LuxTrust Certificate Policy for Server and Code Signing Certificates (QCA)

SSL/TLS Certificates and Code Signing (or Object Signing) Certificates generated by qualified CA

Version number: 1.4

Publication Date: 15/09/2011

Effective Date: 30/09/2011

Document Information

Document title:	LuxTrust Certificate Policy for Server and Code Signing Certificates (QCA)
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Certificate Policy
Document Distribution List	Any
Document Classification	Public
Document Owner	LuxTrust CSP Board

Version History

Version	Who	Date	Reason of modification
1.0	PHI	15/06/2008	First Version
1.1	PHI	15/02/2011	Minor modifications
1.2	PHI	13/05/2011	Modification of certificate profile OU field for Internal Use
1.3	MSC	15/06/2011	Added SAN certificates and removal of 5 year certificates and 1024 bit keys
1.4	MSC	12/09/2011	Re-allow 1024 bits key size for one year certificates

Table of content

Intellectual Property Rights

References

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

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

[3] ETSI TS 101 456 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

[4] ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[5] ICAO (International Civil Aviation Organization) – Machine Readable Travel Documents – Technical Report – PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, October 01, 2004

[6] ETSI TS 102 023 – Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

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

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

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

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

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

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

1 INTRODUCTION

1.1 Overview

1.1.1 The LuxTrust project

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

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

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

1.1.2 Goal of the LuxTrust PKI

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

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

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

1.1.3 LuxTrust PKI Hierarchy

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

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

LuxTrust S.A., acting as CSP as described in the law of Grand-Duchy of Luxembourg modified on 14/08/2000 [7], is using several Certification Authorities (CAs), as shown in the certificates hierarchy, to issue LuxTrust end-users certificates. These top level CAs are the LuxTrust Root CA, LuxTrust Normalised CA and LuxTrust Qualified CA. Additional CAs may be root-signed by the LuxTrust Root CA in the future.

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

This responsibility and liability is still valid when LuxTrust S.A. acting as CSP through any of its CAs is sub-contracting services or part of services process to third parties. Sub-contracting agreements shall include back-to-back provisions to ensure that sub-contractors shall support the liability and responsibility for the sub-contracted provisioned services.

