LUXTRUST
Enabling a digital world

LuxTrust Qualified TS CA
Certification Practice Statement

Version number: **1.00**
Publication Date: **26.01.2024**
Effective Date: **09.02.2024**

Document O.I.D:
1.3.171.1.1.1.16
1.3.171.1.1.1.17

LuxTrust S.A.
13-15, Parc d'activités
L-8308 Capellen, Luxembourg

VAT LU 20976985
RCS B112233
Business Number N°00135240/5

+352 26 68 15 – 1
info@luxtrust.lu
www.luxtrust.com

Document Information

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

Version History

Version	Who	Date	Reason of modification
1.0	YNU	27/11/2023	First version

Table of content

DOCUMENT INFORMATION 2
VERSION HISTORY 2
TABLE OF CONTENT 3
INTELLECTUAL PROPERTY RIGHTS 4
REFERENCES 5
1 INTRODUCTION 6
1.1 OVERVIEW 6
1.2 DOCUMENT NAME AND IDENTIFICATION 7
1.3 PKI PARTICIPANTS 7
1.4 CERTIFICATE USAGE 9
1.5 POLICY ADMINISTRATION 9
1.6 DEFINITIONS AND ACRONYMS 12
1.7 RELATIONSHIP WITH THE EUROPEAN EUROPEAN REGULATION 910/2014 17
2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES 18
2.1 IDENTIFICATION OF ENTITIES OPERATING REPOSITORIES 18
2.2 PUBLICATION OF CERTIFICATION INFORMATION 18
2.3 TIME OF FREQUENCY OF PUBLICATION 19
2.4 ACCESS CONTROL ON REPOSITORIES 19
3 IDENTIFICATION AND AUTHENTICATION 20
3.1 NAMING 20
3.2 INITIAL IDENTITY VALIDATION 21
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY & UPDATE REQUESTS 21
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 22
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 23
4.1 CERTIFICATE APPLICATION 23
4.2 CERTIFICATE APPLICATION PROCESSING 24
4.3 CERTIFICATE ISSUANCE 24
4.4 CERTIFICATE ACCEPTANCE 24
4.5 KEY PAIR AND CERTIFICATE USAGE 25
4.6 CERTIFICATE RENEWAL 26
4.7 CERTIFICATE RE-KEY 26
4.8 CERTIFICATE MODIFICATION 26
4.9 CERTIFICATE REVOCATION 26
4.10 CERTIFICATE STATUS SERVICES 28
4.11 END OF SUBSCRIPTION 29
4.12 KEY ESCROW AND RECOVERY 29
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 30
5.1 PHYSICAL CONTROLS 30
5.2 PROCEDURAL CONTROLS 32
5.3 PERSONNEL CONTROLS 33

5.4 AUDIT LOGGING PROCEDURES 35
5.5 RECORDS ARCHIVAL 36
5.6 KEY CHANGEOVER 37
5.7 COMPROMISE AND DISASTER RECOVERY 37
5.8 CA, RA TERMINATION 39

6 TECHNICAL SECURITY CONTROLS 40

6.1 KEY PAIR GENERATION AND INSTALLATION 40
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 44
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 48
6.4 ACTIVATION DATA 48
6.5 COMPUTER SECURITY CONTROLS 48
6.6 LIFE CYCLE TECHNICAL CONTROLS 48
6.7 NETWORK SECURITY CONTROLS 49

7 CERTIFICATE AND CRL PROFILES 50

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 51

9 OTHER BUSINESS AND LEGAL MATTERS 52

9.1 FEES 52
9.2 FINANCIAL RESPONSIBILITY 52
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 52
9.4 PROTECTION OF PERSONAL INFORMATION 52
9.5 INTELLECTUAL PROPERTY RIGHTS 53
9.6 REPRESENTATIONS AND WARRANTIES 53
9.7 DISCLAIMERS OF WARRANTIES 54
9.8 LIMITATIONS OF LIABILITY 55
9.9 INDEMNITIES 56
9.10 TERM AND TERMINATION 56
9.12 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 57
9.13 AMENDMENTS 57
9.14 GOVERNING LAW AND JURISDICTION 58
9.15 COMPLIANCE WITH APPLICABLE LAW 58
9.16 MISCELLANEOUS PROVISIONS 58

Intellectual Property Rights

References

[1] Regulation (EU) N°910/2014.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

[3] ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[4] Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique.

[5] LuxTrust SelfSigned CA - Certificate Profiles latest version in force available on LuxTrust site[6]

[6] ETSI EN 319 411-1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements.

[7] ETSI EN 319 421 “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

1 Introduction

1.1 Overview

1.1.1 *The LuxTrust project*

The LuxTrust project was created in the form of a Trusted Service Provider (hereafter also "TSP"), with an international reach, aiming to establish a national expertise centre for Luxembourg. LuxTrust as TSP 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 Trust Service Provider ("TSP") as defined in the Luxembourg Law of 17/07/2020 on electronic commerce as amended itself derived from the European Regulation N°910/2014. Before mentioned law and regulation set out the legal framework for electronic signatures in the Grand Duchy of Luxembourg as well as for LuxTrust activities as TSP.

