form), the un-suspension requestor must present himself to a LRA to proceed to the authentication of his request or the un-suspension requestor must mail by post to the CRA the same documents and authentication proofs as for the initial registration (see applicable CP).

4.9.16 Limits on suspension period

In case of (S)SCD Subscribers, the Certificates are generated in a suspended mode by the LuxTrust CA (Factory). This initial suspension is set for a maximum period of 60 days; afterwards if not correctly un-suspended the Certificates are revoked.

When otherwise than initially suspended, the Certificate is suspended for a maximum period of 30 days. After this period, unless the Certificate has been validly requested to be un-suspended, the Certificate is automatically revoked.

4.10 Certificate status services

4.10.1 Operational characteristics

See section 4.9.7 of the present document.

4.10.2 Service availability

See section 4.9.9 of the present document.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

Subscription termination is subject to appropriate clause within the Subscriber Agreement (e.g., in the General Terms and Conditions). End of subscription is materialised by the expiration or the revocation of the Certificate while the other Certification services are still available to the Subscriber as it is for any Relying Party.

4.12 Key escrow and recovery

Subscriber's key back-up, escrow and key recovery are not allowed except for the sole purpose of and in the context of LuxTrust Signing Server Account disaster recovery as stated and ruled by the present CPS.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, operational, procedural, personnel and physical (non-technical security) controls that are used by LuxTrust S.A. with regards to its Certification Authorities (CAs), Time Stamping Authorities (TSAs), and the other PKI Participants other than Subscribers and Relying Parties to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, Time Stamp Tokens (TSTs) issuance, auditing and archiving are compliant with the following technical standards:

- ETSI TS 102 023 “Policy requirements for time-stamping authorities” [6] for LuxTrust Time Stamping Services,
- ETSI TS 102 042 “Policy requirements for certification authorities issuing public key certificates” [4],
- ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates” [3].

These controls are further described and ruled by the next sub-sections.

LuxTrust S.A. carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is available as an internal document at LuxTrust S.A..

LuxTrust S.A., acting as CSP including activities and provision of Time Stamping Services[15], provides direction on information security through its CSP Board, responsible for defining the CSP’s information security policy and ensuring publication and communication of the policy to all personnel who are impacted by the policy.

This information security policy is implemented with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. Appropriate systems, infrastructures and measures for quality and information security management are implemented and maintained at all times. Any changes that would impact on the level of security provided must be approved by LuxTrust S.A. through its LuxTrust CSP Board. The LuxTrust information security policy as well as documentation on security controls and operating procedures are available as separate and internal documents at LuxTrust S.A..

LuxTrust S.A., acting as CSP, ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose LuxTrust S.A. maintains an inventory of all information assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

LuxTrust information security management is guided by and compliant with ISO /IEC 17799. [16]

5.1 Physical controls

LuxTrust S.A. acting as CSP implements and ensures implementation of physical security controls on all sites and premises, either own, leased or rented, that are used to support its certification and time stamping services. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities, and to avoid compromise or theft of information and information processing facilities.

[15] The LuxTrust Time Stamping Services (TSS) consists of the management of the infrastructure for, and the provisioning of Time Stamp Tokens. These services are provided by LuxTrust S.A. acting as LuxTrust Time Stamping Services Provider (TSSP) to the Subscribers and are an integral part of the LuxTrust PKI and in the context of the broad definition of CSP as given by the European Directive on electronic signatures [1]. Hereafter the term CSP includes the activities of TSSP.

[16] ISO 17799 is often used as a generic term to describe what actually two different documents are: ISO17799 (aka ISO 27002), which is a set of security controls (a code of practice), and ISO 27001 (formerly BS7799-2), which is a standard 'specification' for an Information Security Management System (ISMS).

Detailed descriptions of the secure sites and premises that are used by LuxTrust S.A. to provide certification and time stamping services, as well as Access Control Security Policies are available in LuxTrust S.A. internal documents.

5.1.1 Site location and construction

Several secure premises are used according to the type of component service that is used as part of the provision of LuxTrust certification and time stamping services. All these premises are protected through numbered zones and locked rooms, cages, safes, and cabinets. The following types of secure sites are identified:

- **Highly secure areas for high-security operations**: These highly secure areas are used to operate software/hardware used by component services like Certificate Generation Services (CA Factory), Dissemination (Publication) and Repository Services, (S)SCD Provisioning Services, Certificate Revocation Status Services, Time-Stamping Services.

- **Highly secure areas for disaster recovery of critical services**: These highly secure areas are equipped and maintained in order to ensure disaster recovery of the LuxTrust PKI and certification services according to section 5.7 of the present CPS.

- **Highly secure areas for LuxTrust PKI Central Operations Management**: In these highly secure areas resides the operations management of the Central Registration Services (CRA(O)), Suspension & Revocation Services (SRA(O)).

- **Secure areas for Local Registration Authorities**: LRA(O)s operate in areas equipped to meet the requirements laid down in section 4.1.2.3 of the present CPS and benefit from appropriate physical security measures.

5.1.2 Physical access

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CSP operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token, and biometric readers and access control lists.

The secure areas on LuxTrust secure sites and premises are regularly inspected to verify that access control systems are always operational and running. Intrusion detection, monitoring and logging systems shall also be implemented in all sites for all secure areas.

Highly secure areas on LuxTrust sites and premises are protected against unauthorised access by at least three (3) perimeters protections, allowing access for only one person at a time and/or under dual control. Other secure areas shall be protected against unauthorised access by at least two (2) perimeters protections.

Strict access control is enforced to all secure areas. Access to the secure areas is limited to authorised personnel listed on an access list, which is subject to audit and control.

5.1.3 Power and air conditioning

Power and air conditioning operate with a high degree of redundancy in highly secure areas.

5.1.4 Water exposures

Secure areas are protected from any water exposures.

5.1.5 Fire prevention and protection

Secure areas benefit from appropriate prevention and protection measures against fire exposures.

5.1.6 Media storage

Media are stored securely. Backup media are securely stored in a separate location from the original media location. All media storage areas are protected from fire and water exposure and damages.

5.1.7 Waste disposal

Waste disposal is securely implemented in order to prevent unauthorised disclosure of sensitive data. Cleaning operations, as well as other types of operations not directly linked to the certification or time stamping (component) services operations, shall be strictly monitored and implemented in order to prevent unauthorised actions and/or disclosure of sensitive data.

5.1.8 Off-site backup

Backup media are securely stored in a separate location from the original media location and are protected against fire and water exposure. LuxTrust S.A., acting as CSP, implements the necessary measures to ensure a full and automatic recovery of its services in case of a disaster, corrupted servers, software or data. Backup and Disaster recovery sites are located in separate premises sufficiently distant from the primary locations and benefit from equivalent security measures. See section 5.7 of the present CPS for further details on recovery procedures.

5.2 Procedural controls

The CSP for both CA and TSA activities ensures that CA/TSA systems are secure and correctly operated with minimal risk of failure in strict compliance with technical standards ETSI TS 102 023 [6], 102 042 [4], and 101 456 [3] when this latter document imposes higher requirements, and in particular for operations management, system access management, trustworthy systems deployment and maintenance, business continuity management and incident handling.

5.2.1 Trusted Roles

All members of the personnel staff that involved for the provision of the LuxTrust certification and time stamping services are either employees of LuxTrust S.A. or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services.

All members are subject to personnel and management practices that LuxTrust S.A. follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and time stamping related technologies.

LuxTrust S.A. acting as CSP obtains a signed statement from each member of the staff on not having conflicting interests with the CSP, maintaining confidentiality and protecting personal data.

All members of the staff operating certificate and or TST generation services, key management operations (including (S)SCD devices provisioning), acting as officers of either Local Registration Authorities, Central Registration Authorities, Suspension/Revocation Authorities, security officers, system operators, system administrators, quality control manager and system auditors or any other operations that materially affect such operations, and members of the LuxTrust CSP Board are considered as serving in a trusted position.

LuxTrust S.A. acting as CSP ensures that:

- All tasks, roles and responsibilities with respect to the LuxTrust certification and time stamping services are:
    - Described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and

employee training and awareness, and differentiating between general functions and CA specific functions.

- Allocated to the system of the CSP and/or to the member of the staff according to its trusted role.

- All actions with respect to the LuxTrust certification and time stamping services can be attributed to the system of the CSP and/or to the member of the staff that has performed the action.

- Personnel shall exercise administrative and management procedures and processes that are in line with the LuxTrust information security management procedures (see introduction of section 5 of the present CPS).

- Trusted or management roles are formally appointed to trusted roles by senior management responsible for security and are not appointed to any person who is known to have a conviction for a serious crime or other offense which affects his/her suitability for the position and/or until necessary checks are completed.

- Appointment to trusted roles is such that the possibility of fraud is minimised.

- Managerial personnel possess expertise in the electronic signature, time stamping technology, mechanisms for calibration or synchronisation the TSU clocks with UTC, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities.

- CA personnel are formally appointed to trusted roles by senior management responsible for security.

5.2.2 Number of persons required per task

Where dual control is required at least two trusted staff members need their respective and split knowledge in order to be able to proceed with the on-going operation.

For tasks related to critical CA or TSA functions such as but not limited to key management and in particular CA or TSA key generation, more than two persons are required (see section 6) for extended security and control reasons.

5.2.3 Identification and authentication for each role

Each member of the personnel staff are issued a LuxTrust credential (e.g., a LuxTrust Smart Card with LuxTrust NCP+ certificates as a minimum) in order to ensure proper identification and authentication prior being allowed to perform any trusted action.