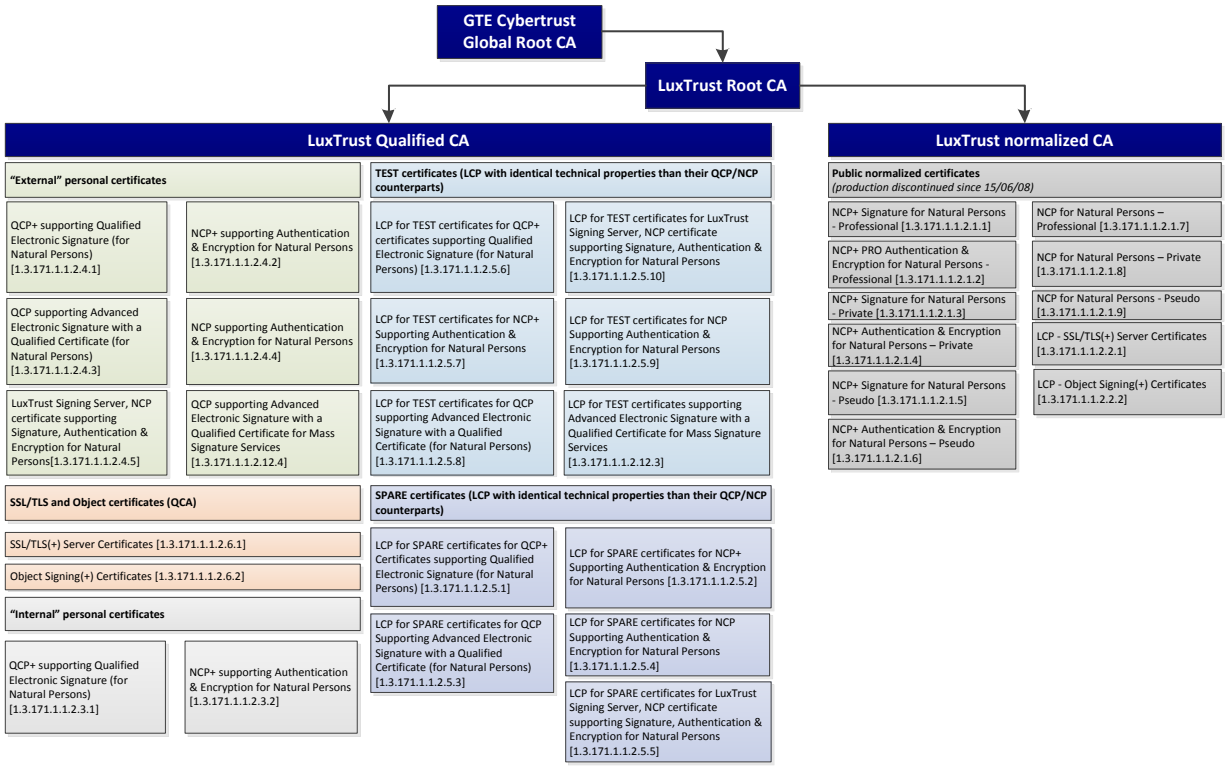

Figure 1 - LuxTrust PKI CA hierarchy, related CPS/CPs and contractural documents

1.1.4 The present document - LuxTrust Certificate Policy for Server and Code Signing Certificates (QCA)

The present document is the "LuxTrust Certificate Policy for Server and Code Signing Certificates – SSL/TLS Certificates and Code Signing (or Object Signing) Certificates CP". This Certificate Policy (CP) document indicates:

- the applicability of certificates in the form of *LuxTrust Server and Code Signing Certificates* (hereinafter referred to as the "Certificates") issued by LuxTrust S.A. acting as Certification Service Provider (CSP), as well as,

- the requirements, procedures to be followed and the responsibilities of the parties involved during the life-cycle of the Certificates, in accordance with the LuxTrust S.A.'s Certification Practice Statement (CPS) [6].

The purpose of the present CP is to establish what participants within the LuxTrust PKI must do in the context of requesting, issuing, managing and using the here above defined Certificates.

The present CP is a set of rules, requirements and definitions determining the level of security reached by the LuxTrust Server and Code Signing Certificates. Two kinds of Certificates are covered by the present CP:

- **"LuxTrust LCP Server"** Certificates: SSL – TLS compliant ETSI TS 102 042 [5] LCP Certificate not on SSCD Hardware token, with creation of the keys by the Subscriber, 1024-bit key size for one (1) year, or 2048-bit key size for one (1) or three (3) years validity, and with a key usage limited to digital signature (authentication), key and data encryption.

- **"LuxTrust LCP Code Signing"** Certificates: ETSI TS 102 042 [5] LCP compliant Certificate not on SSCD Hardware token, with creation of the keys by the Subscriber, 2048-bit key size, one (1) or three (3) years validity, and with a key usage limited to digital signature (authentication) to the exclusion of electronic signature.

SSL – TLS Server Certificates (hereinafter called "Server Certificates")

These Certificates meet the requirements for SSL and TLS[1] purposes since they provide authentication, encryption and added features. They can be used for proving the identity and ownership of a (domain) server name and for enabling confidential communication between a (web) server and the connected customers. The LuxTrust Server Certificates are convenient for both SSL and TLS support.

- Certificates are not certified as stored and protected by Secure Signature Creation Device as it is not possible for LuxTrust S.A. acting as CSP to validate such assertion. It is however strongly recommended to use a secure device (e.g., HSM, SSCD, etc.) to use, store and protect the server private key.
- Creation of the keys is performed by the Subscriber or by his organisation (i.e. a system administrator). Creation of the keys is not performed by LuxTrust S.A.
- The key size must be 1024 bits for one (1) year certificates or 2048 bits for one (1) or three (3) years certificates.
- Certificates have either one (1) or three (3) years validity.
- Certificates key usage is limited to digital signature (authentication purposes to the exclusion of electronic signature – non-repudiation)2 and key & data encryption.
- Certificates are compatible with, and meet the requirements laid down in, ETSI TS 102 042 Lightweight Certificate Policy (LCP) [5].