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

LuxTrust services are in line with the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS).

1.1.2 *Purpose of the LuxTrust PKI*

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

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

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

1.1.3 *LuxTrust PKI Hierarchy*

LuxTrust S.A., acting as a "TSP" as described in the Luxembourg Law of 17/07/2020 on electronic commerce as amended, is using several Certification Authorities (CAs) to issue LuxTrust end-user certificates.

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 anyone of its CAs, as described in section 1.3.

This responsibility and liability are still valid when LuxTrust S.A., acting as a TSP 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.

1.1.4 *The present document*

The present document is the LuxTrust S.A. public statement of the practices followed by the LuxTrust Qualified TimeStamping (TS) CA when issuing certificates, and is therefore named the "LuxTrust Qualified TS CA Certification Practice Statement" or "LT QTSCA CPS". Throughout this document, the use of the term "CPS" refers to the present document, unless otherwise specified.

The purpose of the CPS is to describe:

- Practices that are common to all certificate types (or policies) and that are related to all certificate life cycle services (e.g., issuance, management, revocation, renewal or re-keying, etc.) issued by the CA LT QTSCA-EC and LT QTS CA-RSA
- 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 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.

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 ETSI standards. Issued LuxTrust certificates shall include the OIDs of the CPs or CPS to which they comply. The referred to applicable CP shall always refer and include by reference the CPS.

1.2 Document name and identification

The CPS can be identified by any party through the following OIDs:

1.3.171.1.1.1.16: LuxTrust Qualified TimeStamping CA-EC
1.3.171.1.1.1.17: LuxTrust Qualified TimeStamping CA-RSA

1.3 PKI Participants

The LuxTrust PKI Participants are the legal entities or set of legal entities filling the role of participants 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 TSP 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
    - (Qualified) Signature Creation Device (QSCD) Providers
    - Certificate Revocation Status Services Provider
    - Suspension Revocation Authority
    - Dissemination (Publication) and Repository Services

- Time Stamping Services

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.
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*

For issuing certificates, the LT QTS CA uses a self-signed Certification Authority (CA) that directly issues end-entity certificates. The legal person (organization) responsible for this CA is LuxTrust S.A. acting as a CSP.
LuxTrust S.A. acting as CSP ensures the availability of all services pertaining to the LTQTSCA including issuance, revocation and renewal services.
Technical management and operations of the LT QTS CA are compliant with the CPS and provided through a CA Factory Services provider supporting disaster recovery capabilities within secure facilities in the Grand Duchy of Luxembourg.

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

This is also certified by a CAB against ETSI EN 319 411 1 and EN 319 421 in application of the Luxembourg Law of 17/07/2020 on electronic commerce as amended. For further details please refer to section 8 of the CPS.

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 LT QTS CA only issues certificates for the LuxTrust time-stamping service. In this context, only LuxTrust is the RA authorised to manage the life cycle of the dedicated certificate.

1.3.3 *Relying Parties*

Cf. 5.3 of the latest LuxTrust_Time_Stamping_V2_Policy.

1.3.4 *Other Participants*

1.3.4.1 **CA Factory Services Provider**

The provision of CA Factory Services under the CPS, in compliance with the relevant LuxTrust CPs is ensured by the external providers supporting LuxTrust activities under a signed contractual agreement with LuxTrust S.A. acting as TSP.

1.3.4.2 **(Qualified) Signature/Seal Creation Device Provider**

The provision of physical end-user (Qualified) Signature/Seal Creation Device QSCD Services is ensured by LuxTrust S.A. and the external providers supporting LuxTrust activities under a signed contractual agreement with LuxTrust S.A. acting as TSP.

1.3.4.3 **Certificate revocation status Services Provider**

The provision of Certificate Revocation Status Services under the CPS, in compliance with the relevant LuxTrust CPs is ensured by the external providers supporting LuxTrust activities under a signed contractual agreement with LuxTrust S.A. acting as TSP.

1.3.4.4 **Revocation Authority**

The provision of Revocation Authority Services under the CPS, in compliance with the relevant LuxTrust CPs is ensured by the external providers supporting LuxTrust activities under a signed contractual agreement with LuxTrust S.A. acting as TSP

1.3.4.5 Dissemination (Publication) and Repository Services

The Dissemination Services (publication of CPS, CP's, General Terms and Conditions, and other public LuxTrust TSP related documents if any) are available from the official LuxTrust TSP Web Site available in https://repository.luxtrust.com. 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 CPS.

1.4 Certificate usage

1.4.1 *Appropriate certificate uses*

Appropriate certificate uses of Certificates issued under a specific CP covered by the 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.

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

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 and chapter 7 of the CPS or in the applicable CP is prohibited.

Relying Parties shall use the LuxTrust Certificate Policy Notice and OID as identified in the Certificate to appropriately accept or reject a Certificate usage.