As stated in section 5.2.1, LuxTrust S.A. acting as CSP ensures that all actions with respect to the LuxTrust certifications services can be attributed to the system of the CSP and/or to the member of the staff that has performed the action.

5.2.4 Roles requiring separation of duties

All audit and/or control roles are performed with regards to the separation of duties versus the audited and/or controlled role.

Personnel exercising tasks, roles and responsibilities with regards to the provisioning of Signing Server services are independent, different and separated from the personnel exercising tasks, roles and responsibilities with regards to the provisioning of Signing Server Authentication services. See section 1.3.5.2 of the present CPS.

5.3 Personnel controls

Personnel security controls are documented in a policy and include the topics covered by the next sub-sections.

5.3.1 Qualifications, experience, and clearance requirements

Managerial personnel possess expertise and training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

LuxTrust S.A. ensures that all members of the personnel staff that are involved for the provision of the LuxTrust certification and time stamping services whether employees of LuxTrust S.A. or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services are checked regarding qualifications, expert knowledge, experiences and clearance needed and as appropriate to fill trusted roles and to perform the related specific job function. Such checks are specifically directed towards:

- Misrepresentations by the candidate;
- Appropriateness of validated references;
- Any clearance as deemed appropriate.

5.3.2 Background check procedures

LuxTrust S.A. acting as CSP makes or ensures that the relevant checks are performed to prospective personnel by means of status reports issued by a competent authority, third-party statements or signed self-declarations.

5.3.3 Training requirements

LuxTrust S.A. acting as CSP makes or ensures that the relevant trainings are provided to members of the LuxTrust personnel staff to carry out their specific job functions related to the provision of the LuxTrust certification and/or time stamping (component) services.

5.3.4 Re-training frequency and requirements

After completion of initial training, periodic (at least yearly) training updates are performed to all categories of members of LuxTrust personnel staff to establish continuity and updates in the knowledge of the personnel and in procedures.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanction for unauthorised actions

LuxTrust S.A. acting as CSP sanctions or ensures that relevant sanctions are provided to members of the LuxTrust personnel staff for policies or procedures violations, unauthorised actions, unauthorised use of authority and unauthorised use of systems for the purpose of imposing accountability on the CSP personnel, as it may be appropriate under the circumstances. This may include among others revocation of privileges, administrative discipline and/or criminal pursuit.

5.3.7 Independent contractor requirements

Independent LuxTrust S.A. subcontractors and their personnel are subject to the same background checks as the CSP personnel.

5.3.7.1.1 Additional requirements on LuxTrust S.A. sub-contractors

Selected LuxTrust S.A. sub-contractors for provision of some LuxTrust certification and time stamping component services are grouped in a consortium under a designated Primary Contractor that is the main responsible and contracting party towards LuxTrust S.A. The Primary Contractor is then sub-contracting other companies for the provision of services that are not provided by the Primary Contractor. These sub-contracts have been communicated to LuxTrust S.A. and there should not be more than one subcontractor per component service.

The Primary Contractor provides the legal structure of all its sub-contractors and the description of the involved teams and skills of each team member.

The Primary Contractor and the subcontractors must provide proof of their PSF status (PSF: Professionnel du Secteur Financier – Financial Sector Professional as defined by the Grand-Duchy of Luxembourg Law).

The Primary Contractor of the LuxTrust outsourced services and LuxTrust S.A. are "PSF – Agent administratif". Since the Validation Services are to be provided by the CA Factory Services Provider for security reasons, the CA Factory Services Provider implicitly have the "PSF – Agent administratif" status as well.

5.3.8 Documentation supplied to personnel

LuxTrust S.A. acting as CSP makes the relevant documentation or ensures that the relevant documentation are provided to members of the LuxTrust personnel staff to carry out their specific job functions related to the provision of the LuxTrust certification and/or time stamping (component) services. Documentation distribution shall occur during initial training, re-training and whenever otherwise appropriate.

5.4 Audit logging procedures

5.4.1 Type of events recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. LuxTrust S.A. acting as CSP implements or ensures the following controls being implemented:

- All events relating to the life-cycle of CA and TSA keys are recorded;
- The LuxTrust CAs and TSAs event logging systems record events related to certificate or TST lifecycle operations including but not limited to:
    - Subject key generation;
    - Preparation of (S)SCDs;
    - Issuance of a certificate;
    - Revocation of a certificate;
    - Suspension of a certificate;
    - Automatic revocation;
    - Publishing of a CRL;
    - Request for TST;
    - TST generation.
- All other LuxTrust certification or time stamping component services are equipped with event logging systems that record events related to any operation performed on behalf of the component services. Note for the LRA component service, this include but is not limited to registration information including but not limited to certificate application information provided by Subscribers.
- LuxTrust S.A. acting as CSP audits all event-logging records. Audit trail records contain:
    - The identification of the operation;
    - The date and time of the operation;
    - The identification of the Certificate or TST, involved in the operation;
    - The identity of the transaction requestor.
- In addition, LuxTrust S.A. acting as CSP maintains or ensures maintenance of internal logs and audit trails of relevant operational events in the whole infrastructure whatever the component service, including, but not limited to:
    - Start and stop of servers;
    - Outages and major problems;
    - Physical access of personnel and other persons to sensitive parts of any secure site or area;
    - Back-up and restore;
    - Report of disaster recovery tests;
    - Audit inspections;

- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Other documents that are required for audits include:

- Infrastructure plans and descriptions;
- Physical site plans (including but not limited to secure areas) and descriptions;
- Configuration of hardware and software;
- Personnel access control lists.

LuxTrust S.A. acting as CSP ensures that the precise time all events, records and documents listed above are recorded. The precise time of significant CA environmental, key management and certificate management events are supported by LuxTrust S.A. Time-Stamping services.

LuxTrust S.A. acting as CSP ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events. Log files and audit trails are archived for inspection by the authorised personnel of LuxTrust S.A., of the CA Factory services provider, of the LRAs and designated auditors as described in internal documents.

Auditing events are not given log notice.

5.4.2 Frequency of processing log

Audit logs are processed continuously and/or following any alarm or anomalous event. Audit logs are archived continuously.

5.4.3 Retention period for audit log

Audit log are kept for a minimum of 10 years.

5.4.4 Protection of audit log

The log files are properly protected by an access control mechanism. Only authorised auditors can have access to audit logs. Appropriate protection against modification and deletion of the audit logs is implemented such that no one may modify or delete audit records except for transfer to long term media for archiving purposes.

5.4.5 Audit log backup procedures

Log files and audit trails are backed up according to internal procedures.

5.4.6 Audit collection system (internal vs. external)

Audit systems are an integral part of the CA respectively of the LuxTrust registration platform.

5.4.7 Notification to event-causing subject

If required, LuxTrust notifies the originator of the audit event.

5.4.8 Vulnerability assessment

Vulnerability assessment related to the audit log systems is part of the risk analysis carried out by LuxTrust S.A. and available as a separate internal and confidential document.

5.5 Records Archival

5.5.1 Type of records archived

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 present 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;
- All TST's will be archived for duration of 10 years, starting from the time mentioned in the TST. Archive retention period of TSA events journal is 10 years
- The very last back up of a TSA archive for 10 years following the issuance of the last TST by this TSA.

LuxTrust S.A. acting as CSP keeps archives or ensures that archives are kept in a retrievable format.
Archives are accessible to the authorised personnel of LuxTrust S.A., of the CA Factory services provider, of the LRAs and designated auditors as described in internal documents.

5.5.2 Retention period for archive

See section 5.5.1.

5.5.3 Protection of archive

LuxTrust S.A. acting as CSP ensures:

- implementation of proper copy mechanisms to prevent data loss or data access loss over time and,
- that the confidentiality and integrity of the archive and its physical storage media is maintained during its retention period, and
- that records concerning certificates are completely and confidentially archived in accordance with the present CPS.

Archives are accessible to the authorised personnel of LuxTrust S.A., of the CA Factory services provider, of the LRAs and designated auditors as described in internal documents.

5.5.4 Archive backup procedures

See section 5.5.3.

5.5.5 Requirements for time-stamping of records

LuxTrust S.A. acting as CSP ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 is recorded. This is accomplished through accurate NTP synchronization of all systems.

5.5.6 Archive collection system

Archive collection systems are internal to the component service or legal entity operating the component service.

5.5.7 Procedure to obtain and verify archive information

Archives are accessible to the authorised personnel of LuxTrust S.A., of the CA Factory services provider, of the LRAs and designated auditors as described in internal documents. Records are retained in electronic or in paper-based format.

Records concerning TSTs and certificates may be made available (if required) for the purposes of providing evidence of certification for the purpose of legal proceedings. The Certificate Subject, and within the constraints of data protection requirements the Subscriber, may access to related registration records and other information relating to the Certificate Subject.

5.6 Key changeover

Not applicable unless in the context of TSA / CA key pair re-generation and re-installation (see section 6.1.4 of the present CPS) and in the context of TSA / CA private key compromise (see section 5.7.3 of the present CPS).
In the TSA context, key pair re-generation is covered within the applicable CP.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The applicable and appropriate incident and/or compromise reporting and handling procedures, disaster recovery procedures and Business Continuity Plan have been established and are available as a separate internal document. All such procedures are compliant against ISO/IEC 17799 standard. [17]

All incident and/or compromise events are documented and any associated records are archived as described in section 5.5 of the present CPS.

