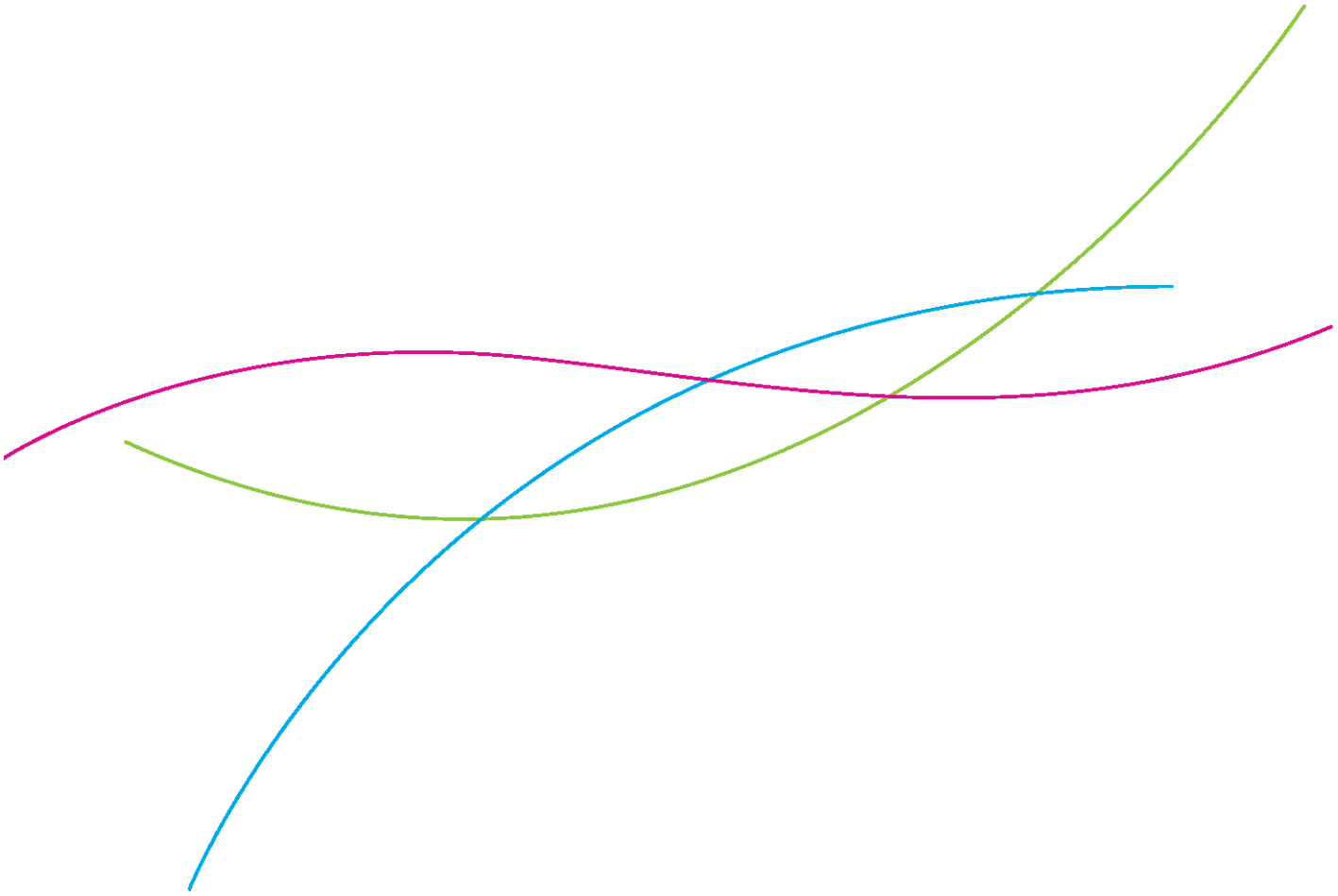

Certification Practice Statement
LuxTrust SSL CA

Version number: **1.7**
Publication Date: **22/03/2019**
Effective Date: **05/04/2019**
Document O.I.D: **1.3.171.1.1.1.10.5**

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

Document Information

Document title:	Certification Practice Statement for LuxTrust SSL CA
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Certification Practice Statement
Document Distribution List	Any
Document Classification	Public
Document Owner	LuxTrust CSP Board

Version History

Version	Who	Date	Reason for modification
1.0	CSP Board	05/12/2013	Initial Version
1.1	YNU	18/01/2014	Add clarification on Mozilla request
1.2	YNU	1/10/2014	Scope updated based on Mozilla request
1.3	YNU	03/11/2015	Update Trademarks section Update section: Procedure for revocation request
1.4	DEL	20/03/2017	Add QWAC certificate profile
1.5	DEL	10/10/2017	Make CAA Checking Mandatory as stated in the CAB Forum
1.6	NDE	24/11/2017	Increase CRL validity from 4h30min to 8h30min
1.7	DEL	19/03/2019	Change FQDN validation method

Table of content

Intellectual Property Rights

References

[1] The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

[3] ETSI TS 102 042 V2.4.1 (2013-02) – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[4] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.

[5] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.

[6] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.

[7] Règlement Grand-Ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».

[8] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[9] LuxTrust Time Stamping Policy. Document OID 1.3.171.1.1.3.1.0, latest version in force.

[10] Guidelines for the Issuance And Management Of Extended Validation Certificates. CA/Browser Forum. Latest version in force.

[11] LuxTrust Central Registration Authority – Procedures & Guidelines for the registration of a new LuxTrust user via RA Software, latest version in force

[12] LuxTrust Global Root CP, latest version in force available on LuxTrust site

[13] LuxTrust Global Root CA, Certification Practice Statement – Document OID: 1.3.171.1.1.1.10.1.00

[14] ILNAS – QTSP Procedure n° 001 – Supervision of Qualified Trust Service Providers (QTSPs).

[15] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, Version 1.6.4

Figures

1 INTRODUCTION

1.1 Overview

1.1.1 The LuxTrust project

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

Established in November 2005 through a partnership between the Luxembourg government and the major private financial actors in Luxembourg, LUXTRUST S.A. was created to become a provider of certification services as defined in the law of the Grand-Duchy of Luxembourg modified on 14/08/2000 [4] itself derived from the European Directive on electronic signatures (1999/93/EC [1]). These laws and directives set out the legal framework for electronic signatures in the Grand-Duchy of Luxembourg as well as for LuxTrust activities as TTP.

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

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) [20].

1.1.2 Goal of the LuxTrust PKI

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

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

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

1.1.3 LuxTrust PKI Hierarchy

LuxTrust S.A., acting as a "Certification Service Provider" (CSP) as described in the Luxembourg Law of 14/08/2000 on electronic commerce as amended [5], is using several Certification Authorities (CAs), as shown in the certificates hierarchy, to issue LuxTrust end-user certificates.

In all (CA-) certificates issued to these CAs, LuxTrust S.A. is referred to as the legal entity being the certificate issuing authority, assuming final responsibility and liability for all LuxTrust CAs and services used by LuxTrust S.A. for provision of LuxTrust certification services through any of its CAs, as described in section 1.3.

These responsibility and liability are still valid when LuxTrust S.A., acting as a CSP through any of its CAs, is sub-contracting services or part of services processes 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 SSL CA, and is therefore named the "Certification Practice Statement for LuxTrust SSL CA". Throughout this document, the use of the term "CPS" refers to the present document, unless otherwise specified.
For the particular case of Certificates intended to be used for authenticating servers accessible through the Internet, this document conforms to the current version of the following CA/Browser Forum documents published at http://www.cabforum.org:

- Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines [10]")
- Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")

In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, LuxTrust will include (directly or by reference) the applicable requirements of these Guidelines in all contracts with subordinate CAs, RAs, Enterprise RAs, and subcontractors, that involve or relate to the issuance or maintenance of these Certificates.

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

The 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.