1.5 Policy administration

1.5.1 *Organisation administering the CPS*

The Organisation administering the CPS is LuxTrust S.A. acting as Trusted Service Provider (TSP) 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 Practice Statements and Certificate.
- Defining the review process that ensures that the LuxTrust CAs properly implements the above practices.
- Defining the review process that ensures that the Certificate Policies are supported by the LuxTrust Practice Statement(s).

- Publication to the Subscribers and Relying Parties of the Certificates Policies and Certification 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.com.

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.com*

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 TSP, 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 CPS and the covered CPs is LuxTrust S.A. acting as TSP, 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	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.
Centre	Information Technology Centre of the State
Certification Authority (CA)	Authority trusted by one or more users to create and assign certificates. A certification authority may optionally create the users' keys.
Certificate	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)	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. (cf. Ch. 7)
Certification Practice Statement	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)	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certification Path	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	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).
Device	Combination of the key pair, the corresponding certificate and secured user device

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 Regulation: means data in electronic form that are attached to or logically associated with other electronic data. – 17/07/2020 Luxembourg Law : 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	Certificate which meets the requirements laid down in Annex I of eIDAS regulation
Public RA	Publicly accessible RA to all potential LuxTrust client
Private RA	RA dedicated to a closed user group

Secure User Device	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	Refers to unique data, such as codes or private cryptographic keys used by the signatory to create an electronic signature.
Signature Creation Device	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	Data, such as codes or public cryptographic keys used for the purpose of verifying an electronic signature.
Signature-Verification Device	Configured software or hardware used to implement the signature verification-data.
Signatory	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 TSP 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.
Trust Service Provider (TSP)	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
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 (TSA)	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.

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	Acronym	Definition
AES	Advanced Electronic Signature	**PIN**	Personal Identification Number
ARL	Authority Revocation List	**PKI**	Public Key Infrastructure
B2B	Business to Business	**PKIX**	Public Key Infrastructure (X.509) (IETF Working Group)
CA	Certification Authority	**PKCS**	Public Key Certificates Standard
CME	Cryptographic Module Engineering	**PSF**	Professionnel du Secteur Financier (PSF – Professional of the Financial Sector)
CP	Certificate Policy	**QES**	Qualified Electronic Signature
CPS	Certification Practice Statement	**QCP**	Qualified Certificate Policy
CRL	Certificate Revocation List	**RA**	Registration Authority
CSP	Certification Service Provider	**RAO**	Registration Authority Officer
DSA	Digital Signature Algorithm	**RFC**	Request for Comments
EC	Family of public-key cryptosystems, which is based on the algebraic structures of the elliptic curves over finite fields.	**RSA**	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
HSM	Hardware Security Module	**SCD**	Signature Creation Device
IETF	Internet Engineering Task Force	**SRA**	Suspension and Revocation Authority
ISO	International Organisation for Standardisation	**SRAO**	Suspension and Revocation Authority Officer
ITU	International Telecommunications Union	**SSCD**	Secure Signature Creation Device
KYC	Know Your Customer	**TSA**	Time Stamping Authority
LCP	Lightweight Certificate Policy	**TSP**	Trusted Service Provider
LDAP	Lightweight Directory Access Protocol	**TSSP**	Time Stamping Service Provider
NCP	Normalised Certificate Policy	**TSU**	Time Stamping Unit
NCP+	Normalised Certificate Policy +	**URL**	Uniform Resource Locator
OID	Object Identifier	**UTC**	Coordinated Universal Time
OCSP	Online Certificate Status Protocol		

1.7 Relationship with the European European Regulation 910/2014

The LT QTS CAs are certified by a CAB respectively against EN 319 411-1 and EN 319 421 in application of the Luxembourg Law of 17/07/2020 on electronic commerce as amended. This law is based on European Regulation 910/2014 (eIDAS) and lays out the legal framework of electronic signatures in the Grand Duchy of Luxembourg. The LuxTrust Global Qualified CA is listed as granted by ILNAS, the Luxembourg public standardisation service, as a Trusted Service Provider (TSP) under number 2018/8/001.

In the context of eIDAS regulation, ILNAS is the national supervisory body, which is responsible for undertaking supervision of LuxTrust under the regulation N°910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (supervision procedure). LuxTrust is certified by a Certification Accredited Body (CAB).

2 Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

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

- The CPS (Certification Practice Statement);
- The covered CPs (Certificate Policies);
- 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 aforementioned documents as well as complementary information are available from online publicly accessible website accessible on https://repository.luxtrust.com as described in section 2.2. Note: published documents and information can be physically available and managed on repositories that are technically operated by the external providers supporting LuxTrust activities.

2.2 Publication of Certification Information

LuxTrust S.A. acting as TSP, 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.com. This repository shall also contain any other public documents where LuxTrust S.A. acting as TSP makes certain disclosures about its practices, procedures and the content of certain of its policies, including the CPS, and the covered CPs. It reserves right to make available and publish information on its policies by any means it sees fit.

This service is available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the LuxTrust S.A, LuxTrust S.A. shall make best endeavours to ensure that this service is not unavailable for longer than 5 days.