This type of Certificate provides a good degree of assurance of the correctness of the Certificate Subject identity and its link with the certified public key and its authorised usage. The Certificate Subject identity is the electronic identity of a Server and can reflect its belonging to an authenticated organisation (e.g. but not limited to a company domain name or URL of a company web server).
The validation of the request will require evidence of the identity of the Subscriber and evidence that he/she represents the organisation owning the (domain) server name to be certified. The Subscriber is either the legal representative of the company (organisation) that is responsible for, or the owner of, the (Web) Server or the URL, or is a duly authorized representative thereof. The link between the (Web) Server identity and the public key is certified. This type of Certificate also guarantees that the authenticated organisation (e.g., company) is the owner of, or responsible for, the (Web) Server. Applications are only accepted if the Subscriber can prove that the (Web) Server or the URL belongs to the organisation.

The Subscriber needs to provide the CRA for verification, a signed copy of his/her identity document and proof of his/her professional status (link to or representation of the organisation), together with any supporting information to be certified and documents proving ownership of the (Web) Server to the organisation.

In addition to the specific LuxTrust requirements for Server Certificates stated in the present document, these Server Certificates meet the requirements for "LCP" certificate policy as specified by ETSI TS 102 042 [5] and include accordingly the ETSI TS 102 042 LCP certificate policy identifier (see section 1.2).

Such Certificates can be used for the following security services: encryption and / or digital signatures for entity authentication purposes and for data origin authentication and integrity.

A public key certified in this way must be used solely for establishing secure connections between (Web) Servers and (Web) clients and for the authentication of (Web) Servers.

[1] All major web server software supports SSL or its successor TLS for securing server-to-browser connections.

[2] Please refer to section 1.4 of the present CP, in order to take knowledge of the usage restriction of such a certificate even if the technical usage of such an authentication within a contract establishment process may lead to a valid signature of a contract.

LuxTrust S.A. acting as CSP indicates and guarantees within the present CP that it complies, through the associated LuxTrust Qualified CA, with the LuxTrust CPS [6] and with the regulatory and standard texts as applicable to the Server Certificate types described in the present document.

Code Signing (or Object Signing) Certificates

The Public keys certified by the LuxTrust Code Signing Certificates can be used in the framework of electronic signature of Software Code by the organisation owning the certificate. These Certificates have the following characteristics:

- Certificates are not certified as stored and protected by Secure Signature Creation Device as it is not possible for LuxTrust S.A. acting as CSP to validate such assertion. It is however strongly recommended to use a secure device (e.g., HSM, SSCD, etc.) to use, store and protect the signing private key.
- Creation of the keys is performed by the Subscriber or by his organisation (i.e. a system administrator). Creation of the keys is not performed by LuxTrust S.A.
- The key size must be 2048 bits.
- Certificates have one (1) or three (3) years validity.
- Certificates key usage is limited to digital signature (authentication purposes to the exclusion of electronic signature – non-repudiation)3.
- Certificates are compatible with, and meet the requirements laid down in, ETSI TS 102 042 Lightweight Certificate Policy (LCP) [5].

This type of Certificate provides a good degree of assurance of the correctness of the Certificate Subject identity and its link with the certified public key and its authorised usage. The Certificate Subject identity is the official identity of the organisation requesting the certificates such as stated in articles of association, including the legal form. The necessary proofs to authenticate this legal entity are described in CPS section 3.3.2.

The validation of the request will require evidence of the identity of the Subscriber and evidence that he/she represents the organisation applying for a Code Signing certificate. The Subscriber is either the legal representative of the company (organisation) or a duly authorized delegate thereof.
The Subscriber needs to provide the CRA for verification, a signed copy of his/her identity document together with any supporting proof of information to be certified and documents linking him to the organisation and proving this status.