5.7.2 Computing resources, software, and/or data are corrupted

LuxTrust S.A. acting as CSP, as supported in its tasks by the CA Factory Services provider for operating the LuxTrust CAs, and by all other PKI Participants (other than Subscribers and Relying Parties), establishes the necessary measures to ensure full and highly automated recovery of the LuxTrust certification and time stamping services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 17799 standard.

Disaster recovery resources are established at sufficient distance from the original resources to avoid that a disaster would corrupt resources at both sites. Sufficiently fast communications are established between original and remote sites to ensure data integrity. Secured communications infrastructures are established from both sites to the RAs, the Internet, the certificate revocation status and repository services.

Disaster recovery infrastructure and procedures are fully tested at least once a year with witnessing of more than one member of the LuxTrust CSP Board.

5.7.3 Entity private key compromise procedures

Compromise of the CA private key(s) or of the associated activation data implies immediate revocation of the certificate of the compromised key(s).

The CA, i.e., LuxTrust S.A. acting as CSP, will additionally take the following measures:

- Notify all Certification Authorities with whom it is cross-certified
- Notify all other PKI Participants
- Notify the public at large through several channels, including a message on the LuxTrust repository and web site, a press release in the Grand-Duchy of Luxembourg,
- List the certificate of the corrupted CA in CRLs (ARLs),
- Update this certificate status in the Web interface service,
- Revoke all the certificates signed by the corrupted CA,

[17] ISO 17799 is often used as a generic term to describe what are two different documents: ISO17799 (aka ISO 27002), which is a set of security controls (a code of practice), and ISO 27001 (formerly BS7799-2), which is a standard 'specification' for an Information Security Management System (ISMS).

- LuxTrust S.A. acting as CSP may generate a new key pair and associated certificate for the CA, and re-issue all issued certificates that were revoked as a consequence of the CA corruption. This process is to be followed only after the following conditions:
    - assessing the reasons for corruption of the CA private key
    - revocation of the CA certificate,
    - having taken all the necessary measures to avoid the cause of revocation in the future,
    - decision from LuxTrust CSP Board,

Compromise of private key(s), or of the private keys associated activation data, of other entities (including Subscribers) leads to immediate revocation of the certificates associated to the compromised key(s). These entities are (contractually) bound to notify LuxTrust S.A. acting as CSP with regards to the issuing CA of any (suspicion of) such compromise of their private key(s) or of the associated activation data. See the applicable sections of the present CPS and of the applicable CP for further details on PKI Participants obligations in that matter.

The previous paragraph is also applicable in case PKI algorithms or associated parameters become insufficient for its remaining intended usage.

Compromise of the TSA private key(s) or of the associated activation data shall imply the immediate revocation of the certificate of the compromised key(s). Provisions of section 7.4.8 of the technical standard ETSI TS 102 023 [6] shall be satisfied.

The TSA, i.e., LuxTrust S.A. acting as TSSP, will additionally take the following measures:

- Notify all other PKI Participants
- Notify the public at large through several channels, including a message on the LuxTrust repository and web site, a press release in the Grand-Duchy of Luxembourg
- List the certificate of the corrupted TSA in CRLs (ARLs),
- After assessing the reasons for corruption of the TSA private key and revocation of the TSA certificate, and after having taken all the necessary measures to avoid the cause of revocation in the future, and after decision from LuxTrust CSP Board, LuxTrust S.A. acting as TSSP may generate a new key pair and associated certificate for the TSA.

5.7.4 Business continuity capabilities after a disaster

LuxTrust S.A. acting as CSP establishes the necessary measures to ensure full and highly automated recovery of the LuxTrust certification and time stamping services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 17799 standard.

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.8 CA, RA or TSA termination

LuxTrust S.A. acting as CSP ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of one of the following:

- the termination of one of the LuxTrust CA's services,
- the termination of one of the LuxTrust LRA networks or more,
- the termination of the LuxTrust TSA services,
- the termination of the LuxTrust certification services (including all CAs and all RAs services)

In all these cases LuxTrust S.A. guarantees continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

LuxTrust S.A. acting as CSP complies with the Grand-Duchy of Luxembourg 14/02/2000 modified law to the extent of the applicable provisions.

In particular:

- Before LuxTrust S.A. terminates (one of) its services the following procedures will be executed as a minimum:
    - LuxTrust S.A. will inform within a reasonable delay the following of the termination:
        - The Grand-Duchy of Luxembourg National Authority of Accreditation and Supervision as defined by the 14/08/2000 modified law;
        - All Subscribers and other entities with which LuxTrust S.A. has agreements or other form of established relations, among which Relying Parties and other CAs or CSPs;
        - In addition, this information will be made available to other relying parties;
    - LuxTrust S.A. will terminate all authorisations of sub-contractors to act on behalf of the terminated service (CA, TSA or RA) in the performance of any functions related to the process of issuing certificates.

- LuxTrust S.A. may take the necessary undertakings to transfer its time stamping activities towards a time stamping service provider having the same accreditation as LuxTrust S.A. if any.

- LuxTrust S.A. may take the necessary undertakings to transfer part or the entirety of its activities towards a (certification) service provider having the same accreditation as LuxTrust S.A. if any. The transfer (if any) of the impacted certificates will be operated under the following conditions:
    - LuxTrust S.A. informs every Subscriber (and/or Subject) whose certificate is still valid that it is willing to transfer the certificate to another CSP at least one (1) month before the effective transfer;
    - LuxTrust S.A. indicates the identity of the CSP to which the transfer is envisaged;
    - LuxTrust S.A. indicates to every Subscriber (and/or Subject) whose certificate is still valid his/her faculty of refusing the envisaged transfer within fifteen (15) days following the notification in written to the contact coordinates indicated in the notification. Without express indication by the Subscriber (and/or Subject) of his/her transfer acceptation within this period, his/her certificate shall be revoked.
    - LuxTrust S.A. acting as CSP, shall destroy, or withdraw from use, its private keys related to the terminated certification (component) services, as described in section 6.2.10 of the present CPS.

- In case LuxTrust S.A. will terminate its activities without a transfer of part or the entirety of its activities, LuxTrust S.A. will revoke the impacted certificates one (1) month after having notified Subscribers and/or Subjects. LuxTrust S.A. will perform necessary undertakings to transfer obligations for maintaining registration information, and event log archives, including revocation status information, for their respective period of time as indicated to the Subscriber and Relying Parties (see applicable sections of the present CPS).

- LuxTrust S.A. has arrangements to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

- Termination of TSA activities will be in particular done in compliance with section 7.4.9 of the technical standard ETSI TS 102 023 [6].

6 TECHNICAL SECURITY CONTROLS

The security measures taken by LuxTrust S.A. with regards to its CAs to protect CAs cryptographic key and activation data, the constraints on repositories, subject CAs, and other PKI Participants, including TSA, to protect their Private Keys, activation data for their Private Keys, and critical security parameters, ensuring secure key management, and other technical security controls used by LuxTrust S.A. to perform securely the functions of key generation, user authentication, Certificate registration, Certificate revocation, auditing, archiving, and other technical security controls on PKI Participants are compliant with the following technical standards:

- ETSI TS 102 023 “Policy requirements for time-stamping authorities” [6] for LuxTrust Time Stamping Services,
- ETSI TS 102 042 “Policy requirements for certification authorities issuing public key certificates” [4],
- ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates” [3].

These controls are further described and ruled by the following sub-sections.

As a general requirement, all communications between PKI Participants involved in the LuxTrust PKI services provision are (electronically) signed and protected against unauthorised disclosure (e.g., encrypted). When implemented, encryption will not depend on PKI Participants decryption keys but shall combine appropriate encryption and access control mechanisms to avoid usage of any key escrow mechanism.

6.1 Key pair generation and installation

Key pair generation and installation is considered for the relevant PKI Participants, which are the issuing CA (including the LuxTrust Root CA, the LuxTrust Normalised CA and the LuxTrust Qualified CA), (S)SCD services providers, repositories, RAs, SRAs, Time Stamping Authority (TSA), and Subscribers.

6.1.1 Key pair generation

6.1.1.1 LuxTrust CA Key pair generation and installation

6.1.1.1.1 LuxTrust CA Key generation process

LuxTrust S.A. acting as CSP, through the support of the CA Factory services provider, uses a trustworthy process and systems for the generation of its LuxTrust Root CA, LuxTrust Normalised CA, LuxTrust Qualified CA private keys (and certificates) according to a documented internal procedure.

The secret shares of these private keys are distributed amongst authorised secret-shareholders under the authority of the CSP according to a documented procedure. The CSP (and the CAs) acknowledges public, international and European standards on trustworthy systems.

LuxTrust S.A. acting as CSP ensures that CAs private keys are securely generated, used and protected, using a trustworthy system, and that the necessary measures are taken to prevent their compromise or unauthorised usage. The CAs key management (including but not limited to generation, usage, and dismissal) is implemented and documented in line with the LuxTrust CPS. These documented procedures shall meet the requirements as laid down in the technical standard ETSI TS 101 456 [3] and in the technical standard ETSI TS 102 042 [4] for the respective CAs.

CAs key pair (and certificates) generation and installation procedure, CAs Key Ceremony, involve several trusted personnel among which:

- at least three (3) trusted and appropriately authorised operatives including more than one (1) appropriately authorised member of CA Factory staff serving in trustworthy positions,
- at least one (1) representative of LuxTrust CSP,

- a Master of Key Ceremony, and
- at least two independent and external auditors.

This process is witnessed by LuxTrust CSP representative(s) to ensure confidence in the proper and secure execution of the CAs Key generation procedure.