LuxTrust publishes the digital Certificates in (an) online publicly available repositories(y). LuxTrust S.A., acting as TSP, reserves right to publish Certificate status information on third party repositories.

The CA publishes revocation status information as indicated in section 4.9 of the CPS:

- CRLs are published at regular intervals.
- an OCSP responder server at http://qtsca.ocsp.luxtrust.lu provides notice on the status of a Certificate issued by the CA, upon request from a Relying Party, in compliance with the IETF RFC 6960.

Note: 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.

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

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

- The CPS (Certification Practice Statement);
- The covered CPs (Certificate Policies);
- 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 aforementioned documents as well as complementary information are available from online publicly accessible website accessible on https://repository.luxtrust.com as described in section 2.2. Note: published documents and information can be physically available and managed on repositories that are technically operated by the external providers supporting LuxTrust activities.

3 IDENTIFICATION AND AUTHENTICATION

3.1 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.

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).

Within the LT QTS CA domain, the LuxTrust TSP is only authorised to issue the following names in the CA Certificates it issues.

LuxTrust Qualified TimeStamping CA Certificate	
Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust Qualified Timestamping CA ECx[1] or LuxTrust Qualified Timestamping CA RSAx[1]

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).

3.1.3 *Anonymity or pseudonymity of Subscribers*

This is not applicable for the LT QTS CA.

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 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*

All trademarks, products and services marks, trade name and firm name within the meaning of the Law Approving the Benelux Convention on Intellectual Property (Trademarks and Designs), signed at The Hague, February 25, 2005 (Mem. 2006, 1738 (2006)) 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.

[1] x is a positive sequential value to distinguish the old CA from the renewed CA. The value 1 is omitted as it is the first CA issued.

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.

3.2 Initial identity validation

Initial Identity validation is part of the certificate application process described in chapter 4.1. Initial identity validation procedures for PKI Participants or organisation of PKI Participants other than Subscribers, comply with provisions of the CPS (and in particular with section 5.2.1) and are fully detailed in LuxTrust S.A. internal documents.

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 CPS and the applicable CP).

3.2.1 *Method to prove possession of private key*

The key generation process is ensured by the TSP it is done in compliance with the ETSI EN 319 401, ETSI EN 319 411-1 and technical standard. In that case, the private key activation data may be sent to the Certificate Subject through out-of-band mechanisms.

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 organisation in the Grand Duchy of Luxembourg.

LuxTrust is the only entity authorised to request and receive a certificate issued by this CA. In this context. LuxTrust has all the internal data required to guarantee its identity on the basis of official documents such as

- Recent constitutive act, or recent extract of the commercial register (or the foreign equivalent for foreign companies registered under foreign law;
- 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.);
- 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;
- The information about their legal address, civil state, and profession;

3.2.3 *Non-verified subscriber information*

Not applicable.

3.2.4 *Validation of authority*

Not applicable.

3.2.5 *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 CPS and are fully detailed in LuxTrust S.A. internal documents, including applicable CP for PKI Participants other than Subscribers.

The processes associated to revocation are detailed in section 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All PKI Participants within the CAs domains, including the Relying Parties, are subject to 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 for proper correction of the affected information (including revocation of the Certificate if applicable), ensuring that accurate and correct information is kept by the CA.

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, applications for end-entity certificates can be submitted only by LuxTrust which complies with provisions set within the registration forms and processes, the CP/CPS and the LuxTrust end-user agreement. The CA issues or revokes Certificates only at authenticated request of LuxTrust S.A. acting as TSP, to the exclusion of any other entity, unless explicitly instructed so by the TSP.

4.1.2 *Enrolment process and responsibilities*

LuxTrust is the only entity authorised to request and receive a certificate issued by this CA. The registration process is documented internally. A dedicated report on the progress of the process is issued each time a certificate is issued. This report mentions the roles and responsibilities of the internal parties involved in this process.

At time of registration, the RA performs the Subscribers identification and authentication and guarantees the accuracy at the time of registration of all information contained in the certificate request of all information contained in the certificate. The RA 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 Certificate issuance.

Upon successful validation, the RA combines and securely archives all the submitted documents and uses the RA Interface to send the certificate request to the CA.

4.1.2.1 **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 EN 319 411-1.

4.1.2.1.1 RA enrolment process

Only LuxTrust acting as TSP is entitled to perform registration operations. LuxTrust, as RA and its Officers (RAOs) must:

- Be part of LuxTrust S.A.;
- Attest 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;
- Undergo continuing education.

4.2 Certificate application processing

4.2.1 *Performing identification and authentication functions*

The Certificate Subscriber has already been identified, by the RA, as described in section 3.2 of the CPS,

4.2.2 *Approval or rejection of certificate applications*

Upon successful validation of the Subscriber registration, the RA sends the Certificate request to LT QTSA CA and requests the issuing authority for the generation of the certificate as well as other components if required.

When the application for the Certificate is rejected by the RA, 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.

CAs issuing end-entity certificates validate and ensure 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), 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 CAs authenticate the signed certificate requests and only accept requests sent by the LuxTrust RA.

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 CPS.