Such Certificate can be used for the following security services: digital signature of Software Code with the exclusion of qualified electronic signature.

In addition to the specific LuxTrust requirements for Code Signing Certificates stated in the present document, these Code Signing Certificates meet the requirements for “LCP” certificate policy as specified by ETSI TS 102 042 [5] and include accordingly the ETSI TS 102 042 LCP certificate policy identifier (see section 1.2).

LuxTrust S.A. acting as CSP indicates and guarantees within the present CP that it complies, through the associated LuxTrust Qualified CA, with the LuxTrust CPS [6] and with the regulatory and standard texts as applicable to the Server Certificate types described in the present document.

[3] Please refer to section 1.4 of the present CP, in order to take knowledge of the usage restriction of such a certificate even if the technical usage of such an authentication within a contract establishment process may lead to a valid signature of a contract.

1.2 Document name and identification

The present document is identified by the following identifier:

1.3.171.1.1.2.6.0.1(version).3(subversion)

In addition to the specific LuxTrust requirements for LuxTrust Server and Code Signing Certificates stated in the present document, these Certificates meet the requirements for "LCP" certificate policy, as specified by ETSI TS 102 042 [5] and include accordingly the ETSI TS 102 042 LCP certificate policy identifier.

The identifiers (OID – object identifier) for the Server and Code Signing Certificate Policies and for the related Certificates defined in this document are defined as follows:

- **"LuxTrust LCP Server"**:
  - *ETSI 102 042 OID: 0.4.0.2042.1.3*
  - *LuxTrust LCP Server OID:* 1.3.171.1.1.2.6.1

- **"LuxTrust LCP Code Signing"**:
  - *ETSI 102 042 OID: 0.4.0.2042.1.3*
  - *LuxTrust LCP Authentication & Encryption OID:* 1.3.171.1.1.2.6.2

1.3 PKI participants

The LuxTrust PKI Participants are the legal entities or set of legal entities filling the role of participant within the LuxTrust PKI, that is either making use of, or providing LuxTrust PKI certification services[4] that are used by LuxTrust S.A. acting as CSP to provide its LuxTrust certification services.

The PKI participants within the LuxTrust PKI that are used by LuxTrust S.A. to provide or support the certification services related to the present CP are identified as follows:

- LuxTrust Certification Authority
- Central Registration Authorities
- Subscribers / Subjects
- Relying Parties
- And other participants as:
- CA Factory Services Provider
- Certificate Validation Services Provider
- Suspension Revocation Authority
- Root Signing Services Provider

The parties mentioned here above are collectively called the PKI participants. All these PKI participants implement practices, procedures and controls meeting the requirements as stated in the present CP as described in the LuxTrust Certification Practice Statement in force [6].

[4] Or "component services" as defined by ETSI TS 102 042 in its section 4.2 as the break downed services constituting the service of issuing public key certificates.

1.3.1 Certification Authority

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

Within the LuxTrust PKI, the "LuxTrust Qualified CA" is used by LuxTrust S.A. acting as CSP to issue the LuxTrust QCP(+), NCP(+) and LCP Certificates as defined in section 1.1.3.

The "LuxTrust Qualified CA (LTQCA)", hereafter referred to as the "CA" operates within a grant of authority for issuing *LuxTrust Certificates* under the present CP. This grant has been provided by the "LuxTrust Root CA" (hereinafter referred to as the LTRCA) under the responsibility and authority of LuxTrust S.A. acting as CSP.

Note 1: *In the following text, unless explicitly indicated otherwise, when referring to "the CA", it is expressly meant "the LuxTrust Qualified CA granted to issue LuxTrust Server and Code Signing Certificates by the LuxTrust Root CA under the ultimate responsibility of LuxTrust S.A. acting as CSP". The CA is thus legally designating LuxTrust S.A. acting as CSP.*

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

The LTQCA, as well as all supporting component services, shall target accreditation against ETSI TS 102 042 [5] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. ILNAS shall be the accreditation entity. For further details please refer to section 8 of the present CP.