The present CPS currently covers at least the following types of certificates:

- **"LuxTrust SSL"** Certificates (hereinafter called "SSL Certificate")
- **"LuxTrust Extended Validation SSL"** Certificates (hereinafter called "EV SSL Certificate")
- **"LuxTrust Object signing"** Certificates (hereinafter called "Object signing Certificate")
- **"LuxTrust QWAC" certificates: Qualified Website Authentication Certificates**

LuxTrust S.A. acting as CSP indicates and guarantees within the present CPS that it complies, through the associated LuxTrust SSL CA, with the LuxTrust Global Root CP [12].

1.2 Document name and identification

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

1.3.171.1.1.1.10.5.1

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

1.3 PKI Participants

The LuxTrust PKI Participants are described in the LuxTrust Global Root CA, Certification Practice Statement [13].

1.3.1 Certification Authorities

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

1.3.1.1 Two-level CA hierarchy

The LuxTrust PKI consists in a two-level CA hierarchy:
- One "LuxTrust Global Root CA" root-signing all subordinates LuxTrust CAs
- LuxTrust subordinate CAs. Each of these CAs is root-signed by the LuxTrust Root CA.

The LuxTrust SSL CA is one of the sub CAs, see Figure 3.

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

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

As “top root self-signed CA”, LuxTrust manages this hierarchy of CAs according to published practices that can be found under https://repository.luxtrust.lu

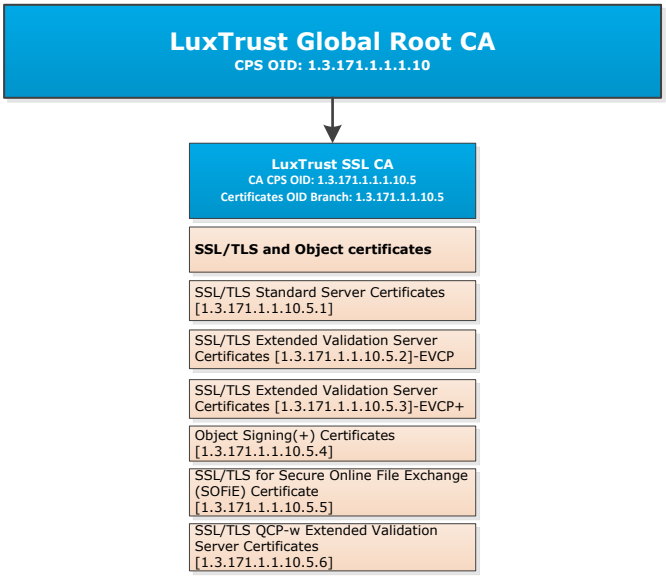

Figure 1: LuxTrust SSL CA hierarchy

1.3.2 Registration Authorities

The LuxTrust Registration Authority Network is made of a Central Registration Authority (CRA) and of a set of Registration Authorities (RAs), each of them being made of one or several Local Registration Authorities (LRAs).
The list of the authorised RAs governed by this CPS is published on LuxTrust’s website https://www.luxtrust.lu.

1.3.2.1 Central Registration Authorities

The Central Registration Authority (CRA) aims to mutualise the RA facilities for several LRAs and provide a central operational communication point between the LRAs and the rest of the LuxTrust PKI (e.g. Certificate Factory - CA, LuxTrust (secure) user devices providers, SRA).

Within the CA domain, the LRAs register and verify Subscriber’s application data on behalf of the CRA. With regards to the registration, LRAs may have direct contact with the Subscribers and must have direct contact with the CRA, but have no direct contacts with the CA.

The CRA is the entity that has final authority and decision upon the issuance and the revocation of a Certificate under this CPS.

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

- By setting up a Revocation Hotline Service for immediate[1] processing of certificate revocation (validity status of the certificate will be updated accordingly in the entries of the Validation Services / Certificate Suspension/Revocation Status Services) through a 24/7 Hotline. Contact details of this SRA Hotline are available at https://sra.luxtrust.lu.
- By setting-up a LuxTrust Hotline and support website for help desk services, those are available at https://support.luxtrust.lu.
- By registering Subscribers for certification services
- By setting up facilities
    - For notification of changes in certified information or in information supporting certification. Note that any change to certified information shall lead to the revocation of the related certificate (see section 4.8 of the present CPS).

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

The provision of Central Registration Services is ensured by the external providers supporting LuxTrust activities under signed contractual agreements with LuxTrust S.A. acting as CSP, under the present CPS and in compliance with the LuxTrust Global Root CP [12].

1.3.2.2 Local Registration Authorities

The mission of the Local Registration Authorities (LRA) is to proceed to the registration of the LuxTrust Subscribers and to validate the certificate revocation requests from the certified Subscribers when their physical presence is requested.

Within the LuxTrust SSL CA domain, the LRAs register and verify Subscriber's application data on behalf of the CRA. With regards to the registration, LRAs have direct contact with the Subscribers and with the CRA, but have no direct contacts with the LuxTrust SSL CA Certificate generation services.

The LRA, in specific, operates the following tasks:

- Registration of end-users subscription to LuxTrust certification services;
- Validation of revocation requests of Subscribers' certificates; and
- To certain extent, customer oriented tasks while these will be centralised to a maximum (e.g. notification of changes in certified information or in information supporting certification, request for information, etc.).

The provision of Local Registration Services under the present CPS and in compliance with the LuxTrust Global Root CP [12] is ensured by LuxTrust's subcontractors under a signed contractual agreement with LuxTrust S.A.

1.3.3 Subscribers

The Subscribers of the LuxTrust Certificates related certification services in the LuxTrust SSL CA domain are physical persons either identified as private persons, or identified as private persons entitled to represent a legal person or qualified by professional attributes (e.g. self-employed, employee), and registering a non-physical entity as Subject of a LuxTrust Certificate.

In order to be eligible for receiving these certification services, the Subscriber shall comply with the requirements related to the Certificate application procedures and to the Subscriber's obligations and liabilities as stated in the relevant sections of the present CPS.

1.3.4 Relying Parties

The Relying Parties are entities including physical or legal persons who rely on a Certificate and/or a security operation verifiable with reference to a public key listed in a Certificate.

To verify the validity of a digital certificate they intend to use in a security operation, Relying Parties must always verify with a CA Validation Service (e.g. OCSP, CRL, certificate status web interface) and Certificate Policy information prior to relying on information featured in a Certificate. Relying Parties shall also comply with the Relying Parties obligations and liabilities as stated in the relevant sections of the present CPS.

Relying Parties are entities that are not necessarily Subscribers.

1.3.5 Other participants

1.3.5.1 CA Factory Services Provider

The provision of CA Factory Services under the present CPS, in compliance with the LuxTrust Global Root CP [12] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by the external providers supporting LuxTrust activities.

1.3.5.2 Certificate Validation Services Provider

The provision of Certificate Validation Services under the present CPS, in compliance with the LuxTrust Global Root CP [12] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by the external providers supporting LuxTrust activities.

---

[1] The maximum delay between the receipt of a suspension (or revocation) request or report and the change of certificate validity status information being available to all Relying Parties is stated in section 4.9.5.

1.3.5.3 Suspension Revocation Authority

The provision of Suspension Revocation Authority Services under the present CPS, in compliance with the LuxTrust Global Root CP [12] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by the external providers supporting LuxTrust activities.

1.3.5.4 Dissemination (Publication) and Repository Services

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Please refer to the LuxTrust Global Root CP [12], for further details on appropriate certificate uses.

1.4.2 Prohibited certificate uses

Please refer to the LuxTrust Global Root CP [12], for further details on prohibited certificate uses.

1.5 Policy administration

1.5.1 Organisation administering the document

The Organisation administering the document is LuxTrust S.A. via its LuxTrust CSP Board, acting as Policy Approval Authority.

It can be contacted using the following coordinates:

LuxTrust contact information

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

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 implement the above practices;
- Defining the review process that ensures that the Certificate Policies are supported by the LuxTrust Certification 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.lu.