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 TSP Public Repository of Certificates (if applicable) 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 TSP of any inconsistency the Subscriber has noted between the information in the Subscriber Agreement and the content of the Certificate.

In case of objections to accepting an issued Certificate, a request is sent to 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 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*

The Certificate is published in the LuxTrust Public Repository of Certificates (https://repository.luxtrust.com). This repository is in the public domain and is accessible at all times as stated in Section 2 of the CPS.

4.4.3 *Notification of Certificate issuance by the CA to other entities*

The certificate issuance is notified by the CA to other entities through the publication of the Certificate in the LuxTrust Public Repository of Certificates (https://repository.luxtrust.com), available in the public domain and accessible at all times as stated in Section 2 of the 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*

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 has sole liability for the use of the Private Key.
- 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 and the LuxTrust CPS.
- The Subscriber must ask the TSP 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[2]; 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 revocation process and procedures are set out in Section 4.9 of the CPS.
- The Subscriber must inform the TSP of any changes to data not included in the Certificate but submitted and registered during the enrolment process. The TSP then rectifies the registered data.

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 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, compliant with RFC 5280.
- 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),

[2] 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).

- Un-trust a Certificate if it has expired or is 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.
- 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

Certificate re-key process shall be identical to the original initial certification process. When a certificate is renewed, the private key is changed. The goal of the rekey is to align a subject's certificate public key with his/her new private key. All the other fields are kept unchanged.

See applicable CP for possible further details.

4.8 Certificate modification

The Subscriber must immediately inform LuxTrust S.A. acting as Certification Services Provider of any changes to the data on the Certificate, or when the certified data has become inaccurate or has changed in any way. The Subscriber must ask the TSP to revoke the Certificate. The Certificate revocation process is then started immediately. The revocation procedures are set out in Section 4.9 of the CPS.

In case the Subscriber wants to change the certified information, the Subscriber shall process to a full Certificate application as following the initial certification process (see section 4.1 of the CPS).

4.9 Certificate revocation

The revocation processes are managed by the LuxTrust RA.

A Certificate status can be valid or revoked. 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 CPS.

LuxTrust S.A. may apply for 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 revocation of the Certificate.

Revocation status information is made available beyond the validity period of the certificate.

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 TSP 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 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 RA directly will request the revocation of a Certificate after having received notice by the Subscriber, or when applicable, by the Subscriber's organisation.

4.9.2 *Who can request revocation*

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

Under specific circumstances, LuxTrust S.A. acting as TSP may request revocation of any Certificate in accordance with the CPS.

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

4.9.3 *Procedure for revocation request*

The revocation will be performed according to internal procedures that include dual control and prior approval of the CSPBOARD.

4.9.4 *Revocation request grace period*

LuxTrust S.A. acting as TSP 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. The precise issuance time of the revocation data is specified in section 7 of the present document.

4.9.5 *Time within which CA must process the revocation request*

The revocation service is available 24 hours a day, 7 days a week. Upon authentication and validation of the request, the revocation service requests revocations or suspensions via the RA towards the CA.

There is a maximum period of 24 hours between the receipt of a certificate revocation request and the publication of the revoked status of the corresponding 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 **CRLs**

A CRL is issued on a periodical basis at an agreed time. CRLs are signed and time-marked by the CA response. The validity period is defined in section 7 of the present CPS.

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 CPS.

4.9.7.2 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 of the CPS). 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 http://qtsca.crl.luxtrust.lu/LTQTSCA-XX[3]-1.crl.
- OCSP service is available from http://qtsca.ocsp.luxtrust.lu.

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. Revocation status of an expired certificate

The revocation status of an expired certificate is available through the LuxTrust OCSP service.

4.9.10 *On-line revocation checking requirements*

See section 4.9.6 of the CPS.

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 CPS).

4.9.12 *Special requirements regarding key compromise*

Not applicable.

4.10 Certificate status services

4.10.1 *Operational characteristics*

See section 4.9.7 of the CPS.

[3] RSA or EC

4.10.2 *Service availability*

See section 4.9.9 of the CPS.

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 disaster recovery as stated and ruled by the 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 qualified CAs 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, , auditing and archiving are compliant with the following technical standards:

- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

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 TSP including activities , provides direction on information security through its CSP Board, responsible for defining the TSP'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 TSP, 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 27002.

5.1 Physical controls

LuxTrust S.A. acting as TSP 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 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.

Detailed descriptions of the secure sites and premises that are used by LuxTrust S.A. to provide certification 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 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, Certificate Revocation Status 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 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)), Revocation Services.

- **Secure areas for Local Registration Authorities**: RA(O)s operate in areas equipped to meet the requirements laid down in section 4.1.2.3 of the 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 TSP 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/or 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 are 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 according to internal CA risk analysis.

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, are 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 TSP, 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 CPS for further details on recovery procedures.

5.2 Procedural controls

The TSP for both CA activities ensures that CA systems are secure and correctly operated with minimal risk of failure in strict compliance with technical standards EN 319 411-1 and EN 319 421 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 TSP obtains a signed statement from each member of the staff on not having conflicting interests with the TSP, maintaining confidentiality and protecting personal data.