The LTQCA, that is, LuxTrust S.A. acting as CSP, is established in Grand-Duchy of Luxembourg. LuxTrust S.A. can be contacted, with respect to the LTQCA, using the coordinates as provided in the section 1.5.1 of the present CP. The technical management and operations of the LTQCA (including the Certificate generation services) are ensured by a CA Factory Services provider (see section 1.3.5.1) in accordance with the present CP, the LuxTrust CPS [6] and within a secure facility compliant with the LuxTrust CPS and providing a disaster recovery facility in the Grand-Duchy of Luxembourg.

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

1.3.2 Registration Authorities

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

- The Central Registration Authority (CRA): It 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, LuxTrust (secure) user devices providers, SRA). In particular, the task of certificate suspension, notification of changes in the information supporting the certification process of an end-user, password reset requests will be centralised in CRA activities.
- The Local Registration Authority (LRA): Its mission is to proceed to the registration[5] of the LuxTrust Certificate Subscribers and to validate the certificate un-suspension and revocation requests from the certified users when the physical presence of the user is requested.

[5] Initial registration or registration related to certificate re-key (see sections 4.1 and 4.7 respectively). Certificate renewal is not allowed (see section 4.7) and certificate modification leads to revocation of the certificate (see section 4.8).

All communications between LRAs, CRA, SRA, the LTQCA, and (S)SCD Service Providers regarding any phase of the life cycle of the Certificate are secured with PKI based encryption and signing techniques to ensure confidentiality, mutual authentication and secure logging/auditing as described in the LuxTrust CPS [6].

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). In particular, the task of certificate suspension, notification of changes in the information supporting the certification process of an end-user, password reset requests will be centralised in CRA activities.

Within the CA domain, the LRA 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 of a Certificate under this CP, upon the suspension and revocation of a Certificate under this CP.

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

- By setting up a Suspension Revocation Hotline Service for immediate[6] processing of certificate suspension (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 CP).
    - For collection and approval of requests related to the provision of a new Activation Data (e.g., password, authentication mechanism, etc.) for LuxTrust Signing Server accounts

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

The provision of Central Registration Services is ensured by u-trust consortium[7] under a signed contractual agreement with LuxTrust S.A. acting as CSP, under the present CP and in compliance with the LuxTrust CPS [6].

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 un-suspension and revocation requests from the certified Subscribers when their physical presence is requested.

[6] 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.

[7] The u-trust consortium is constituted by legal persons (Clearstream Services S.A., Cetrel S.A., eBRC and HITeC S.A.) that are different and independent from each other.

Within the LTQCA domain, the LRA 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 LTQCA Certificate generation services.

The LRA, in specific, operates the following tasks:

- Registration of end-users subscription to LuxTrust certification services
- Delivery of SSCD or SCD related protection information
- Validation of rehabilitation (un-suspension) or 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 LRA can send opted-in Subscribers appropriate invitation letter to apply for LuxTrust Smart Card Certificates.

The provision of Local Registration Services under the present CP and in compliance with the LuxTrust CPS [6] is ensured by LuxTrust's subcontractors under a signed contractual agreement with LuxTrust S.A. The list of authorised LRAs under the present CP is available from https://ra.luxtrust.lu.

1.3.3 Subscribers

The Subscribers of the LuxTrust Server or Code Signing Certificates related certification services in the LuxTrust Qualified CA (LTQCA) 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 Server or Code Signing Certificate (e.g., (web) server, object signing entity, IPsec entity, etc.).

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 CP.

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 CP.

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 CP, in compliance with the LuxTrust CPS [6] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by u-trust consortium.

1.3.5.2 Certificate Validation Services Provider

The provision of Certificate Validation Services under the present CP, in compliance with the LuxTrust CPS [6] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by u-trust consortium.

1.3.5.3 Suspension Revocation Authority

The provision of Suspension Revocation Authority Services under the present CP, in compliance with the LuxTrust CPS [6] and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by u-trust consortium.