At least three trusted operatives participate in all operations required in preparation of and subsequent to the CAs Key generation ceremony. More than one member of the LuxTrust CSP Board makes authorisation of key generation in writing in accordance to the decision rules in force within the LuxTrust CSP Board.

The CA key pair certificate requests are made available (under standard format) to LuxTrust S.A. and are protected by appropriate measures to prevent unauthorised usage. More than one member of the LuxTrust CSP Board makes authorisation of CA key pair certificate requests in writing in accordance to the decision rules in force within the LuxTrust CSP Board.

6.1.1.1.2 LuxTrust CA Key generation devices and key storage

The generation and storage of CA private keys of the LuxTrust CAs occurs within a secure cryptographic device meeting appropriate requirements as set forth in section 6.2.1 of the present CPS (for CA secure cryptographic devices requirements).

Such secure CA cryptographic devices is prepared, distributed and managed in compliance with the technical standard ETSI TS 101 456 [3].

The storage of the private key of the CA requires multiple controls by appropriately authorised members of the CA Factory staff serving in trustworthy positions. More than one member of the LuxTrust CSP (Board) makes authorisation of key storage and of assigned personnel in writing.

6.1.1.1.3 LuxTrust CA Key pair re-generation and re-installation

In case of LuxTrust CAs key pair re-generation and re-installation, when replacing private keys by new ones, LuxTrust S.A. ensures that exactly the same procedure as for initial key generation is used. Appropriate measures are taken to communicate the end of CA key life cycle and replacement to Subscribers and Relying Parties, also taking into account statements made in the section 6.1.4 of the present CPS.

At the end of their lifetime, the CA private keys that have been used in the past must be decommissioned and destroyed as well as the active tamper resistant devices and as well as all back-up copies of past private keys in accordance with section 6.2.10.

The CA certificate roll-over are taking into account the issuing and usage period of LuxTrust TSA certificates and the resulting validity period of issued Time Stamp Tokens (TST).

Similar rules apply for re-generation and key usage periods for LuxTrust Qualified CAs (LTQCAs) for issuing LuxTrust Qualified Certificates.

6.1.1.2 LuxTrust RA Key pair *generation* and installation

When not specified in the following text, “RA” shall collectively designate the CRA, SRA, LRA and their respective Officers, “CRA” shall collectively designate CRAs and their respective Officers, and similarly for “LRA”.

6.1.1.2.1 LuxTrust RA Key generation process

RAOs (either CRAOs or LRAOs) key generation follow the same process as for LuxTrust Subscriber initial identification and authentication process with the following identified differences:

- Delivery of LuxTrust Smart Cards exclusively (thus no LuxTrust Signing Server Account),
- The Local Registration Authority (Officers) that (who) is in charge of RAOs registration is the authorised members of the *LuxTrust RA Network Coordination Cell* acting as Chief LRAOs,

- The Certificate policy is the same but with a specific OID for identification of RAO certificates as well as for clear segregation of duties and access rights to certificate type generation process in RAO software.

When RAs entities are not identified (and authenticated) as Officers (human being) but as hardware used in connection with an automated process or server, keys are protected with HSMs complying with requirements as described in section 6.2.1 of the present CPS. Such entities are registered as for CA entities. and the RA HSM devices are prepared, distributed and managed in compliance with the technical standard ETSI TS 101 456 [3].

6.1.1.2.2 LuxTrust RA Key generation devices and key storage

The generation and storage of RA private keys of the LuxTrust RAs occurs within a secure cryptographic device meeting appropriate security requirements as applicable in the relevant CP. Such devices meet SSCD requirements as available in Annex III of the Directive [1], and successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

Such secure cryptographic devices are prepared, distributed and managed in compliance with the technical standard ETSI TS 101 456 [3]. See section 6.2.1 of the present CPS for requirements on RA secure HSM devices and for RAO Smart Card requirements.

6.1.1.2.3 LuxTrust RA Key pair re-generation and re-installation

In case of RAs key pair re-generation and re-installation, when replacing private keys by new ones, exactly the same procedure as for initial key generation shall be used. Subsequently and without any delay, the obsolete private keys must be decommissioned and destroyed and the active tamper resistant devices securely recycled or destroyed.

6.1.1.3 Other PKI Participants Authorities Key pair generation and installation

Key Pair generation and installation for other PKI Participant Authorities (i.e., other than Subscribers and Relying Parties), e.g., for CA Factory Services provider, (Secure) Signature Creation Device Providers, OCSP validation services provider, etc. is applicable as for RAs, when applicable, to the exception of Time Stamping Authority (TSA) for which the applicable rules are the ones as applicable for CAs and are compliant with the technical standard ETSI TS 102 023 [6] (e.g., section 7.2).

See section 6.1.1.1.3 for specifications ruling the re-generation and key usage periods for LuxTrust Qualified TSAs for issuing LuxTrust TSTs. If required Officers from these PKI Participants may receive the same type of secure cryptographic devices as for RAOs.

6.1.1.4 Subscribers Key pair generation and installation

6.1.1.4.1 Key pair generation by CSP

When key generation process is ensured by LuxTrust S.A. acting as CSP, generation is performed in compliance with the ETSI TS 102 042 [4] technical specifications, or the ETSI TS 101 456 [3] technical specifications respectively for Normalised or Qualified certificates. The private key activation data may be sent to the Certificate Subject (identified person) or delivered to the certificate Subject according to a physical presentation based procedure that is strictly followed by the LRAO registering the Subscriber (Certificate Subject), as an internal and auditable document (non-identified person).

In case of LuxTrust Signing Server Account, the Subscriber's private key:

- Is generated securely within the LuxTrust Signing Server in such a way that the Subscriber's private key shall never leave the LuxTrust Signing Server,
- Is not be used in a way that was not authorised (activated) by the Subscriber's activation data, in a way that can reach, or be as close as possible to, the level of "under the sole control of the Subscriber",
- Is not be distributed to the Subscriber but securely hosted by the LuxTrust Signing Server Services Provider in accordance with the LuxTrust CPS.

To the sole exception of the pseudonym certificates, none of the PKI Participants (other than the Subscriber) are ever, in possession of both the full Subscriber's Activation Data (i.e., both UID/static PWD and OTP-Credential) and the Subscriber private key. Only the Subscriber shall be in possession of the full Subscriber's Activation Data, i.e., both UID/static PWD and OTP-Credential.

In case of LuxTrust physical SSCD end-user devices, the Subscriber's private key:

- Is generated securely within the LuxTrust SSCD, in accordance with the SSCD requirements,
- Has its corresponding Public Key certified by the CA in an immediately suspended Certificate once generated,
- Is sent to the Subscribers (identified person) shipping address after registration at back-office.
- Is distributed to the Subscriber in a face-to-face process once identified and authenticated by a LuxTrust authorised LRAO in accordance with the applicable CP and with the LuxTrust CPS,
- Is distributed using a channel that is separated from the one used for distribution of Subscriber's Private Key Activation Data

To the sole exception of the pseudonym certificates, the CRA(O) and LRA(O) are never, at a time, in possession of both the Subscriber's Activation Data (i.e., Smart Card PIN/PUK-Letter) and the (S)SCD, even if they are both in separated sealed envelopes.

6.1.1.4.2 Key pair generation by Subscriber

When key generation process is ensured by the Subscriber, this is performed in compliance with the ETSI TS 102 042 [4] technical standard, LCP Policy, the applicable CP and is performed under the sole and entire responsibility of the Subscriber or Subscriber's organisation. The private key activation data is delivered to the certificate Subject by the Subscriber and under the responsibility of the Subscriber.

Key generation by Subscriber is limited to LuxTrust SSL/TLS Server certificates and Object Signing certificates.

6.1.1.4.3 LuxTrust Subscriber Key generation devices and key storage

LuxTrust secure devices

Generation and storage of Subscriber's private keys occurs within a (secure) cryptographic device meeting appropriate security requirements as applicable in the relevant Certificate Policy.

Secure Subscriber Devices used by the CSP for generation and storage of LuxTrust Subscribers private keys (and certificates) meet SSCD requirements as available in Annex III of the Directive [1], and are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

Such NCP+ or QCP+ devices are prepared, distributed and managed in compliance with the technical standard ETSI TS 102 042 [4] and with ETSI TS 101 456 [3] when this standard impose higher requirements.

LuxTrust Signing Server

LuxTrust Signing Server devices used for generation and storage of LuxTrust NCP private keys (and certificates) are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High. Such NCP devices are prepared, made available to the Subscriber and managed in compliance with the technical standard ETSI TS 102 042 [4]. Situations for which the Subscriber's private key is leaving the Signing Server secure environment or is generated or used on the Subscriber environment (e.g., PC, PDA, etc.) are strictly forbidden.

See section 6.2.1 of the present CPS for requirements on Subscriber's secure cryptographic devices when provided by LuxTrust S.A.

6.1.1.4.4 LuxTrust Subscriber Key pair re-generation and re-installation

See section 4.7 of the present CPS.

6.1.2 Private key delivery to Subscriber

See section 6.1.1.4 for key generation done by CSP.

6.1.3 Public key delivery to certificate issuer

See section 6.1.1.4 when key generation is done by CSP.

When key generation is done by the Subscriber, the certificate request process ensures that the Subject (or Subscriber in case different from the Subject) has possession of the Private Key associated with the Public Key presented for certification, and that the procedure of issuing the certificate is securely linked to the associated registration or certificate re-key. See applicable CP for further details.