1.5.2 Contact person

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

1.5.3 Entity determining CPS suitability for the Certificate Policy

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

1.5.4 CPS Approval Procedure

The Entity approving the present CPS is LuxTrust S.A. via its LuxTrust CSP Board, acting as Policy Approval Authority. See section 1.5.1 for 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.
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 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.
Certification Practice Statement (CPS)	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.
CRL Distribution Point	A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.
Data To Be Signed (DTBS)	The complete electronic data to be signed (including both Signer's Document and Signature Attributes).
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g. by the recipient).
End Entity	A certificate subject that uses its public key for purposes other than signing certificates.
Electronic Signature	– European Directive [1]: means data in electronic form that are attached to or logically associated with other electronic data. – 14/08/2000 Luxembourg Law [4]: 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.
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 Regulation (EU) No 910/2014.
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.
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 CSP supplying the signer's certificate).
Signer's Document	Electronic data to which the electronic signature is attached to or logically associated with.
Subject	Entity to which a Certificate is issued.
Subscriber	Entity that requests and subscribes to a Certificate and for which it is either the Subject or not.
Trusted Third Party (TTP)	Authority trusted (and widely recognised, possibly accredited) by one or more users to provide Trusted Services such as Time-Stamping, Certification, etc.
Time-Stamp	Proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time-Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.
Time-Stamping Authority	Authority trusted by one or more users to provide a Time-Stamping Service.
Time-Stamping Service	Service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.
External providers supporting LuxTrust activities	External providers supporting LuxTrust activities are: – Clearstream Services; – CTIE;

	– INCERT.
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.

1.6.2 Acronyms

Acronym	Definition	Acronym	Definition
ARL	Authority Revocation List	**OID**	Object Identifier
CA	Certification Authority	**OCSP**	Online Certificate Status Protocol
CP	Certificate Policy	**PIN**	Personal Identification Number
CPS	Certification Practice Statement	**PKI**	Public Key Infrastructure
CRA	Central Registration Authority	**PKCS**	Public Key Certificates Standard
CRL	Certificate Revocation List	**PSF**	Professionnel du Secteur Financier (FSP – Financial Sector Professional)
CSP	Certification Service Provider	**RA**	Registration Authority
HSM	Hardware Security Module	**RAO**	Registration Authority Officer
IETF	Internet Engineering Task Force	**RFC**	Request for Comments
ISO	International Organisation for Standardisation	**SCD**	Signature Creation Device
ITU	International Telecommunications Union	**SRA**	Suspension and Revocation Authority
KYC	Know Your Customer	**SRAO**	Suspension and Revocation Authority Officer
LCP	Lightweight Certificate Policy	**SSCD**	Secure Signature Creation Device
LRA	Local Registration Authority	**URL**	Uniform Resource Locator

1.7 Relationship with the ETSI specifications

LuxTrust S.A. acting as CSP through its LuxTrust Qualified CA operates:

- Following the terms of the Luxembourg Law of 14/08/2000 on electronic commerce as amended [5]. This law is based on European Directive on electronic signatures 1999/93/EC and lays out the legal framework of electronic signatures in the Grand Duchy of Luxembourg,
- According to the ETSI standard EN 319 411-1 and 2,

Please refer to the LuxTrust Global Root CP [12], for further details on appropriate and prohibited certificate uses.

2 Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

LuxTrust S.A. acting as CSP, via its LuxTrust CSP Board acting as Policy Approval Authority, is the ultimate entity responsible for the operation of online and 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 Certificate Revocation Lists (CRLs).

The aforementioned documents as well as complementary information are available from online publicly accessible website accessible on https://repository.luxtrust.lu. Note: published documents and information can be physically available and managed on repositories that are technically operated by Clearstream Services and Ebrc.

2.2 Publication of Certification Information

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

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

LuxTrust S.A., acting as CSP, 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 on http://crl.luxtrust.lu;
- An OCSP responder server at http://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 2560.

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

LuxTrust does not publish any Certificate issued by LuxTrust SSL CA.

2.3.2 Frequency of Publication of Revocation information

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

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

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details on access control on repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The Subject names in a LuxTrust Certificate comply with the X.500 Distinguished Name (DN) form.
In particular, for EV SSL Certificates, LuxTrust SSL CA shall use a single naming convention as set forth in the EV Guidelines [10] and the Baseline Requirements published by the CA/Browser Forum.

Please refer to the LuxTrust Global Root CP [12], for further details on types of names.

3.1.2 Need for names to be meaningful

The value of the Common Name to be used in a LuxTrust Certificate shall be the Applicant's fully qualified hostname or path that is used in the DNS of the World Wide Web server on which the Applicant is intending to install the LuxTrust Certificate.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable as not allowed.

3.1.4 Rules for interpreting various name forms

Subject names for LuxTrust Certificates shall be interpreted as set forth in 3.1.1 and 3.1.2.

3.1.5 Uniqueness of names

The full combination of the Subject Attributes (Distinguished name) has to be unique.
The use of name of the company (or organisation), as published in the memorandum and articles of association of the company (or organisation) shall ensure this uniqueness.

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

Before issuing a LuxTrust Certificate, the LuxTrust SSL CA ensures that all Subject organization information in the LuxTrust Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this CPS – and in the particular case of SSL/EV SSL Certificates with the trusGuidelines [10] published by the CA/Browser Forum – and matches the information confirmed and documented by the RA pursuant to its verification processes.

Details on the initial identity validation procedures for Subscribers/Subjects are given in the next sub-sections as well as in the relevant Order Forms.

Please refer to the LuxTrust Global Root CP [12], for further details on initial identity validation.

3.2.1 Method to prove possession of private key

The key generation process is ensured by the Subscriber as appropriate (see section 4.5) for the requested Certificate and in accordance with the Order Form, he/she must provide a PKCS#10 Certificate Signing Request (CSR) when registering to the CRA. The key generation process shall be in compliance with the technical standard ETSI EN 319 411 1 & 2.

As prescribed by PKCS, PKCS#10 requires that the request is signed with the Subscriber's private key enabling the CRA to check the possession of the private key by the Subscriber.

3.2.2 Authentication of organisation identity

The rules concerning the identification of the Subscriber's organisation shall be compliant with the legal rules applied to naming and identification of organisation in the Grand-Duchy of Luxembourg.

RAs operating under the LuxTrust SSL CA shall perform a verification of any organizational identities that are submitted by an Applicant or Subscriber.

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

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

In the particular case of Object signing Certificates, RAs operating under the LuxTrust SSL CA shall verify the subscriber's identity and authority, and the organization's identity and existence.

In the particular case of SSL, RAs operating under the LuxTrust SSL CA shall determine whether the domain referenced in the SSL Certificate application is owned and controlled by the subscriber.
LuxTrust validates that the Subscriber has the right to control the domain names using the following verification procedures:

[1] Communicating with the technical contact information provided by the Subscriber in the order form.

[2] Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;

[3] Relying upon a Domain Authorization Document which contains the signature of an authorized representative of the domain holder, a date that is on or after the certificate request and a statement confirming the Subscriber's control over the domain names in the certificate. LuxTrust also relies on a reliable third-party, the Chamber of Commerce of Luxembourg, to confirm the authenticity of the Domain Authorization Document.

LuxTrust examines the Certification Authority Authorization (CAA) DNS Resource Records as specified in RFC 6844 following the processing instructions set down in RFC 6844 for any records found, if such CAA Records are present and do not grant LuxTrust the authority to issue the Certificate, the application is rejected.

In the particular case of EV SSL Certificates, RAs operating under the LuxTrust SSL CA shall determine whether the organizational identity, legal existence, physical existence, operational existence, and domain name provided with a LuxTrust EV SSL Certificate Application are consistent with the requirements set forth in the EV Guidelines [10] published by the CA/Browser Forum. The information and sources used for the verification of LuxTrust EV SSL Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.
In addition, for EV SSL Certificates, for organisations registered for less than 3 years, a document from a regulated financial institution proving the existence of a current account is also required for the identification of the organisation.

Moreover, LuxTrust does not issue certificates for private IP addresses or internal domains.

The LuxTrust Policy Authority may, in its discretion, update verification practices to improve the organization identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the CPS.