1.3.5.4 Root Signing Services

The Root Signing Services Provider shall ensure trust in the LuxTrust Root CA (LTRCA) in widely used applications (e.g., browsers, routers, etc.). It shall ensure that its own root shall remain trusted by widely used applications and shall notify LuxTrust S.A. of any event affecting trust to its own root.

The entity providing Root Signing Services to the LTRCA is GTE Cybertrust Global Root in compliance with the LuxTrust CPS [6] and under a contractual agreement signed with LuxTrust S.A. acting as CSP.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Server Certificates

This type of Certificate provides assurance of the electronic identity of a (Web) Server implementing SSL or TLS secure communication protocol or implementing Certificate enabled security services namely encryption and / or digital signatures for entity authentication purposes and for data origin authentication and integrity. It can therefore also be used to protect top-level applications in a client/server, browser/server model, such as major commercial transactions, conclusion of contracts and signing of files, bank transactions and interactions with public institutions.

Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section 7 of this document). The LuxTrust LCP Server Certificate is an ETSI TS 102 042 LCP compliant Certificate with a key usage combining digital signature (authentication), key encryption and data encryption purposes. The keyUsage bits “digitalSignature”, “keyEncypherment” and “keyEncypherment” as well as the extended key usages “serverAuthentication”, clientAuthentication” and “emailProtection” are set to the exclusion of any other usage. It shall be explicitly stated in the Certificate that Electronic Signatures are authorised to be computed as supported by such a Certificate, and that Relying Parties shall accept such a Certificate to support valid Electronic Signatures. Electronic signatures supported by such a Certificate are Advanced Electronic Signatures as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

The applications for which the Certificate is deemed to be trustworthy must be decided by the Relying Parties themselves on the basis of the nature and purpose of the Certificate, including any applicable limitation as written in the Certificate or included by reference, and on the basis of the level of security of the procedures followed for issuing the Certificate as described in the present CP and the LuxTrust CPS [6].

Code Signing Certificates

This kind of Certificates guarantees the electronic identity of an organisation for the purposes of authenticating the origin and ensuring integrity of signed codes, programs, or similar objects (e.g., software codes such as JAVA applets, ActiveX, …). The certified public key can only be used in the framework of digital signature of software code.

Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section 7 of this document). The LuxTrust LCP Code Signing Certificate is an ETSI TS 102 042 LCP compliant Certificate with a key usage set to digital signature. The keyUsage bits “digitalSignature”, is set to the exclusion of any other usage. It shall be explicitly stated in the Certificate that Electronic Signatures are authorised to be computed as supported by such a Certificate, and that Relying Parties shall accept such a Certificate to support valid Electronic Signatures of codes or other similar objects. Electronic signatures

supported by such a Certificate are Advanced Electronic signatures as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

The applications for which the Certificate is deemed to be trustworthy must be decided by the Relying Parties themselves on the basis of the nature and purpose of the Certificate, including any applicable limitation as written in the Certificate or included by reference, and on the basis of the level of security of the procedures followed for issuing the Certificate as described in the present CP and the LuxTrust CPS [6].

1.4.2 Prohibited certificate uses

Usage of Certificates that are issued under the present CP, other than to support applications identified in Section 1.4.1 is prohibited.

Relying Parties are strongly recommended to make use of the Certificate LuxTrust OID (see section 1.2 of the present CP) to appropriately accept or reject a Certificate usage.

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*

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 policy

The Entity determining CPS suitability for the 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 CP Approval Procedure

The Entity approving the present CP 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 [1]	Refers to Electronic Signature meeting the following requirements: – It is uniquely linked to the signatory; – It is capable of identifying the signatory; – It is created using means that the signatory can maintain under his sole control; and – It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
Certification Authority (CA) [2]	Authority trusted by one or more users to create and assign certificates. A certification authority may optionally create the users' keys.
Certificate [2]	Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.
Certificate Identifier	A unique identifier of a Certificate consisting of the name of the CA and of the certificate serial number assigned by the CA.
Certificate Policy (CP) [2]	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement [2]	Statement of the practices which a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Certificate Validity Period	The time interval during which the CA warrants that it will maintain information about the status of the certificate. (Time interval between start validity date and time and final validity date and time).
Certificate Revocation List (CRL) [2]	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certification Path [3]	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Service Provider [1]	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Commitment Type	A signer-selected indication of the exact intent of an electronic signature.
CRL Distribution Point	A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