6.1.4 CA public key delivery to Relying Parties

The LuxTrust CAs public keys are securely provided to potential Relying Parties using the following channels:

- Initial publication of the LuxTrust CAs public keys certificates (at least the fingerprints) may be ensured through addendum publication of the LuxTrust S.A. articles of associations in the Grand-Duchy of Luxembourg official registry of legal persons. Alternative measures may be taken in order to give assurance of the correctness of these certificates.
- LuxTrust CAs public keys certificates are available in a SSL session from the LuxTrust S.A. repository available at https://repository.luxtrust.lu
- The LuxTrust TSAs and RAs certified public keys are securely provided to potential Relying Parties using a SSL session from the LuxTrust repository available at https://repository.luxtrust.lu.

6.1.5 Key sizes

6.1.5.1 LuxTrust CA Private Key Type

For its root key the LuxTrust Root CA makes use of the RSA SHA-1 algorithm with a key length of **minimum 2048 bits**. First LuxTrust Root private key shall be certified for a period of up to 15 years.

For its primary key the LuxTrust Normalised CA makes uses of RSA SHA-1 algorithm with a key length of **minimum 2048 bits**. First LuxTrust Normalised CA private key shall be certified for a period of up to 10 years.

For its primary key the LuxTrust Qualified CA makes uses of RSA SHA-1 algorithm with a key length of **minimum 2048 bits**. First LuxTrust Qualified CA private key shall be certified for a period of up to 10 years.

Other CAs root signed by the LuxTrust Root CA and incorporated within the LuxTrust PKI (CA Factory operation) domain may have private key length within the range of minimum 2048 bits and the Root CA key size as a maximum (e.g., 3072 bits in the 2048-4096 range).

Other CAs **not** root signed by the LuxTrust Root CA and incorporated within the LuxTrust PKI (CA Factory operation) domain may be added with a private key length above 4096 bits.

LuxTrust CSP may implement, through the support of the CA Factory services provider, other algorithms than RSA SHA-1 for signature generation or verification, namely the DSA algorithm and, optionally, the Elliptic Curve DSA algorithm with appropriate and state-of-the-art key sizes, as well as other hashing functions than SHA-1 with appropriate and state-of-the-art key sizes.

6.1.5.2 LuxTrust RA Private Key Type

LuxTrust RA operators are provided with an SSCD with keys with an RSA key length of **minimum 1024 bits** or equivalent. Certificates are issued under the LuxTrust qualified CA for a period of 3 years.

6.1.5.3 LuxTrust other PKI Participant Authorities Private Key Type

Private Key type requirements, when applicable, for other PKI Participant Authorities (i.e., other than Subscribers and Relying Parties), e.g., for CA Factory Services provider, (Secure) Signature Creation Device Providers, OCSP validation services provider, etc. are applicable as for RAs.

Private Key type requirements for LuxTrust TSA are such that primary key of the LuxTrust TSA have an RSA key length of **minimum 1024 bits** or equivalent are certified for a period of 5 years (i.e. 60 months). Public key parameters generation and checking during TSA key pair generation are implemented according to the LuxTrust Time Stamping Policy [12] and the technical standard ETSI TS 102 023 [6].

6.1.5.4 LuxTrust Subscriber Private Key Type

Subscriber's minimum private key length is RSA **1024 bits** or equivalent. Certificate validity period is defined in the applicable CP (e.g., LuxTrust Normalised NCP(+) certificates issued by the LTNCA shall be certified for a period of 3 years, while LuxTrust Certificates issued by the LTQCA are certified for a period of 3 years or 5 years with a minimum key size of respectively 1024 bits and 2048 bits).

6.1.6 Public key parameters generation and quality checking

Public key parameters generation and checking during CA key pair generation are implemented according to the applicable CP.

By default, public key RSA exponents are chosen secure (e.g., Fermat 4). Public Key module generation is done with state of the art parameter generation technology (e.g., Blum Blum Schub). Parameter generation is implemented using state of the art technology and are regularly re-evaluated regarding new advances in cryptology.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

6.1.7.1 LuxTrust CA Private Key purposes

LuxTrust S.A. ensures that the CA Private Keys are protected in accordance with the LuxTrust CPS and that the CA private signing key(s) are only used for signing certificates CRLs and OCSP responses as well as certificates in accordance with the intended use of each of these keys. LuxTrust S.A. ensures that the CA private keys are not used within the CA in any way outside the scope of the LuxTrust PKI domain.

6.1.7.1.1 LuxTrust Root CA key usage and purpose

Private key of the LuxTrust Top Root CA is used to sign sub-ordinates LuxTrust CAs as the LuxTrust Normalised CA and the LuxTrust Qualified CA, corresponding ARLs. LuxTrust Root CA is an off-line CA and is never used for signing end-entity certificates.

6.1.7.1.2 LuxTrust Normalized CA key usage and purpose

The private key of the LuxTrust Normalised CA is used to sign Certificates issued to end-entities, the corresponding CRLs and OCSP certificates. Other usages are restricted. LuxTrust Normalised CA is an on-line CA.

6.1.7.1.3 LuxTrust Qualified CA key usage and purpose

The private key of the LuxTrust Qualified CA is used to sign Certificates issued to end-entities, the corresponding CRLs and OCSP certificates. Other usages are restricted. LuxTrust Qualified CA is an on-line CA.

6.1.7.2 LuxTrust RA and other PKI Participant Authorities Private Key purposes

The RA protects its Private Key(s) in accordance with the LuxTrust CPS. The RA uses its private signing key(s) only and exclusively for using the RA software in the context of their role in the Subscribers registration process and certificate life-cycle management in accordance with the intended use of each of these keys, the LuxTrust CPS and the applicable Certificate Policy.

The private key of the LuxTrust Chief LRA is only and exclusively used in the RA software in the context of their role in the LRA (and potentially Subscribers) registration process in accordance with the intended use of each of these keys, the LuxTrust CPS and the applicable Certificate Policy.

The private key of the LuxTrust TSAs is only and exclusively used in the context of their role in the LuxTrust time stamping services they are providing in accordance with the intended use of each of these keys, the LuxTrust CPS and the applicable LuxTrust Time Stamping Policy [12] and the technical standard ETSI TS 102 023 [6].

The private key of other LuxTrust PKI Participant Authorities or service providers are only and exclusively used in the context of their role in the LuxTrust certification component services they are providing in accordance with the intended use of each of these keys, the LuxTrust CPS and the applicable Certificate Policy.

6.1.7.3 LuxTrust Subscriber Private Key purposes

In accordance with the present LuxTrust CPS and the applicable CP, upon signature of the Subscriber Agreement, the Subscriber gives his/her acceptance to the following responsibilities related to the Subscriber private key and Certificate usage:

- In using the Key Pair, the Subscriber must comply with any limitations (e.g., Key usage, Limitations, etc.) indicated in the Certificate, in the applicable CP or in applicable contractual agreements.
- the Subscriber must protect the Private Key and its Activation Data at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. Once the Private and Public key pair has been delivered to the Subscriber, the Subscriber is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Subscriber is deemed the sole user of the Private Key. The Private Key Activation Data (e.g., PIN-code or password(s)) used to prevent unauthorised use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without adequate protection. The Subscriber must never leave the Private Key or the Private Key Activation Data unsupervised when it is not locked (e.g., leave it unsupervised in a work station when the PIN code or password has been entered). The Subscriber has sole liability for the use of the Private Key. The CA or LuxTrust S.A. acting as CSP is not liable for the use made of the Key Pair belonging to the Subscriber or for any damage resulting from misuse of the Key Pair.
- The Subscriber shall refrain from tampering with a Certificate.
- The Subscriber shall only use Private Key and Certificate for legal and authorised purposes in accordance with the present CP, the Subscriber Agreement and the LuxTrust CPS, and as it may be reasonable under the circumstances.

The Key usage fields of the LuxTrust Certificates are respectively set in the applicable CP.

6.2 Private key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

6.2.1.1 Private key protection and CME control for CAs

The CSP uses appropriate secure cryptographic devices to perform CA key management tasks. These cryptographic devices are known as Hardware Security Modules (HSMs). When applicable other PKI Participants make use of such HSMs as well (see section 6.1 of the present CPS).

See section 6.2.1.3 of the present CPS for further details about HSM requirements.

Hardware and software mechanisms that protect CA private keys are adequately documented. HSMs are prepared, distributed and managed in compliance with the following technical standards:

- ETSI TS 102 042 [4];
- ETSI TS 101 456 [4];
- CWA 14167-1:2003.

HSMs do not leave the secure environment of the CA secured premises. In case HSMs require maintenance or repair that cannot be performed within CA secured premises (under dual control of more than one authorised member of CA Factory staff serving in trustworthy positions), they are securely shipped to their manufacturer.

The CA private keys are not present on HSM when it is securely shipped for maintenance or repair outside the CA secure premises. Between usages sessions, HSMs are kept securely within the CA secure premises.

The CA private keys remain under n out of m multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CAs private keys. CAs keys are then active for defined time periods.

The CA archives its own public keys and related certificates; the CA private key is not escrowed.

6.2.1.2 Private key protection and CME control for other PKI Participants

When applicable, the TSA, RA, SRA, (S)SCD or other services providers when using automated CMEs, use appropriate secure cryptographic devices to perform their tasks. These cryptographic devices are known as Hardware Security Modules (HSMs). See section 6.1 and section 6.2.1.3 of the present document for further details about such HSM requirements.