All members of the staff operating certificate, key management operations, 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 TSP 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 TSP 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 TSP 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 CPS).

- Trusted or management roles are formally appointed to trusted roles by senior management responsible for compliance or 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 or compliance.

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 functions such as but not limited to key management and in particular CA 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 is 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 TSP ensures that all actions with respect to the LuxTrust certifications services can be attributed to the system of the TSP 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.

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 TSP 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 TSP 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 TSP 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 TSP 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 TSP personnel.

5.3.8 *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 must provide proof of their PSF status (PSF: Professionnel du Secteur Financier – Financial Sector Professional as defined by the Grand Duchy of Luxembourg Law).

Since the Validation Services are to be provided by the CA Factory Services Provider for security reasons, the CA Factory Services Provider must have the “PSF – Agent administratif” status.

5.3.9 *Documentation supplied to personnel*

LuxTrust S.A. acting as TSP makes the relevant documentation or ensures that the relevant documentation is 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 TSP implements or ensures the following controls being implemented:

- All events relating to the life-cycle of CA keys are recorded;
- The LuxTrust CAs event logging systems record events related to certificate lifecycle operations including but not limited to:
    - Subject key generation;
    - Preparation of (Q)SCDs;
    - Issuance of a certificate;
    - Revocation of a certificate;
    - Automatic revocation;
    - Publishing of a CRL;
- All other LuxTrust certification 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 TSP 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, involved in the operation;
    - The identity of the transaction requestor.
- In addition, LuxTrust S.A. acting as TSP 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 TSP 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 TSP 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 TSP keeps internal records or ensures the archival, in a trustworthy manner, of the following items:

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

LuxTrust S.A. acting as TSP keep archives or ensure 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.
Archives are made available to provide evidence of the correct operation of the services for the purpose of legal proceedings.

5.5.2 *Retention period for archive*

See section 5.5.1.

5.5.3 *Protection of archive*

LuxTrust S.A. acting as TSP 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 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 TSP 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.

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

The CA parameters are set so that the expiracy date of an end entity certificate does not exceed the expiracy date of the issuing CA.

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 27001 and ISO/IEC 27002 standard.

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

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

LuxTrust S.A. acting as TSP, 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 27002 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 at least one member of the LuxTrust who provides his report to the 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 TSP, 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,
- LuxTrust S.A. acting as TSP 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 TSP 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 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.

5.7.4 *Business continuity capabilities after a disaster*

LuxTrust S.A. acting as TSP 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 27002 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 termination

LuxTrust S.A. acting as TSP 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 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 TSP complies with the Luxembourg Law of 17/07/2020 on electronic commerce as amended 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 Luxembourg Law of 17/07/2020 on electronic commerce as amended ;
    - 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 TSPs;
    - 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, RA) in the performance of any functions related to the process of issuing certificates.
  - LuxTrust will issue a last CRL with the next Update field set according to IETF RFC 5280.

- 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 TSP at least one (1) month before the effective transfer;
  - LuxTrust S.A. indicates the identity of the TSP 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 TSP, shall destroy, or withdraw from use, its private keys related to the terminated certification (component) services, as described in section 6.2.18 of the 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 CPS).

- In conformity with Law 17/07/2020, LuxTrust S.A. will inform users of the change of status in the Trusted List of its qualified trust services within seven (7) days of the effective date of the change of status .

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.

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, 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 EN 319 411-1
- ETSI EN 319 421

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 Global Qualified CA), repositories, RAs, SRAs, 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 TSP, through the support of the CA Factory services provider, uses a trustworthy process and systems for the generation of its LuxTrust Global 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 TSP according to a documented procedure. The TSP (and the CAs) acknowledges public, international and European standards on trustworthy systems.

LuxTrust S.A. acting as TSP 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, EN 319 411 1 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 TSP,
- a Master of Key Ceremony, and
- at least two independent and external auditors.

This process is witnessed by LuxTrust TSP 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 Qualified Electronic Signature Creation Device (QSCD) meeting appropriate requirements as set forth in section 6.2.1 of the CPS (for CA secure cryptographic devices requirements).

Such secure CA cryptographic devices is prepared, distributed and managed in compliance with the technical standard ETSI EN 319 411-1.

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 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.

Similar rules apply for re-generation and key usage periods for LT QTS CA 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 RA and their respective Officers.

6.1.1.2.1 LuxTrust RA Key generation process

RAOs 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,
- The Registration Authority (Officers) that (who) is in charge of RAOs registration is the authorised members of LuxTrust,

6.1.1.2.2 LuxTrust RA Key generation devices and key storage

The generation and storage of RA private keys of the LuxTrust RA occurs within a secure cryptographic device meeting appropriate security requirements as applicable in the relevant CP. Such devices are 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 EN 319 411-1. See section 6.2.1 of the 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, OCSP validation services provider, etc. is applicable as for RAs for which the applicable rules are the ones as applicable for CAs and are compliant with the technical standard ETSI EN 319 411 1.