Data To Be Signed (DTBS)	The complete electronic data to be signed (including both Signer's Document and Signature Attributes).
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient
End Entity	A certificate subject that uses its public key for purposes other than signing certificates
Electronic Signature	– European Directive [1]: means data in electronic form that are attached to or logically associated with other electronic data. – 14/08/2000 Luxembourg Law [7]: Art. 6. « Signature » - Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé : "La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte. Elle peut être manuscrite ou électronique. La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article."
Hash Function	Cryptographic function that maps a variable length string of bits to fixed-length strings of bits, satisfying the following two properties: – It is computationally unfeasible to find for a given output an input which maps to this output; – It is computationally unfeasible to find for a given input a second input which maps to the same output.
Key Pair	Public Key and the corresponding Private Key.
Mass Signature Services (MSS)	LuxTrust service providing advanced signature based on Qualified Certificates following QCP Public, whose certificates are covered by this CP. Signature Creation Devices remains within LuxTrust premises and Subjects are provided with secure access through the public internet.
De-centralized Mass Signature Service (D-MSS)	LuxTrust service providing advanced signature based on Qualified Certificates following QCP Public, whose certificates are covered by this CP. Signature Creation Devices are located within the Subjects' premises and Subjects are provided with secure access to the devices through their networks.
Object Identifier (OID)	Sequence of numbers that uniquely and permanently references an object.
Online Certificate Status Protocol (OCSP) Provider	Online trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the OSCP server (which contains the certificate status) and the client application (which is informed of that status).
Public Key	Key of an entity's asymmetric key pair that can be made public.
Private Key	Key of an entity's asymmetric key pair that should only be used by that entity.

Qualified Certificate [1]	Certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive [1].
Secure User Device [4]	Device which holds the user's private key and protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signature Attributes	Additional information that is signed together with the Signer's Document.
Signature Creation Data [1]	Refers to unique data, such as codes or private cryptographic keys used by the signatory to create an electronic signature.
Signature Creation Device [1]	Refers to configured software or hardware used to implement the signature creation data.
Signature Policy	Set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.
Signature Policy Identifier	Object Identifier that unambiguously identifies a Signature Policy.
Signature Policy Issuer	Organization creating, maintaining and publishing a signature policy.
Signature Policy Issuer Name	Name of a Signature Policy Issuer.
Signature Verification	Process performed by a verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.
Signature-Verification-Data [1]	Data, such as codes or public cryptographic keys used for the purpose of verifying an electronic signature.
Signature-Verification Device [1]	Configured software or hardware used to implement the signature verification-data.
Signatory [1]	A person who holds a signature creation device and acts either on his own behalf or on behalf of the natural legal person or entity he represents.
Signer	Entity that creates an (electronic) signature.
Signer's Identity	Registered name of the signer (i.e. as registered by the CSP supplying the signer's certificate).
Signer's Document	Electronic data to which the electronic signature is attached to or logically associated with.
Subject	Entity to which a Certificate is issued.
Subscriber	Entity that requests and subscribes to a Certificate and for which it is either the Subject or not.
Trusted Third Party (TTP)	Authority trusted (and widely recognised, possibly accredited) by one or more users to provide Trusted Services such as Timestamping, Certification …
Time Stamp	Proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.

Time Stamping Authority	Authority trusted by one or more users to provide a Time Stamping Service.
Time Stamping Service	Service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.
U-Trust	A consortium of entities that are subcontracting part of the maintenance of LuxTrust activities. U-Trust is composed by: – CETREL S.A.; – Clearstream Services; – eBRC; – HiTec
Validation Data	Additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.
Verifier	Entity that validates or verifies an electronic signature. This may be either a relying party or a third party interested in the validity of an electronic signature.
What Is Presented is What Is Signed (WIPIWIS)	Description of the required qualities of the interface able to unambiguously present the signer's document to the verifier according to the content format of the signer's document.
What You See Is What You Sign (WYSIWYS)	Description of the required qualities of the interface able to unambiguously present to the signer the document to be signed according to the content and format.