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 3.2) and are fully detailed in LuxTrust S.A. internal documents [11]. At expiration of the Certificates, the same procedures as for the initial identity validation (i.e. revalidation) are followed.

Initial identity validation procedures comply with Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, Version 1.6.4 [15]. The applicant's ownership of the domain is validated in line with the procedure defined in Section 3.2.2.4.2 of the aforementioned BR.

3.2.3 Authentication of individual identity

RAs operating under the LuxTrust SSL CA shall perform a verification of the identity and authority of the Contract Signer, the Certificate Approver, and the Certificate Requester associated with LuxTrust Certificate Applications that are submitted by an Applicant or Subscriber.
The same documents are required for the identification of Subscriber, as for the identification of the Subscriber's organisation described in the section 3.2.2.

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 3.2) and are fully detailed in LuxTrust S.A. internal document [11]. At expiration of the Certificates, the same procedures as for the initial identity validation (i.e. revalidation) are followed.

To ensure the accuracy of the information and to ensure that no misleading information is included in the certificate, each verification shall be validated by a RA Officer before the information can be used to issue a certificate.

For QWAC certificates (*Qualified Website Authentication Certificates*), identification is performed through a face-to-face identification at least equivalent to the level of PSF rules set by the CSSF. Face to face registration of an individual entity includes the following:

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

In specific cases, e.g., the individual to be identified cannot perform a face to face, remote registration is allowed. In that case, the authentication process can be performed remotely through the use of an "apostille" (see *The Hague Convention, October 5, 1961)*.

3.2.4 Non-verified subscriber information

Not applicable

3.2.5 Validation of authority

Not applicable.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key & update requests

3.3.1 Identification and authentication for routine re-key & update

See sections 4.7 and 4.8.

3.3.2 Identification and authentication for re-key after revocation

The same process as for initial identity validation is used.

3.4 Identification and authentication for revocation request

The identification and authentication procedures for revocation requests related to PKI Participants or organisation of PKI Participants other than Subscribers are described in LuxTrust S.A. internal documents [11] covering the present CPS.

The whole processes associated to revocation and re-instatement is described in section 4.9.

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The general requirements imposed upon issuing CA, subject CAs, RA, SRA, Subscribers and other PKI Participants' Certificates are described in the LuxTrust internal documents covering the present CPS.

For all PKI participants within the LuxTrust SSL CA domain, including the Relying Parties, there is a continuous obligation to inform in a timely manner LuxTrust S.A. with regards to the LuxTrust SSL 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.

LuxTrust S.A., acting as CSP, with regards to its LuxTrust SSL CA, shall then take appropriate measures to make sure that the situation is corrected (including revocation of the Certificate if applicable).

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any physical person can submit a Certificate application.

In addition, EV SSL Certificates are only issued for Private Organisations and Government Entities (see EV Guidelines [10] for detailed definitions).

The LuxTrust SSL CA shall issue or revoke Certificates only at the request of the CRA, or LuxTrust S.A. acting as CSP, to the exclusion of any other entity, unless explicitly instructed to do so by the CSP.

4.1.2 Enrolment process and responsibilities

To fulfil the tasks related to the LuxTrust SSL certification services, LuxTrust S.A. may use the services of third party agents under appropriate (sub-) contracting agreements. Towards any party, LuxTrust S.A. acting as CSP assumes full responsibility and accountability for acts or omissions of all third party agents it uses to deliver certification services.

The CRA mission, in the context of Subscriber/Subject registration, is to verify that the Subscriber/Subject is indeed the person he/she/it claims to be and to validate the information that is requested to be certified in the Certificate and the information supporting this certification. This shall be done in compliance with the rules and practices as stated by the LuxTrust Global Root CP [12] and by strictly following the "LuxTrust Central Registration Authority – Procedures & Guidelines for the registration of a new LuxTrust user via RA Software" [11]. This document is an internal document as part of the LuxTrust Full CPS.

The Subscriber will have to proceed to a valid initial identification and authentication of himself/herself, of the Subject and of the organisation or company he/she is representing as described in section 3.2 together with any information supporting his/her registration.

The CRA guarantees the accuracy, at the time of registration, of all information contained in the certificate request and that the Certificate Subscriber, the organisation or company he/she is representing, and the Subject (identified in the certificate request as the "to be certified entity" of the Certificate) have been duly registered and that all required verifications have been performed prior to their successful registration leading to the Certificate issuance.

Upon successful validation of the Subscriber registration, the CRAO collates and securely archives all the submitted documents and uses the RA Graphical User Interface to send the request to the Certificate Factory (operating the Certificate generation services for the LuxTrust SSL CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber and set out the grounds for this rejection.

4.1.2.1 Subscriber enrolment process

To obtain a LuxTrust Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair,
(ii) agree with the Subscriber Agreement (which is made of the relevant Order Form, the General Terms and Conditions, the present CPS and the CP), and
(iii) complete and submit a LuxTrust Certificate Application (i.e. an "Order Form"), providing all information requested by a LuxTrust-operated RA or by an independent third-party RA under a LuxTrust SSL CA without any errors, misrepresentation, or omissions.

Note: In addition, the following Applicant roles are required for the issuance of an EV SSL Certificate:

- **Certificate Requester** – The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either Applicant, employed by Applicant, an authorized agent who has express authority to represent Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of Applicant.
- **Certificate Approver** – The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant to :
    - Act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and
    - Approve EV Certificate Requests submitted by other Certificate Requesters.
- **Contract Signer** – A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant, and who has authority on behalf of Applicant to sign Subscriber Agreements.

One person MAY be authorized by the Applicant to fill one, two, or all three of these roles. An Applicant MAY also authorize more than one person to fill each of these roles.

Upon completion of the aforementioned steps (i) to (iii), a LuxTrust-operated RA or an independent third-party RA operating under the LuxTrust SSL CA shall follow the procedures described in the LuxTrust internal document [14] to perform verification of the information contained in the LuxTrust Certificate Application. If the verification performed by a RA is successful, the RA may, in its sole discretion, request the issuance to the Applicant of a LuxTrust Certificate from the LuxTrust SSL CA. If a RA refuses to request the issuance of a LuxTrust Certificate, the RA shall:

(i) use commercially reasonable efforts to notify the Applicant by email of any reasons for refusal, and
(ii) promptly refund any amounts that have been paid in connection with the LuxTrust Certificate Application.

In addition, at least for EV Certificate Requests, it also shall maintain an internal database of all rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns.

In the event of successful verification of a LuxTrust Certificate Application, the RA shall submit a request to the LuxTrust SSL CA for the issuance of a LuxTrust Certificate and shall notify the Applicant by email once a LuxTrust Certificate has been issued by the LuxTrust SSL CA. The Applicant will be provided with a URL that can be used to retrieve the LuxTrust Certificate.

The enrolment process for the Subscriber to submit Certificate application is described as follows.

Registration preparation
The Subscriber proceeds to the key generation and to the generation of the electronic request under PKCS#10 format.

Online registration
The Subscriber connects on the LuxTrust website for the online registration:

a. The Subscriber fills in his/her Subscriber Order Form for the selected Certificate type (e.g. EV SSL Certificate),
    i. Via this Order Form, the Subscriber sends the pre-generated electronic request (under PKCS#10 format) and provides an e-mail address for receiving back the certificate once issued by the LuxTrust SSL CA.
b. The Subscriber collates necessary registration supporting documents (or indicates references to paper-based registration supporting documents that shall be sent to the CRA).
c. The Subscriber prints the filled-in Order Form

This Order Form and the General Terms and Conditions for the Certificate, together with the Present CPS, constitute the Subscriber Agreement between the Subscriber and LuxTrust S.A. acting as CSP. The Subscriber may also ask the CSP to send him/her copies of the documents in question by post. The correct versions of these documents are deemed to be available on: https://repository.luxtrust.lu. By signing the Order Form, the Subscriber and the Subscriber's organisation accept the General Terms and Conditions, the present CPS and the LuxTrust Global Root CP [12].