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 TSP

The key generation process is ensured by LuxTrust S.A. acting as TSP, generation is performed in compliance with the ETSI EN 319 411 1 & 2 technical specifications. 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 RAO registering the Subscriber (Certificate Subject), as an internal and auditable document (non-identified person).

6.1.1.4.2 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 TSP for generation and storage of LuxTrust Subscribers private keys (and certificates) meet QSCD requirements as available in Annex III of the eIDAS Regulation, 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 devices are, distributed and managed in compliance with the technical standard ETSI 319 411-1.

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

See section 4.7 of the CPS.

6.1.2 *Private Key delivery to Subscriber*

See section 6.1.5 for key generation done by TSP.

6.1.3 *Public key delivery to certificate issuer*

See section 6.1.5 when key generation is done by TSP.

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 thumbprint) 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.com.

- The LuxTrust RAs certified public keys are securely provided to potential Relying Parties using a SSL session from the LuxTrust repository available at https://repository.luxtrust.com.

6.1.5 *Key sizes*

6.1.5.1 LuxTrust CA Private Key Type

For its signature keys the LT QTS CA makes use of the rsassaPss with Hash or ecdsa-with-SHA512 algorithm with appropriate and state-of-the-art key sizes.

6.1.5.2 LuxTrust RA Private Key Type

LuxTrust RA operators are provided with a SSCD with keys with an RSA key length of minimum 3072 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.

6.1.5.4 LuxTrust Subscriber Private Key Type

Subscriber's minimum private key length is RSA 3072 bits or equivalent. Certificate validity period is defined in the applicable CP.

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)*

6.1.8 *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.

Private key of the LT QTS CA is used to sign end-entity certificates, corresponding CRLs. LT QTS CA is an online CA and shall never be used for signing other CA certificates.

6.1.9 *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 RA is only and exclusively used in the RA software in the context of their role in the RA (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 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.

6.1.10 *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 TSP 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 TSP 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 CPS). See section 6.2.1.3 of the 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 EN 319 401
- ETSI EN 319 411-1
- CEN/TS 419 261:2015

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 RA, (Q)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 CPS for further details about such HSM requirements.

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

- ETSI EN 319 401
- ETSI EN 319 411-1
- CEN/TS 419 261:2015

LuxTrust PKI Officers and LuxTrust (Q)SCD Subscribers make use of (Q)SCD whose requirements are provided in section 6.2.1.3 of the CPS.

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.

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 amended version of Luxembourg Law of 17/07/2020 on electronic commerce and the Regulation (EU) N°910/2014). Assessment of such compliance can be made against:

- CWA 14355 : Guidelines for the Implementation of SSCDs.
- CEN/TS 419 261:2015

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 EN 319 411-1.

6.2.1.3.2 LuxTrust Hardware Security Module (HSM) requirements

The LuxTrust HSMs used by CAs in the context of the LuxTrust services provision are secure cryptographic devices meeting at least the requirements of an QSCD as specified by the applicable regulations (e.g., the 17 July 2020 Luxembourg law on e-commerce as modified, and the European Regulation 910/2014).

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 a QSCD as specified by the applicable regulations (e.g., the amended version of Luxembourg Law of 17/07/2020 on electronic commerce, and the European Regulation 910/2014).

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 EN 319 411-1, 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 EN 319 411-1.

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 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 TSP. 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 TSP. 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

LuxTrust S.A. does not perform backup of subscriber secret keys.

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 QSCD by LuxTrust S.A. acting as TSP and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the QSCD.

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

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 Subscriber private keys when provided by LuxTrust S.A. acting as TSP shall be destroyed by any the subject to ensure that these private keys cannot ever be retrieved or used ever again. These Subscriber keys are destroyed by shredding and destroying any hardware modules the keys were stored on.

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 TSP archives its own LuxTrust CA public keys. See section 5.5 of the CPS for archival conditions.

6.3.2 *Subscriber Certificate operational periods and key pair usage periods*

LuxTrust S.A. acting as TSP 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 TSP ensures that activation data associated to LuxTrust CAs 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 QSCD by LuxTrust S.A. acting as TSP and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the QSCD. LuxTrust S.A. acting as TSP 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 TSP, these keys are stored on QSCD and are associated with user activation data (e.g. PIN code) being securely prepared and distributed separately from the QSCD. Subscribers are responsible for the secure management and protection of their activation data.

6.5 Computer security controls

LuxTrust S.A. acting as TSP ensures that computer security controls are implemented in compliance with the technical standard the technical standard ETSI EN 319 411-1 when this standard imposes higher requirements on certification practices. Detailed descriptions of implemented computer security controls are available as internal document(s).

LuxTrust is supervised by ILNAS. The national registry of supervised Trusted Service Providers is publicly available on the ILNAS website http://www.ilnas.public.lu/.

ILNAS is the national supervisory body which supervises LuxTrust under the regulation N°910/2014 of the European parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (http://www.ilnas.public.lu/).