HSMs are prepared, distributed and managed in compliance with the following technical standards:

- ETSI TS 102 042 [4];
- ETSI TS 101 456 [4];
- CWA 14167-1:2003..

LuxTrust PKI Officers and LuxTrust (S)SCD Subscribers make use of (S)SCD whose requirements are provided in section 6.2.1.3 of the present CPS. Requirements on LuxTrust Signing Server tokens are provided in the same section 6.2.1.3.

6.2.1.3 LuxTrust Secure Cryptographic Devices requirements

6.2.1.3.1 LuxTrust Smart Card requirements

The LuxTrust Smart Card and card-carrier will support the following standards

- ISO 7810, format ID-1
- ISO 7816-1 up to ISO 7816-9

Application integration is possible using PKCS#11 and Microsoft Crypto-API, based on PC/SC.
LuxTrust Smart Cards contain at least 2 LuxTrust Certificates as well as the full chain of CA certificates. In particular, smart cards contain one authentication certificate (QCP) and one signature Certificate (QCP+), certifying keys of 1024 up to 2048 bits each.

When considered as SSCD, the security provided by the proposed chip on the card (token) and/or the Card(Token)-OS used meet the requirements of an SSCD as specified by the applicable regulations (e.g., the 14 August 2000 Luxembourg law on e-commerce as modified, and the European Directive 1999/93/EC on electronic signatures). Assessment of such compliance can be made against:

- CWA 14167-1 : Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures : Part 1 - System Security Requirements, and
- CWA 14167-2 : Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures : Part 2 - Protection Profile for CSP Signing Operations, and/or
- CWA 14169 : Secure Signature-Creation Devices “EAL 4+”, and/or

- CWA 14355 : Guidelines for the Implementation of SSCDs.

LuxTrust SSCDs are successfully certified / validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

Such SSCD devices shall be prepared, distributed and managed in compliance with the technical standard ETSI TS 102 042 [4] and with ETSI TS 101 456 [3] when this standard impose higher requirements.

6.2.1.3.2 LuxTrust Signing Server tokens requirements

The HSM used to protect the sensitive signature key(s) are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with **EAL 4+ SOF-High,** against a security target or protection profile which meets the requirements of the technical standard ETSI TS 101 456 [3], based on a risk analysis and taking into account physical and other non-technical security measures.

6.2.1.3.3 LuxTrust Hardware Security Module (HSM) requirements

The LuxTrust HSMs used by CAs and TSAs in the context of the LuxTrust services provision are secure cryptographic devices meeting at least the requirements of an SSCD as specified by the applicable regulations (e.g., the 14 august 2000 Luxembourg law on e-commerce as modified, and the European Directive 1999/93/EC on electronic signatures).

The LuxTrust HSMs used by other PKI Participants other than Subscribers and Relying Parties (RA, SRA, SSCD providers, etc.) in the context of the LuxTrust services provision are secure cryptographic devices meeting at least the requirements of an SSCD as specified by the applicable regulations (e.g., the 14 august 2000 Luxembourg law on e-commerce as modified, and the European Directive 1999/93/EC on electronic signatures).

They are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with **EAL 4+ SOF-High,** against a security target or protection profile which meets the requirements of the technical standard ETSI TS 101 456 [3], based on a risk analysis and taking into account physical and other non-technical security measures.

Such HSM devices are prepared, distributed and managed in compliance with the technical standard ETSI TS 101 456 [3].

6.2.2 Private key (n out of m) multi-person control

6.2.2.1 LuxTrust CA secret shares management

Protection of CA's private keys are, amongst other appropriate measures, ensured by splitting-up of a strong encryption key over several (M) tamper resistant devices (e.g., smart cards, PED keys) that are protected with multiple passphrases (shares). These tamper resistant devices meet requirements as stated in section 6.2.1 of the present CPS.

The LuxTrust CA secret shares are held by multiple authorised holders, to safeguard and improve the trustworthiness of private keys. A certain number of shares ('N' out of 'M'), and at least three ('N' ≥ 3), out of the total shares need to be available and used concurrently to activate or re-activate the CA private key.

Before secret share-holders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody. They must receive the secret share within a physical medium, tamper resistant device, as approved by the LuxTrust CSP. The CA keeps written, auditable, records of secret share distribution. In case secret share custodians (or shareholders) are to be replaced in their role of shareholder, the CA shall keep track of the renewed share device distribution.

More than one member of the LuxTrust CSP (Board) makes authorisation of CA private key shares distribution and of assigned personnel in writing.

Private keys of the CAs are not escrowed. LuxTrust S.A. ensures that internal disaster recovery measures are implemented.

6.2.2.2 LuxTrust secret shares management for other PKI Participants

Not applicable.

6.2.3 Private key escrow

Key escrow is never allowed.

6.2.4 Private key backup

6.2.4.1 LuxTrust CA Key back-up

LuxTrust S.A. ensures that LuxTrust CAs' private keys are backed-up, stored and recovered by multiple and appropriately authorised CA Factory staff serving in trustworthy positions, and witnessed by more than one representative of the LuxTrust CSP. More than one member of the LuxTrust CSP (Board) makes authorisation of key back-up and of assigned personnel in writing.

At the end of a key generation ceremony, new CA keys are burnt encrypted on a back-up key storage media (e.g. dedicated and secure backup token) that ensures similar level of protection as provided by the secure cryptographic device holding CA keys. The CA records each step of the key back-up process using a specific form for logging information. The CA private key is locally archived within the CA premises.

LuxTrust CAs' private keys back-up, storage, and recovery procedures are implemented and documented in accordance with the LuxTrust CPS and in auditable internal documents.

6.2.4.2 LuxTrust RA Key back-up

No back-up and no escrow of the RAs signature private keys are allowed.
No back-up and no escrow of the RAs authentication/encryption private keys are allowed.

6.2.4.3 LuxTrust Subscriber Key back-up

Subscriber's key back-up and key recovery are not allowed except for the sole purpose of and in the context of LuxTrust Signing Server Account disaster recovery as stated and ruled by the LuxTrust CPS and the applicable CP.

Subscriber's key escrow is never allowed.

6.2.5 Private key archival

Not applicable.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

For CAs, see section 6.2.1.1; for RAs,and other PKI Participants other than Subscribers, see section 6.2.1.2; and for Subscribers, see section 6.2.1.3.

6.2.8 Method of activating private key

The CA private keys remain under N out of M multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CAs private keys. CAs keys are then active for defined time periods.

All PKI Participants other than Subscribers and Relying Parties receive, when applicable, private keys that are generated on SSCD by LuxTrust S.A. acting as CSP and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the SSCD.

When Subscribers receive private keys that are generated by LuxTrust S.A. acting as CSP, these keys are stored on (S)SCD and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the (S)SCD.

6.2.9 Method of deactivating private key

The CA private keys remain under N out of M multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CAs private keys. CAs keys are then active for defined time periods.

6.2.10 Method of destroying private key

At the end of their lifetime the CA private keys are destroyed by trusted CA staff members in the presence of more than one representative of the LuxTrust S.A., in order to ensure that these private keys cannot ever be retrieved or used ever again.

The CA keys are destroyed through secure deletion from the primary and backup media, powering off and removing permanently any hardware modules the keys were stored on. These hardware modules are treated in a secure manner as described within documented key destruction internal procedures. Associated records are securely archived within LuxTrust premises.

More than one member of the LuxTrust CSP (Board) makes authorisation of CA private key destruction and of assigned personnel in writing.

At the end of their lifetime the RA private keys are destroyed by more than one representative (Chief LRAO) of the LuxTrust *RA Network Coordination Cell*, in order to ensure that these private keys cannot ever be retrieved or used ever again.

The RA keys are destroyed by shredding their LuxTrust SSCD and/or by deleting, powering off and removing permanently any hardware modules the keys were stored on. These hardware modules are treated in a secure manner as prescribed by internal procedures.

More than one member of the LuxTrust CSP (Board) makes authorisation of RA private key destruction and of assigned personnel in writing.

At the end of their lifetime the Subscriber private keys when provided by LuxTrust S.A. acting as CSP are destroyed by any LuxTrust authorised LRAO in order to ensure that these private keys cannot ever be retrieved or used ever again. These Subscriber keys are destroyed by shredding their LuxTrust (S)SCD and/or by deleting, powering off and/or removing permanently any hardware modules the keys were stored on. These hardware modules are treated in a secure manner as prescribed by internal procedures. The Subscriber keys destruction process shall be documented and any associated records shall be archived.

End of TSA key life cycle shall be managed in conformance with the technical standard ETSI TS 102 023 (e.g., section 7.2.5) [6].

6.2.11 Cryptographic module rating

See section 6.2.1.3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

LuxTrust S.A. acting as CSP archives its own LuxTrust CA public keys. See section 5.5 of the present CPS for archival conditions.

6.3.2 Subscriber Certificate operational periods and key pair usage periods

LuxTrust S.A. acting as CSP issues Subscriber certificates with validity periods as indicated on such certificates, see applicable CP for further details.

6.4 Activation data

LuxTrust S.A. acting as CSP ensures that activation data associated to LuxTrust CAs and TSAs private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 6.1 and 6.2.

All PKI Participants other than Subscribers and Relying Parties receive, when applicable, private keys that are generated on SSCD by LuxTrust S.A. acting as CSP and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the SSCD. LuxTrust S.A. acting as CSP ensures that such PKI Participants activation data are securely managed and protected by such participants through applicable CP, contractual agreement and internal procedures made available to these participants.