Offline registration
The Subscriber sends per post (and/or faxes) to the CRA:

a. The printed LuxTrust **Order Form** correctly and duly filled in, and
b. The required **registration supporting documents**.

The Order Form is falls into seven (7) parts:

a. Part 1: to choose the type of Certificate;
b. Part 2: to specify the data that will appear in the Certificate (e.g. name of the entity);
c. Part 3: to specify the entity's phone number, the Requester, the Approver and the Signer's details;
d. Part 4: for the Requester and the Approver to sign the Order Form;
e. Part 5: for the Contract Signer to sign off;
f. Part 6: for the invoicing information;

Appendix: to give the list of documents that shall be provided by the Subscriber.

4.1.2.1.1 Supporting registration documents

The Subscriber applying for LuxTrust Certificates must provide several documents (via postal mail and/or fax to the CRA) that are listed in the Order Form.

4.1.2.1.2 Reuse and Updating Information and Documentation

(a) Use of Documentation to Support Multiple Certificates: LuxTrust S.A. may issue multiple Certificates listing the same Subject and based on a single Certificate Request, subject to the aging and updating requirement in (b) below.

(b) Use of Pre-Existing Information or Documentation

(1) Each Certificate issued by LuxTrust S.A. MUST be supported by a valid current Certificate Request and a Subscriber Agreement signed by the Applicant Representative on behalf of the Applicant.

(2) The age of information used by LuxTrust S.A. to verify such a Certificate Request MUST not exceed the Maximum Validity Period for such information set forth in these procedures (and the EV Guidelines [10] for EV Certificates), based on the earlier of the date the information was obtained (e.g. the date of a confirmation phone call) or the date the information was last updated by the source (e.g. if an online database was accessed by LuxTrust on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).

(3) In the case of outdated information, LuxTrust S.A. repeats the verification processes required in these procedures.

4.1.2.1.3 Enrolment of a Subscriber: high level overview

1. Online Registration step: as indicated above, the Subscriber connects on the LuxTrust RA website:
    a. The Subscriber fills in his/her Subscriber Order Form,
        i. Via this Order Form, the Subscriber sends the pre-generated electronic request (PKCS#10) and provides an e-mail address for receiving back the certificate once issued by the LuxTrust SSL CA.
    b. The Subscriber collates necessary registration supporting documents (or indicates references to paper-based registration supporting documents that shall be sent to the CRA).
    c. The Subscriber prints the Order Form.
2. The Subscriber sends per post (and/or faxes) to the CRA:
    a. The printed LuxTrust Order Form correctly and duly filled in, and
    b. The required registration supporting documents.
3. The CRA verifies the documents received and checks the following:
    a. The identity of the person applying for the Certificate (the subscriber) and its link with the organisation applying for a server certificate;
    b. On the basis of proofs (supporting documents) submitted by the person applying for the Certificate, the data to be certified in relation to ownership of the Subject names for certification; and
    c. The public key in the electronic request has been signed by the corresponding private key.
4. To confirm the accuracy of the information provided in the customer's Registration File, the CRA may call back the Subscriber or the Subscriber's organisation representative by telephone.
5. When accepted by the CRA Officer (CRAO), the electronic application for a Certificate is sent to the LuxTrust SSL CA for Certificate issuing. Should the application for the Certificate be rejected by the CRAO, the latter must inform the Subscriber and set out the grounds for this rejection.
6. The LuxTrust SSL CA responds with the Certificate to the Central RA.
7. The Central RA will send the Certificates back to the Subscriber.
8. The CRA archives the file. The archival of the registration related information is the closing task of the CRAO once registration of a new Subscriber is performed. It means for the CRAO to securely store and archive the Subscriber's application related information in an appropriate secure location according to the requirements laid down in relevant sections of the present CPS. This archiving is done on both paper-based and electronic collected information.
9. The Subscriber will add the Certificates to the server.

The detailed procedures and guidelines for CRA Officers are collected in the document "LuxTrust Central Registration Authority – Procedures & Guidelines for the registration of a new LuxTrust user via RA Software" [11]. This document is an internal document as part of the LuxTrust Full CPS.

4.1.2.2 Other PKI Participants enrolment process

The enrolment process for PKI Participants other than Subscribers is described and ruled in the LuxTrust internal document [14].

4.1.2.3 PKI Participants responsibilities related to enrolment process

4.1.2.3.1 Subscribers' responsibilities

By signing the Subscriber Agreement, the Subscriber agrees with and accepts the associated General Terms and conditions, the Present CPS and the LuxTrust Global Root CP [12].

More specifically, the Subscriber hereby gives his/her acceptance to the following responsibilities related to the enrolment process:

- The information submitted during enrolment process by the Subscriber must be valid, correct, precise, accurate, complete and meet the requirements for the type of Certificate requested and the present CPS , and in particular with the corresponding enrolment (registration) procedures. The Subscriber is responsible for the accuracy of the data provided during enrolment process.
- The Subscriber must agree to the retention - for a period of 10 years from the date of expiry of the last Subscriber Certificate - by the CSP and CRA of all information used for the purposes of registration, for the provision of a certificate or for the

revocation of the Certificate, and, in the event that the CSP ceases its activities, the Subscriber must permit this information to be transmitted to third parties under the same terms and conditions as those laid down in this CPS.

- The Subscriber hereby acknowledges the rights, obligations and responsibilities of the CSP, and other PKI participants. These are set out in the CPS currently in effect, in the Order Form and in the General Terms and Conditions relating thereto, and in the present CPS.

4.1.2.3.2 CRA responsibilities

The CRA is under a contractual obligation to comply scrupulously with the registration procedures described in the LuxTrust Global Root CP [12] and within related LuxTrust internal CRA procedures.

The CRA guarantees that:

- Subscribers are properly identified and authenticated both with regard to the personal identity of the Subscriber as a natural private person and with regard to information about the organisation he/she represents;
- Any application for Certificates submitted to the CA is complete, accurate, valid and duly authorized;
- The CRA Officer (CRAO) informs the Subscriber of the terms and conditions for the use of the Certificate. These are set out in the Order Form and the General Terms and Conditions to be signed by the Subscriber (in paper or notarised electronic form);
- The CRAO checks the identity of the Subscriber and of Subscriber's organisation representative(s) on the basis of valid identity documents recognised under Grand-Duchy of Luxembourg law. These identity documents must indicate the full name (last name and first names), date and place of birth of its owner;
- The CRAO also verifies information relating to the Subscriber's relationship with the organisation he/she represents, as indicated in Sections 3.2.2 of the present CPS;
- If the Subscriber is an affiliate of a legal person, the CRAO validates the documentation supplied as proof of the existence of this relationship;
- The CRAO ensures the storage of one copy of the information provided by the Subscriber during the enrolment process, in particular:
  - A copy of all information used to check the identity of the Subscriber and any references to his/her link with the organisation he/she represents, including any reference numbers on documentation used for this verification as well as any limitations on its validity.
  - A copy of the contractual agreement signed by the Subscriber, including the latter's agreement to all obligations incumbent on him/her.
  - This information is retained by the CRA for a period of 10 years from the date of expiry of the last Certificate linked to the Subscriber's registration by the CRA.
- The CRAO ensures compliance with the requirements relating to the processing of personal data and the protection of privacy with respect to the Subscriber enrolment process, in compliance with the Grand-Duchy of Luxembourg Law of 02/08/2002.
- The CRA puts in place clear and appropriate measures with respect to:
  - The physical security of the information provided by the Subscriber during enrolment process and, where appropriate, of the systems concerned;
  - Confidentiality regulations, specifically also those regarding banking secrecy, if applicable;
  - Logical access to any software;
  - CRAOs dealing with Subscriber enrolment process.
- The classification of and responsibility for this data are treated as of crucial importance, i.e.,
  - the data itself (registration data, guidelines and procedures, etc.) in paper form and, where applicable, in electronic form;
  - The software applications used and their configuration;
  - The equipment (hardware, telecommunications tools, etc.) and their configuration;
  - Physical access to the data (buildings, safes, access controls and conditional access to software, etc.).