6.6 Life cycle technical controls

LuxTrust S.A. acting as TSP ensures that periodic development control, security management and life cycle security controls are implemented in compliance with the standard ETSI EN 319 411-1 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 TSP 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 standard ETSI EN 319 411-1 when this standard impose higher requirements on certification practices.

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

7 CERTIFICATE AND CRL PROFILES

The CP are composed of the CPS and the document “LuxTrust SelfSigned CA - Certificate Profiles”.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

With regard to the provision of LuxTrust Certificates, LuxTrust S.A. acting as TSP through its LuxTrust Qualified CA operates:

- Following the terms of regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market,
- Following the terms of the amended version of Luxembourg Law of 17/07/2020 on electronic commerce,
- According to the ETSI standard EN 319 411-1,
- According to the present LuxTrust CPS and the applicable CP.

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

The maximum interval between two audits or security checks of the TSP's practices is 12 months.

LuxTrust issues qualified electronic certificates as of June 15th, 2008.

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)
- 9.1.5 Fees for other services, as specified from time to time in updated versions of the 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.
- 9.1.6 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, TSP, CA, RA, QSCD 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 TSP 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 CPS.
LuxTrust S.A. acting as a TSP 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 a TSP operates within the boundaries of the Luxembourg law and the European General Data Protection Regulation (GDPR). Personal data communicated to LuxTrust S.A. by the applicant are kept in a suitably protected file held by the LuxTrust S.A.

9.5 Intellectual property rights

All title, copyrights, , 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.

Without limiting the "all rights reserved" copyright on the CPS, 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.

9.6 Representations and warranties

9.6.1 *CA representations and warranties*

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

The LuxTrust CAs issues Certificates compliant with either, ETSI EN 319 411-1 or ETSI EN 319 421 requirements. To this end, the CA 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) 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 TSP through one of its CAs is that its procedures are implemented in accordance with the 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 CPS as applicable at the time of issuance. In addition other warranties may be implied in the applicable CP definition by operation of law.

In certain cases described in the CPS, LuxTrust S.A. acting as TSP may revoke 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 TSP guarantees that each Key pair created by the TSP 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 standard ETSI EN 319 411-1 or ETSI EN 319 421 as applicable.

LuxTrust S.A. acting as TSP guarantees that it will provide a QSCD in a secured way and in accordance with the requirements set out in the technical standard ETSI EN 319 411-1 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 CPS, with the relevant section of the applicable CP, 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 TSP and setting out the procedures used for providing the Certificates.

The Subscriber agrees to the CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the CPS and the applicable CP.

In particular, the Subscriber is liable towards Relying Parties for any use that is made of his / her QSCD, 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 CPS).
- Decision to rely on a certificate must always be a ***conscious one*** and can only be taken by ***the Relying Party itself based on RFC 5280***.
- Therefore, ***before deciding to rely on a certificate 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*
  - ***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 CPS.
- Without prejudice to the warranties provided in the present CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it. LuxTrust S.A. acting as TSP accepts liability up to an aggregate limit as specified in the general terms and conditions for the concerned service for direct losses, due to non-compliance with this LuxTrust CPS, towards a Relying Party reasonably relying on a Certificate.
- Without prejudice to the warranties provided in the applicable CP or in the LuxTrust CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- If a Relying Party relies on a Certificate without following the above rules, LuxTrust S.A. will not accept liability for any consequences.
- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt.
- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify LuxTrust S.A. acting as TSP.

9.6.5 *Representations and warranties of other participants*

Not applicable.

9.7 Disclaimers of warranties

9.7.1 *Damages covered and disclaimers*

Except as expressly provided elsewhere in the CPS, the applicable CP and in the applicable legislation, LuxTrust S.A. acting as TSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and

further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. LuxTrust S.A. does not warrant “non repudiation” of any Certificate or message. LuxTrust S.A. does not warrant any software.

9.7.2 *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 offered or contemplated by the 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 revoked or expired Certificate.

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 LuxTrust S.A. issues, manages, uses 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, the Subscriber agrees to indemnify and hold LuxTrust S.A. and his agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that LuxTrust S.A. and its agents and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:
   - Falsehood or misrepresentation of fact by the Subscriber;
   - Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive LuxTrust or any person receiving or relying on the Certificate;
   - Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber’s Private Key.

9.8 Limitations of liability

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

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

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

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

9.9 Indemnities

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

9.10 Term and termination

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

9.12 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 CPS shall be in writing and shall be sent, except provided explicitly in the 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 ((Q)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.com*

9.13 Amendments

9.13.1 *Procedure for amendment*

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

9.13.2 *Notification mechanism and period*

All changes to the 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 CPS will be disseminated to interested parties by publishing the new document on the LuxTrust CSP Board web site (https://repository.luxtrust.com). The date of publication and the effective date are indicated on the title page of the CPS.

9.13.3 *Circumstances under which OID must be changed*

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.

9.14 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.com.

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

9.15 Compliance with applicable law

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

The Subscriber shall be compliant with applicable Laws of Grand Duchy of Luxembourg and concretely with Law 17/07/2020 on electronic commerce.

9.16 Miscellaneous provisions

LuxTrust S.A. acting as TSP 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.

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