When Subscribers receive private keys that are generated by LuxTrust S.A. acting as CSP, these keys are stored on (S)SCD and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the (S)SCD. Subscribers are responsible for the secure management and protection of their activation data, see section 4.1.2(.3) of the present CPS and the applicable CP for further details.

6.5 Computer security controls

LuxTrust S.A. acting as CSP ensures that computer security controls are implemented in compliance with the technical standard ETSI TS 102 023 [6] (for TSA activities), the technical standard ETSI TS 102 042 [4] and with ETSI TS 101 456 [3] when this standard imposes higher requirements on certification practices. Detailed descriptions of implemented computer security controls are available as internal document(s).

LuxTrust is accredited by ILNAS acting as accreditation entity. The Accreditation Certificate, issued on Tuesday, October 13th, 2009, testifies that LuxTrust conforms to the following technical standards:

- ETSI TS 101 456 on Policy requirements for certification authorities issuing qualified certificates [3] ;
- ETSI TS 102 042 on Policy requirements for certification authorities issuing public key certificates [4], and
- ETSI TS 102 023 on Policy requirements for time-stamping authorities [6].

The Accreditation Certificate is registered under the reference N° 8/005. The national registry of Accredited Certification Service Providers is publicly available on the ILNAS website http://www.ilnas.lu/.

6.6 Life cycle technical controls

LuxTrust S.A. acting as CSP ensures that periodic development control, security management and life cycle security controls are implemented in compliance with the technical standard ETSI TS 102 023 [6] (for TSA activities), the technical standard ETSI TS 102 042 [4] and with ETSI TS 101 456 [3] when this standard impose higher requirements on certification practices. Detailed descriptions of implemented life cycle technical controls are available as internal document(s).

6.7 Network security controls

LuxTrust S.A. acting as CSP ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the technical standard ETSI TS 102 023 [6] (for TSA activities), the technical standard ETSI TS 102 042 [4] and with ETSI TS 101 456 [3] when this standard impose higher requirements on certification practices.

Detailed descriptions of implemented network security controls are available as internal document(s).

6.8 Time-stamping

The LuxTrust Time-Stamping services as described in section 1.3.5.6 in the present CPS are used by LuxTrust S.A. acting as CSP for the time-stamping of archive records as required by section 5.5.5 of the present CPS in the context of “audit logging procedures”. The LuxTrust Time-Stamping services are provided in compliance with the technical standard ETSI TS 102 023 [6].

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

7.1.1 *Version number(s)*

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

For detailed subscriber certificate profiles, please refer to the applicable CP.

LuxTrust CAs certificate profiles description is available as follows:

LuxTrust Root CA					
Base Profile	OID	Included	Critical	Value	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time **+up to 15 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		US	Fixed
CommonName	{ id-at-3 }	X		GTE CyberTrust Global Root	Fixed
organizationName		X		GTE Corporation .	Fixed
organizationlUnitName		X		GTE CyberTrust Solutions, Inc.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust root CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.6.1.4.1.6334.1.0	Fixed

LuxTrust Root CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://www.public-trust.com/CPS/OmniRoot.html	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://www.public-trust.com/cgi-bin/CRL/2018/cdp.crl l	Fixed
BasicConstraints	{id-ce 19}	X	TRUE		
CA		X		TRUE	Fixed
pathLenConstraint		X		1 (None)	Fixed

LuxTrust Normalised CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing LTRCA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time +**up to 10 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust root CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed

LuxTrust Normalised CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Normalised CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.1.0.1.	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.luxtrust.lu/LTRCA.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed

LuxTrust Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Version		X		V3	
SerialNumber		X		As provided by CA or by LuxTrust S.A.	
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing LTRCA Signature	
Validity					
NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time +**up to 10 years**	Fixed
SubjectPublicKeyInfo		X		Public Key: Key length: 2048 up to 4096 bits (RSA); public exponent: Fermat-4 (=010001).	

LuxTrust Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Issuer					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }	X		LuxTrust root CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
Subject					
CountryName	{ id-at-6 }	X		LU	Fixed
CommonName	{ id-at-3 }			LuxTrust Qualified CA	Fixed
organizationName		X		LuxTrust S.A.	Fixed
CertificatePolicies	{id-ce 32}	X	FALSE		
policyIdentifier		X		1.3.171.1.1.1.1.0	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.luxtrust.lu	Fixed
KeyUsage	{id-ce 15}	X	TRUE		
keyCertSign				Set	Fixed
crlSign				Set	Fixed
offlinecrlSign				Set	Fixed
digitalSignature				Set	Fixed
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Authority public key	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash of Subject public key	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.luxtrust.lu/LTRCA.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE [18]	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – SignatureCA	Fixed

[18] This extension has been set as critical in the current version of the CPS but it is not currently the case in the existing LTNCA certificate. Criticality of this extension should be carefully considered with regards to the compliance with RFC 3280 stating in its section 4.2.1.10 that "*This extension MUST appear as a critical extension in all CA certificates that contain public keys used to validate digital signatures on certificates. This extension MAY appear as a critical or non-critical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates*".

LuxTrust Qualified CA					
Base Profile	**OID**	**Included**	**Critical**	**Value**	
Thumbprint algorithm				Sha1	
Thumbprint				Thumbprint value	

LuxTrust Normalised CA and LuxTrust Qualified CA can have self-signed certificates that are used to the sole discretion of LuxTrust S.A. acting as CSP through decisions of its CSP Board.

7.1.2 *Certificate extensions*

X.509 v3 extensions are supported and used as indicated in the Certificates profiles as described in section 7.1.1 of the present CPS and/or in the applicable CP.

7.1.3 *Algorithm object identifiers*

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

7.1.4 *Name forms*

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

7.1.5 *Name constraints*

Name constraints are supported as per RFC 5280.

7.1.6 *Certificate policy object identifier*

Certificate policy object identifiers are used as per RFC 3739.

7.1.7 *Usage of Policy Constraints extension*

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

7.1.8 *Policy qualifiers syntax and semantics*

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

7.1.9 *Processing semantics for the critical Certificate Policies*

Not applicable.

7.2 CRL profile

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

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

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

LuxTrust CRL Profile	
Field	Comments
Version	v2
Signature	Sha1RSA
Issuer	<subjectCA>
thisUpdate	<creation time>

LuxTrust CRL Profile	
Field	**Comments**
nextUpdate	<creation time + 100 days for Root CA> <creation time + 4,5 hours (4 hours and 30 minutes) for NCA & QCA>
revokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
reasonCode	*<Insert List of used revocation reason code>*
crlExtensions	
cRLNumber	Non-critical <subject key identifier CA>
authorityKeyIdentifier	Non-critical <CA assigned unique number>

7.2.1 Version number(s)

See section 7.2.

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

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

7.2.2 CRL entry extensions

See section 7.2.

7.3 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported. 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.

The OCSP response is signed as described and ruled in the present LuxTrust CPS.

7.3.1 Version number(s)

See section 7.3.

7.3.2 OCSP extensions

See section 7.3.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

With regards to the provision of LuxTrust Normalised Certificates (LCP, NCP & NCP+), LuxTrust S.A. acting as CSP through its LuxTrust Normalised CA operates:

- Following the terms of the Grand-Duchy of Luxembourg law of 14 august 2000 on electronic commerce as modified. This law is based on European Directive on electronic signatures 1999/93/EC and lays out the legal framework of electronic signatures in the Grand-Duchy of Luxembourg,
- According to the ETSI technical standard TS 102 042 “Policy requirements for certification authorities issuing public key certificates” [4],
- According to the present LuxTrust CPS and the applicable CP.

With regard to the provision of LuxTrust Qualified Certificates (QCP & QCP+), LuxTrust S.A. acting as CSP through its LuxTrust Qualified CA operates:

- Following the terms of the Grand-Duchy of Luxembourg law of 14 august 2000 on electronic commerce as modified. This law is based on European Directive on electronic signatures 1999/93/EC and lays out the legal framework of electronic signatures in the Grand-Duchy of Luxembourg,
- According to the ETSI technical standard TS 101 456 “Policy requirements for certification authorities issuing qualified certificates” [3],
- According to the present LuxTrust CPS and the applicable CP.

With regard to the provision of LuxTrust Time Stamping Services, LuxTrust S.A. acting as TSSP through its LuxTrust TSA(s) operates:

- Following the terms of the Grand-Duchy of Luxembourg law of 14 august 2000 on electronic commerce as modified, when applicable,
- According to the ETSI technical standard TS 102 023 “Policy requirements for time-stamping authorities” [6],
- According to the present LuxTrust CPS and the applicable LuxTrust Time Stamping Policy [12].

LuxTrust S.A. acting as CSP accepts compliance audit for its LuxTrust TSAs, LuxTrust CAs and all its supporting certification services to ensure they meet the ILNAS requirements for the voluntary “Accreditation 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.

LuxTrust issues qualified electronic certificates as of June 15th, 2008. LuxTrust is accredited by ILNAS acting as accreditation entity. The Accreditation Certificate, issued on Tuesday, October 13th, 2009, testifies that LuxTrust conforms to the following technical standards:

- ETSI TS 101 456 on Policy requirements for certification authorities issuing qualified certificates [3] ;
- ETSI TS 102 042 on Policy requirements for certification authorities issuing public key certificates [4], and
- ETSI TS 102 023 on Policy requirements for time-stamping authorities [6].