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

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

Please refer to section 9.6.1 of the present CPS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The CRA performs the Subscribers and Subjects identification and authentication and guarantees the accuracy, at the time of registration, of all information contained in the certificate request and that the Subscriber identified in the certificate request and the Subject of the Certificate as the to be certified entity have been duly registered and that all required verifications have been performed prior to his/her successful registration leading to the Certificate issuance.

4.2.2 Approval or rejection of certificate applications

Upon successful validation of the Subscriber registration, the CRAO sends the Certificate request to the Certificate Factory (CA). When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber and set out the grounds for this rejection.

4.2.3 Time to process certificate applications

Not applicable.

4.3 Certificate issuance

4.3.1 Compliance

LuxTrust S.A. shall at all times:

1) Comply with all law applicable to its business and the certificates it issues in each jurisdiction where it operates.

In addition, for EV Certificates, it shall also at all time:

1) Comply with the requirements of the EV Guidelines;
2) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and
3) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

4.3.2 CA actions during certificate issuance

Actions performed by the CA during the issuance of Certificates are described within and ruled by the LuxTrust internal document [11].

4.3.3 Notification to Subscriber by the CA of issuance of Certificate

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

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

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

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

4.4.2 Publication of the Certificate by the CA

LuxTrust does not publish any Certificate issued by LuxTrust SSL CA.

4.4.3 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

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

4.5.1 Subscriber private key and certificate usage

By signing the Subscriber Agreement, the Subscriber hereby 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 present CPS or in applicable contractual agreements;
- In accordance with the LuxTrust Global Root CP [12] and with the present CPS, the Subscriber must protect the Private Key at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. 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 Subscriber has sole liability for the use of the Private Key. LuxTrust S.A. acting as CSP is not liable for the use made of the Key Pair belonging to the Subscriber or for any damage resulting from misuse of the Key Pair;
- The Subscriber shall refrain from tampering with a Certificate;
- The Subscriber shall only use Private Key and Certificate for legal and authorised purposes in accordance with the present CPS, the Subscriber Agreement and the LuxTrust Global Root CP [12], and as it may be reasonable under the circumstances;
- The Subscriber must ask the CSP to revoke the Certificate as required pursuant to the LuxTrust Global Root CP [12], and in particular if:
  - The Private Key of the Subscriber is lost, stolen or potentially compromised; 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 present CPS.
- The Subscriber must inform the CSP of any changes to data not included in the Certificate but submitted during the enrolment process. The CSP then rectifies the data registered;
- The Subscriber should destroy his/her private key once expired or revoked.

4.5.2 Relying Party public key and Certificate usage

Relying Parties who base themselves on Certificates issued in accordance with the present CPS must perform the following and assume the responsibility for having performed the following:

- Successfully perform public key operations as a condition of relying on a Certificate;
- Validate a Certificate by using the CA's Certificate Revocation Lists (CRLs), OCSP or web based Certificate validation services in accordance with the Certificate path validation procedure (see also section 4.9.6);
- Untrust a Certificate if it has been suspended or revoked;
- Rely on a Certificate only for appropriate applications as set forth in LuxTrust Global Root CP [12], taking into account all the limitations on the use of the Certificate specified in the Certificate, the applicable contractual documents and the present CPS;
- Take all other precautions with regard to the use of the Certificate as set out in this CPS 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 as not allowed.

4.7 Certificate re-key

The Certificate re-key process shall be identical to the original initial certification process.

4.8 Certificate modification

The Subscriber must immediately inform the CSP 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 CSP to revoke the Certificate whose certified data has changed. The Certificate revocation process is then started immediately. The revocation procedures are set out in Section 4.9 of the present CPS.

In case the Subscriber wants to change the certified information, or has requested the revocation of his/her Certificate due to circumstances mentioned in the previous paragraph, and wishes to be issued a new Certificate, the Subscriber shall process to Certificate re-key (see section 4.7 of the present CPS).

4.9 Certificate revocation

The revocation processes are managed by the Suspension and Revocation Authority (SRA), through the CRA towards the LuxTrust SSL CA who technically revokes a Certificate. These processes can be either:

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

It is important to note that CRA may initiate a revocation process in case of doubt on the *sanity* of an end-user (as well as any other LuxTrust PKI Participant when applicable and as stated in the LuxTrust CPS). The CRA is a PSF and is thus in possession of specific blacklists. As a consequence, it is an obligation for CRA to initiate revocation whenever necessary.

Under this certificate policy, a Certificate status can be either valid or revoked. The revocation process is irreversible, a certificate cannot be unrevoked. Upon revocation or expiration of a certificate, the corresponding private key must be destroyed in accordance with the LuxTrust Global Root CP [12].

The Certificate Subscriber, the legal representative (or his/her duly appointed delegate) of the Subscriber's company/organisation, the CRA, the LRA or LuxTrust S.A. may apply for revocation of the Certificate. The Certificate Subscriber and, where applicable, the legal representative (or his/her duly appointed delegate) are notified of the revocation of the Certificate.

LuxTrust S.A. acting as CSP, either directly or through one of its services providers (e.g. SRA, CRA) can proceed to revocation of end-user certificates in case it has enough conviction that one of the reasons is met and/or in other circumstances that are left to the appreciation of LuxTrust S.A. as indicated in the LuxTrust Global Root CP [12].

LuxTrust S.A. acting as CSP makes information relating to the status of the revocation of a Certificate available to all parties at all times, as indicated in LuxTrust Global Root CP [12] , and the CPS. Detailed procedures related to the revocation of Certificates for PKI Participants other than Subscribers or Relying Parties are provided to these entities as internal LuxTrust procedures as stated and covered by the LuxTrust Global Root CP [12].

The procedure to be used for applying for the revocation of a Certificate can be obtained from the LuxTrust SRA webpage available at the following URL: https://sra.luxtrust.lu. Applications and reports relating to a revocation are processed on receipt, and are authenticated and confirmed as fully described as follows.

4.9.1 Circumstances for revocation

The Subscriber and, when applicable, the organisation to which the Subscriber is certified (as stated in the Certificate) as linked to the Subscriber, must request the CSP to revoke the Certificate as required pursuant to the LuxTrust Global Root CP [12], and in particular in case of a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have occurred:

- The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
- The certified data is not reflecting the certificate request as verified by the Subscriber in the acceptance period following the issuance (see section 4.4.1 of the present CPS); or,
- The certified data has become inaccurate, incomplete, misleading, 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).

Such revocation request shall be submitted by the Subscriber to the Suspension and Revocation Authority. The SRA requests promptly to the LuxTrust SSL CA the revocation of a Certificate via the CRA after:

- Having received notice by the Subscriber, or when applicable, the Subscriber's organisation of a revocation request for reasons listed in the above paragraph;
- The performance of an obligation of the CRA under the present CPS is delayed or prevented by a natural disaster, computer or communication failure, or other cause beyond reasonable control, and as a result a Subscriber's information is materially threatened or compromised.

If a Subscriber's LuxTrust Certificate is revoked for any reason, the SRA that processed the Subscriber's LuxTrust Certificate Application shall make a commercially reasonable effort to notify such Subscriber by sending an email to the technical and security contacts listed in the LuxTrust Certificate Application.

In addition, the LuxTrust SSL CA shall be entitled to revoke and may revoke, and a RA operating under the LuxTrust SSL CA shall be entitled to request revocation of and shall request revocation of, a Subscriber's LuxTrust Certificate if such LuxTrust SSL CA or RA has knowledge of or a reasonable basis for believing that of any of the following events have occurred:

- Compromise of such LuxTrust SSL CA's Private Key or Compromise of a superior CA's Private Key;
- Breach by the Subscriber of any of the terms of the CPS or the Subscriber's Subscription Agreement;
- Any change in the information contained in a LuxTrust Certificate issued to a Subscriber;
- Non-payment of any LuxTrust Certificate fees or service fees;
- A determination that a LuxTrust Certificate was not issued in accordance with the requirements of the CPS or the Subscriber's Subscription Agreement;
- The LuxTrust SSL CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the LuxTrust Certificate, or that the Subscriber has failed to renew its domain name;
- The LuxTrust SSL CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the LuxTrust SSL CA's jurisdiction of operation;
- The LuxTrust SSL CA ceases operations for any reason or the LuxTrust SSL CA's right to issue LuxTrust Certificates expires or is revoked or terminated and the LuxTrust SSL CA has not arranged for another SSL CA to provide revocation support for the LuxTrust Certificates; or
- Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a LuxTrust Certificate or a LuxTrust SSL CA.

4.9.2 Who can request revocation

Revocation can be requested to the CRA by the Subscriber, by the Subscriber's organisation if applicable, by the SRA, and/or directly initiated by the CRA under the circumstances and conditions as set forth in the Present CPS and the LuxTrust Global Root CP [12].

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

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

4.9.3 Procedure for revocation request

The revocation requestor contacts LuxTrust CRA ("Central Registration Authority") at phone number (+352)-24 550 550 or info@luxtrust.lu where the revocation procedure will be launched and further steps communicated.

The archival of the revocation related information is the closing task of this procedure. It means for the CRAO to securely store /archive the signed confirmation file in an appropriate secure location. This is mainly a paper archival process; the CRA software automatically archives the electronic counterpart of this revocation process.

The detailed procedures and guidelines for CRA Officers are collected in the document "LuxTrust Central Registration Authority – Procedures & Guidelines for the registration of a new LuxTrust user via RA Software" [11]. This document is an internal document as part of this CPS.

In addition, for LuxTrust SSL, Subscribers, Relying parties and other third parties may report SSL Certificate problems at phone number (+352)-24 550 550.

For SSL and Object Signing Certificates, LuxTrust shall make its best effort to begin an investigation of the Certificate Problem Report in a timely manner. For EV SSL Certificates, LuxTrust shall begin an investigation of the Certificate Problem Report within twenty-four (24) hours of receipt.

LuxTrust shall decide whether revocation or other appropriate action is warranted on a least the following criteria:

- The nature of the alleged problem;
- The number of certificate problem reports received about a particular SSL Certificate or
- website;
- The identity of the complainants (for example, complaints from a law enforcement official that a Web site is engaged in illegal activities carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
  Relevant legislation.

For Certificate revocation that is not initiated by the Subscriber, the SRA that requested revocation of the Subscriber's LuxTrust Certificate shall make a commercially reasonable effort to notify the Subscriber by sending an email to the technical and security contacts specified in the Subscriber's LuxTrust Certificate Application.

The revocation of a Certificate is definitive.

4.9.4 Revocation request grace period

In the case of Private Key Compromise, or suspected Private Key Compromise, a Subscriber shall request revocation of the corresponding LuxTrust Certificate immediately upon detection of the Compromise or suspected Compromise. Revocation requests for other required reasons shall be made as soon as reasonably practicable.

LuxTrust S.A. acting as CSP shall make its best effort to ensure that the time needed to process the revocation request and to publish the revocation notification (updated CRL) shall be as reduced as possible. When the revocation is finally decided, the publication in the CRL must not exceed eight (8) hours and thirty (30) minutes.

4.9.5 Time within which CA must process the revocation request

To request the revocation of a Certificate, the revocation requestor must contact the SRA Hotline for revocation or use appropriately the SRA web-based interface for revocation of the Certificate. See section 4.9.3 for further details on procedure for revocation request.

The CRA requests promptly, via the CA, the revocation of the Certificate once the revocation request authenticated and validated. The CA revokes a Certificate immediately only upon revocation request coming from the CRA and having been approved by the CRA.

The maximum delay between the receipt of a revocation request or report and the change of certificate validity status information being available to all Relying Parties is stated in section 4.9.4 of the present CPS.

4.9.6 Revocation checking requirements 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. LuxTrust S.A. acting as CSP and through its LuxTrust SSL CA updates OCSP, and CRLs accordingly. Relying Parties are made aware of the maximum delay between the receipt of a revocation request or report and the change of certificate validity status information being available to all Relying Parties is indicated in section 4.9.5. Relying Parties shall take this information into account when checking validity status of a Certificate.

4.9.7 CRL issuance frequency

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

LuxTrust S.A. makes available Certificate status checking services including CRLs, OCSP and appropriate web interfaces. CRLs are available from https://crl.luxtrust.lu. OCSP services are available from http://ocsp.luxtrust.lu.

A CRL is issued each 4 hours and half, at an agreed time. CRLs are signed and time-marked by the LuxTrust CA.

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

4.9.8 Maximum latency for CRLs

Not applicable.

4.9.9 On-line revocation/status checking availability

LuxTrust S.A. makes available Certificate status checking services related to Certificates issued by the LuxTrust SSL CA including CRLs, OCSP and appropriate web interfaces. See LuxTrust Global Root CA, Certification Practice Statements [13] for access restriction and charging rules.

Certificate revocation status services are available 24 hours per day, 7 days per week. Outside system maintenance windows, system failure or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that the uptime of these services exceeds 99.0%.

4.9.10 On-line revocation checking requirements

See 4.9.6.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

Not applicable.

4.9.13 Circumstances for suspension

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

See section 4.9.7.

4.10.2 Service availability

See section 4.9.9.

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, when performed, is not performed by the CSP, and may be performed by the Subscriber, under the sole responsibility of the Subscriber.

Subscriber's key escrow by the CSP is not allowed.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, operational, procedural, personnel and physical (security) controls that are used by LuxTrust S.A. for its LuxTrust SSL CA (the CA) 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 described and ruled by the LuxTrust Global Root CPS [13].

6 TECHNICAL SECURITY CONTROLS

The security measures taken by LuxTrust S.A. for its LuxTrust SSL CA to protect its cryptographic key and activation data, the constraints on repositories, subject CA, 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. for its LuxTrust SSL CA 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 described and ruled by the LuxTrust Global Root CPS [13].

7 CERTIFICATE AND CRL PROFILES

The profiles of LuxTrust Certificates and CRLs are defined in the LuxTrust Global Root CP [12].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

With regard to the provision of LuxTrust Certificates, LuxTrust S.A. through its LuxTrust SSL CA operates:

- Following the terms of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. This law is based on European Directive on electronic signatures 1999/93/EC and lays out the legal framework of electronic signatures in the Grand-Duchy of Luxembourg [5],
- According to the ETSI technical standard EN 319 411 1&2
- According to the present CPS and the LuxTrust Global Root CP [12].

In addition, for EV SSL Certificates, it also operates according to the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates. Latest version in force, [10]

As described and ruled in the LuxTrust Global Root CP [12], LuxTrust S.A. acting as CSP accepts for its LuxTrust SSL CA and all its supporting certification services compliance audit to ensure they meet the ILNAS requirements for Qualified Trust Service Providers. The Supervision Scheme for Qualified Trust Service Providers is described on the ILNAS website, [14].

Any PKI Participant supporting the LuxTrust CSP activities under the present CPS, in particular but not limited to RA networks, shall accept for being selected for audit or controls, shall provide all required assistance and work to successfully comply and pass audit or controls.

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details on compliance audit and other assessments requirements.

8.1 Security Audit Procedures

Significant security events in the LuxTrust SSL CA are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Audit trail files are archived periodically.

All files including the latest audit trail file are moved to backup media and stored in a secure archive facility.

The LuxTrust SSL CA and all RAs operating under the LuxTrust SSL CA record in detail every action taken to process an LuxTrust Certificate, and in particular: the request to issue an LuxTrust Certificate, including all information generated or received in connection with the request, and every action taken to process the request, including time, date, and personnel involved in the action.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

1) LuxTrust SSL CA key lifecycle management events, including:
   - Key generation, backup, storage, recovery, archival, and destruction; and
   - Cryptographic device lifecycle management events.