The Accreditation Certificate is registered under the reference N° 8/005. The national registry of Accredited Certification Service Providers is publicly available on the ILNAS website www.ilnas.lu.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

LuxTrust S.A. may charge fees for the provision, usage and validation of LuxTrust Certificates and related Certificate services, notably for:

- 9.1.1 Signing Server Certificate issuance or renewal fees.
- 9.1.2 Token mailing service at re-key
- 9.1.3 Revocation or all other Certificate status change
- 9.1.4 Registration data change (not possible in the context of certified data)
- 9.1.4 Fees for other services, as specified from time to time in updated versions of the present CPS, such as:
  - Repositories access fees: None for the time being, but this might be subject to changes in the future depending on several factors.
  - Time Stamping Services fees: None for the time being, but this might be subject to changes in the future depending on several factors
- 9.1.5 Refund policy: not applicable

9.2 Financial responsibility

9.2.1 Insurance coverage

Each PKI Participant not being a Subscriber or a Relying Party of the LuxTrust PKI shall contract an insurance policy covering the risks identified in the Insurance Policy with respect to their services and maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

In particular, CSP, TSA, CA, CRA, (L)RA networks, SRA, (S)SCD services providers and other LuxTrust PKI services providers shall subscribe and bear the costs for own insurance coverage in order to cover their liabilities and duties in performance of their tasks.

LuxTrust S.A. acting as CSP may request documentary evidence of such insurance coverage.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 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 present LuxTrust CPS.

LuxTrust S.A. acting as 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.

9.4 Protection of personal information

LuxTrust S.A. acting as CSP operates within the boundaries of the Grand-Duchy of 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 CSP 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.

9.5 Intellectual property rights

All title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognised in any jurisdiction (the IP Rights) in and to LuxTrust's technology, web sites, documentation, products and services (the Proprietary Materials) are owned and will continue to be exclusively owned by LuxTrust S.A. and/or its licensors. LuxTrust's contractors and / or subcontractors agree to make no claim of interest in or to any such IP Rights. LuxTrust's contractors and / or subcontractors acknowledge that no title to the IP Rights in and to the Proprietary Materials is transferred to them and that they do not obtain any rights, express or implied, in any Proprietary Materials other than the rights expressly granted in the CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

LuxTrust S.A. acting as CSP through its LuxTrust CAs issues X509 v3-compatible Certificates (ISO 9594-8).

The LuxTrust Normalised CA (LTNCA) issues Certificates compliant with ETSI TS 102 042 [4] requirements. To this end, the LTNCA publishes the elements supporting this statement of compliance. The LuxTrust Qualified CA (LTQCA) issues Certificates compliant with ETSI TS 101 456 [3] Qualified Certificates requirements. To this end, the LTQCA publishes the elements supporting this statement of compliance.

LuxTrust S.A. guarantees that all the requirements set out in the applicable CP (and indicated in the Certificate in accordance with Section 7.1) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with the LuxTrust CPS.

To register persons applying for a Certificate, the LuxTrust CAs use a list of approved RAs as indicated in the applicable CP.

The sole guarantee provided by the LuxTrust S.A. acting as CSP through one of its CAs is that its procedures are implemented in accordance with the LuxTrust CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the relevant provisions of the applicable CP, the verification procedures, and the LuxTrust CPS as applicable at the time of issuance. In addition other warranties may be implied in the applicable CP definition by operation of law.

As far as the issuance of non-Qualified Certificates is concerned, only the relevant articles of the Grand-Duchy of Luxembourg law of August 14th, 2000 on electronic commerce as modified govern the liability of the CA (i.e., LuxTrust S.A. acting as CSP).

In certain cases described in the present CPS, LuxTrust S.A. acting as CSP may revoke or suspend the Certificate, provided it informs the Subscriber (and any other concerned authorised party, if applicable) of the Certificate in advance by appropriate means.

LuxTrust S.A. acting as CSP guarantees that each Key pair created by the CSP for a Subscriber is generated in a secure way and that the private character of the Private Key of the Subscriber is guaranteed in accordance with the requirements set out in the technical standard ETSI TS 102 042 [4] or ETSI TS 101 456 [3] as applicable.

LuxTrust S.A. acting as CSP guarantees that it will provide a SCD (NCP/QCP) or SSCD (NCP+/QCP+) in a secured way and in accordance with the requirements set out in the technical standard ETSI TS 102 042 [4] or ETSI TS 101 456 [3] as applicable. The Key pair will be created via this device.

The RAs warrant that they perform their duties in accordance with applicable sections of this CPS, the applicable CP and the internal procedures and guidelines (see next section).

9.6.2 RA representations and warranties

The RA is under a contractual obligation to comply scrupulously with the LuxTrust CPS, with the relevant section of the applicable CP (e.g., but not limited to sections 4.1.2), and with the RA relevant LuxTrust internal procedures.

9.6.3 Subscriber representations and warranties

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 present CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the present CPS and the applicable CP (e.g., but not limited to, 1.3.3, 1.4, 4, 4.1.2.3, 4.5.1, 9).

In particular, the Subscriber is liable towards Relying Parties for any use that is made of his/her (S)SCD, 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.

9.6.4 Relying Party representations and warranties

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 (in particular section 4.5.2 of the present CPS).
- Decision to rely on a certificate must always be a ***conscious*** one and can only be taken by ***the Relying Party itself***.
- Therefore, ***before deciding to rely on a certificate it is needed to 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.***
- See also relevant section 4.5.2 of the present CPS.
- 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.

9.6.5 Representations and warranties of TSA

The TSA shall ensure that all requirements on TSA, as detailed in clause 7 of the technical standard ETSI TS 102 023 [6], are implemented as applicable to the LuxTrust Time Stamping Policy [12].

The TSA shall ensure conformance with the procedures prescribed in the present CPS and the LuxTrust Time Stamping Policy [12], even when the TSA functionality is undertaken by sub-contractors.

The TSA shall also ensure adherence to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

The TSA shall provide all its time stamping services consistent with its practice statement.

The TSA shall meet its claims as given in its terms and conditions including the availability and accuracy of its service as described in the LuxTrust Time Stamping Policy [12].

9.6.6 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

9.7.1.1.1 Damages covered and disclaimers

Except as expressly provided elsewhere in the present CPS, the applicable CP and in the applicable legislation, LuxTrust S.A. acting as CSP (including TSSP activities) 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, TST or message. LuxTrust S.A. does not warrant any software.

9.7.1.1.2 Loss limitations

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

a) 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 (including time stamping services) offered or contemplated by the present CPS even if LuxTrust S.A. has been advised of the possibility of such damages.

b) 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, or TST.

c) 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 (or TST) 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.

d) By accepting a Certificate (TST), 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 (respectively issuing of a TST) 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 (TST);
- 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.

9.8 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 present 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.

9.9 Indemnities

LuxTrust S.A. acting as CSP assumes no financial responsibility for improperly used Certificates, CRLs, TST, etc.

9.10 Term and termination

The present CPS remains in force until notice of the opposite is communicated by LuxTrust S.A. acting as CSP on its repository under http://repository.luxtrust.lu. Notified changes are appropriately marked by an indicated version.

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the present CPS shall be in writing and shall be sent, except provided explicitly in the present CPS, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognised "overnight" or express courier service, (iii) hand delivery (iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or (v) an advanced electronic signature based on a Certificate and a (secure) signature creation device ((S)SCD) and be addressed to:

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*

9.12 Amendments

9.12.1 Procedure for amendment

The LuxTrust S.A. via its CSP Board is responsible for approval and changes of the present CPS.

The only changes that the LuxTrust CSP Board may make to these CPS specifications without notification are minor changes that do not affect the assurance level of this CPS, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document shall be communicated to the contact of the LuxTrust CSP Board as identified in the present CPS. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.

LuxTrust S.A. via its LuxTrust CSP Board shall accept, modify or reject the proposed change after completion of a review phase.

9.12.2 Notification mechanism and period

All changes to the present CPS under consideration by the LuxTrust CSP Board shall be disseminated to interested parties for a period of minimum 14 days. Proposed changes to the present CPS will be disseminated to interested parties by publishing the new document on the LuxTrust CSP Board web site (https://repository.luxtrust.lu/). The date of publication and the effective date are indicated on the title page of the present CPS. The effective date will be the date at which the CPS is published.

9.12.3 Circumstances under which OID must be changed

All changes to the present CPS, other than editorial or typographical corrections, or changes to the contact details, will be subject to an incremented version of the Object Identifier for the present CPS.

Minor changes to this CPS do not require a change in the CPS OID or the CPS pointer qualifier that might be communicated by the CA. Major changes that may materially change the acceptability of Certificates for specific purposes may require corresponding changes to the CPS OID or CPS pointer qualifier.

Minor changes are indicated by version number that contains a decimal number e.g., version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major changes.

9.13 Governing law and jurisdiction

The CPS shall be governed by, and construed in conformity with, the laws of the 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.

9.14 Compliance with applicable law

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

9.15 Miscellaneous provisions

LuxTrust S.A. acting as CSP incorporates by reference, through its LuxTrust CAs, the following information in all Certificates it issues:

- Terms and conditions described in the applicable CP and in the LuxTrust CPS;
- Any other applicable Certificate Policy as may be stated in an issued Certificate;
- The mandatory elements and any non-mandatory but customised elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a Certificate.

LuxTrust S.A. acting as TSSP as part of CSP activities may incorporate by reference, through its LuxTrust TSAs, appropriate information in all TSTs it issues, including but not limited to the LuxTrust Time Stamping Policy [12], and the present CPS.

To incorporate information by reference LuxTrust S.A. through its CAs / TSAs uses computer-based and text based pointers that include URLs, OIDs, etc.