2) LuxTrust SSL CA and Subscriber LuxTrust Certificate lifecycle management events, including:
   - LuxTrust Certificate Requests, renewal and re-key requests, and revocation;
   - All verification activities required by this CPS;
   - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   - Acceptance and rejection of LuxTrust Certificate Requests;
   - Issuance of LuxTrust Certificates; and
   - Generation of Certificate Revocation Lists (CRLs) and OCSP messages.

3) Security events, including:
   - Successful and unsuccessful PKI system access attempts;
   - PKI and security system actions performed;
   - Security profile changes;
   - System crashes, hardware failures, and other anomalies;
   - Firewall and router activities; and
   - Entries to and exits from the LuxTrust SSL CA facility.

4) Log entries include the following elements:
   - Date and time of entry;
   - Identity of the person making the journal entry; and
   - Description of entry.

8.2 Records Archival

The audit trail files, databases and revocation information for LuxTrust SSL CA are both archived. The archive of LuxTrust SSL CA database and the archive of revocation information are retained for at least ten (10) years.

Archives of audit trail files are retained for at least seven (7) year(s) after any LuxTrust Certificate based on that documentation ceases to be valid.

The databases for LuxTrust SSL CA are encrypted and protected by LuxTrust software master keys. The archive media is protected through storage in a restricted-access facility to which only LuxTrust-authorized personnel have access.

Archive files are backed up as they are created. Originals are stored on-site and housed with a LuxTrust SSL CA system. Backup files are stored at a secure and separate geographic location.

Archives are made available to provide evidence of the correct operation of the services for the purpose of legal proceedings.

9 OTHER BUSINESS AND LEGAL MATTERS

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

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 Certificate issuance or renewal fees.
- 9.1.2 Certificate access fees.
- 9.1.3 Revocation or Certificate status information access fees.
- 9.1.4 Fees for other services, as specified from time to time in updated versions of the present CPS , such as:
  - Repositories access fees.
- 9.1.5 Refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

LuxTrust S.A. and 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.

LuxTrust S.A. maintains the following insurance related to its performance and obligations under the EV SSL Guidelines as follows:

Commercial General Liability insurance (occurrence form) with policy limits of at least $2 million in coverage, and Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

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

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

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

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 LuxTrust Global Root CA, Certification Practice Statement [13].
LuxTrust S.A. acting as CSP guarantees the confidentiality of any data not published in the Certificates, according to the applicable laws on privacy, as well as according to the Luxembourg laws on the financial sector, specifically with regard to banking secrecy.
Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

9.4 Protection of personal information

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

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

Data privacy regulations and directives in force shall be respected by CRA(O)s. The received data from end-users can be used solely for the provision of certification services.

The CRA shall guarantee the confidential treatment of any data not to be 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.

9.5 Intellectual property rights

All titles, 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., through its LuxTrust SSL CA issues X509 v3-compatible Certificates (ISO 9594-8).

LuxTrust S.A., through its LuxTrust SSL CA issues Certificates compliant with ETSI EN 319 411-1 &2 Certificates requirements. To this end, LuxTrust S.A. publishes the elements supporting this statement of compliance.

LuxTrust S.A. guarantees that all the requirements set out in the Present CPS (and indicated in the Certificate in accordance with LuxTrust Global Root CP [12]) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with the LuxTrust Global Root CP [12].

To register persons applying for a Certificate, LuxTrust S.A., through its LuxTrust SSL CA, uses the list of approved LRAs as indicated in the present CPS.

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

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

In certain cases described in the present CPS, LuxTrust S.A. acting as CSP 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.

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

See LuxTrust CPS for all additional rights, responsibilities and obligations of LuxTrust S.A. acting as CSP through its LuxTrust SSL CA.

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

9.6.2 RA representations and warranties

The RA are under a contractual obligation to comply scrupulously with the LuxTrust CPS, with the relevant section of the present CPS (e.g. but not limited to sections 4.1.2), and with the CRA 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 CSP and setting out the procedures used for providing the Certificates.
The Subscriber agrees to the present CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the present CPS (e.g. but not limited to, 1.3.3, 1.4, 4, 4.1.2.3, 4.5.1, 9).

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

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

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 Present CPS and of the LuxTrust CPS and associated conditions for Relying Parties (in particular sections 4.5.2 and 4.9.6 of the present CPS);
- Decision to rely on a certificate must always be a ***conscious*** one and can only be taken by ***the Relying Party itself***;
- Therefore, ***before deciding to rely on a certificate it is needed to be assured of its validity.*** If the Relying Party is not certain that its software performs such checks automatically, the Relying Party has to open the Certificate by clicking on it and checking that the Certificate is ***NOT*** either
  - ***expired*** – by looking at the "valid from ___ to ___" notice; *or*
  - ***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 sections 4.5.2 and 4.9.6 of the present CPS;
- Without prejudice to the warranties provided in the Present CPS 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, the LuxTrust CSP Board will not accept liability for any consequences;
- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt;
- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify LuxTrust S.A. acting as CSP.

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

Damages covered and disclaimers

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

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 Present CPS even if LuxTrust S.A. has been advised of the possibility of such damages.

b) In no event shall LuxTrust S.A. be liable for any direct, indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use or the reliance of revoked or expired Certificate.

c) This 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 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.

Please refer to the LuxTrust Global Root CA, Certification Practice Statement [13] for further details.

9.8 Limitations of liability

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

9.8.1 Limitations on EV Certificate Liability

9.8.1.1 CA Liability

(1) Subscribers and Relying Parties
In cases where LuxTrust has issued and managed the EV Certificate in compliance with the Guidelines and its CPS, LuxTrust shall not be liable to the EV Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate. In cases where LuxTrust has not issued or managed the EV Certificate in complete compliance with the Guidelines and this CPS, LuxTrust's liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed 2,500 (two thousand and five hundred) euros.
LuxTrust's liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed 2,500 (two thousand and five hundred) euros.

(2) Indemnification of Application Software Vendors
Notwithstanding any limitations on its liability to Subscribers and Relying Parties, LuxTrust understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with LuxTrust do not assume any obligation or potential liability of LuxTrust under the Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. LuxTrust shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by LuxTrust, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by LuxTrust where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from LuxTrust online, and the browser software either failed to check such status or ignored an indication of revoked status).

In no event will LuxTrust be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS; (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than LuxTrust (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties. In no event shall LuxTrust be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

9.9 Indemnities

The LuxTrust CSP Board assumes no financial responsibility for improperly used Certificates, CRLs, etc.

9.10 Term and termination

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

9.11 Individual notices and communications with participants

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

LuxTrust contact information

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

9.12 Amendments

9.12.1 Procedure for amendment

LuxTrust S.A. via its CSP Board is responsible for approval and changes of the present CPS.
The only changes that the LuxTrust S.A. via its CSP Board may make to these CP specifications without notification are minor changes that do not affect the assurance level of this CP, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document shall be communicated to the contact of the LuxTrust CSP Board as identified in the Present CPS or in the LuxTrust 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 CSP Board shall accept, modify or reject the proposed change after completion of a review phase.

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

All changes to the present CPS, other than editorial or typographical corrections, or changes to the contact details, will be subject to an incremented version of the Object Identifier for the present CPS.
Minor changes to this CPSdo not require a change in the CP OID or the CP 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 CP OID or CP pointer qualifier.
Minor changes are indicated by version number that contains a decimal number e.g., version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major changes.

9.13 Dispute resolution provisions

All disputes associated with the Present CPS will be resolved according to the law of Grand-Duchy of Luxembourg.

9.14 Governing law

The laws of Grand-Duchy of Luxembourg shall govern the enforceability, construction, interpretation, and validity of the present CPS.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

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

- Terms and conditions described in the Present CPS and in the LuxTrust Global Root CA, Certification Practice Statement [13];
- General Terms and Conditions related to the subscription to such a Certificate;
- Any other applicable Certificate Policy as may be stated in an issued Certificate;
- The mandatory elements and any non-mandatory but customized 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 LuxTrust SSL CA uses computer-based and text based pointers that include URLs, OIDs, etc.