1.6.2 Acronyms:

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

Acronym	Definition	Acronym	Definition
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
LDAP	Lightweight Directory Access Protocol	TSP	Time Stamping Policy
NCP	Normalised Certificate Policy	TSSP	Time Stamping Service Provider
NCP+	Normalised Certificate Policy +	TSU	Time Stamping Unit
OID	Object Identifier	URL	Uniform Resource Locator
OCSP	Online Certificate Status Protocol	UTC	Coordinated Universal Time

1.7 Relationship with the European Directive on Electronic Signatures

The LTQCA, as well as all supporting component services, shall target accreditation against ETSI TS 102 042 [5] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. ILNAS shall be the accreditation entity. For further details please refer to section 8 of the present CP.

Electronic signatures supported by the Certificates issued under the present CP are Advanced Electronic Signatures as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable. See the section 1.4 for further details on authorized and prohibited usages of these certificates.

2 Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

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

- The CPS
- The present CP
- The related subscriber contractual agreements (e.g., Purchase Orders, General Terms and Conditions, etc.)
- The Certification Authority Certificates, Certification Paths and related ARLs
- The Certificates Public Registry
- The Certificate Revocation Lists (CRLs)

The above mentioned documents and information are available from online publicly available website accessible at https://repository.luxtrust.lu.

The above mentioned documents and information can be physically available and managed on repositories that are technically operated by u-trust consortium.

2.2 Publication of Certification Information

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

The LuxTrust CPS [6] covering the practices used by LuxTrust S.A. through its LTQCA to issue the Certificates under the present CP is available online on https://repository.luxtruxt.lu. This repository shall also contain any other public documents where LuxTrust S.A. acting as CSP makes certain disclosures about its practices, procedures and the content of certain of its policies, including the present CP. It reserves right to make available and publish information on its policies by any means it sees fit.

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

The Certificates issued by the LTQCA are available for download on https://certs.luxtruxt.lu.

The LTQCA publishes CRL's at regular intervals at https://crl.luxtrust.lu as indicated in the LuxTrust CPS.

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

LuxTrust S.A. maintains the CRL distribution point and the information on this URL until the expiration date of all Certificates containing the CRL distribution point.

A web interface for Certificate status checking services is available from https://status.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

2.3 Time of Frequency of Publication

2.3.1 Frequency of Publication of Certificates

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

2.3.2 Frequency of Publication of Revocation information

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

2.3.3 Frequency of Publication of Terms & Conditions

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

2.4 Access Control on Repositories

All repositories as listed in 2.1 are available in public anonymous read-only access. Only Trusted Staff functions, as specified in section 5 of the LuxTrust CPS [6] have write and change access on these repositories, with strong PKI Credentials based access control. State-of-the-art security measures protect these repositories.

While the primary objective of LuxTrust S.A. is to keep access to its public repositories free of charge, it reserve 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. may take reasonable measures to protect and prevent against abuse of the OCSP, Web interface status verification and CRL download services.

Note 1: *Privacy issues shall be taken into account in compliance with section 9.4.*

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Server Certificates

The rules concerning the naming and identification of the organisation owning the server to be certified are such that:

- Country (C) is the Country in which the organisation's registered office is established (as specified in the memorandum and articles of association)
- Locality (L) is the location in which the organisation's registered office is established (as specified in the memorandum and articles of association).
- Organisation (O) is the official name of the organisation, as published in the memorandum and articles of association of the organisation, including the legal form
- Common Name (CN) is the exact and full name (identity) of the Server/Application (e.g., this can be an URL for a web server, or the IP address of the server/application or any other name or identifier that uniquely identifies an server/application) according to the provided proof of ownership as presented by the Subscriber and validated by the CRA
- Rfc822Name is the Subject's e-mail address.
- Optionally: up to ten (10) subject alternative names, conforming to the CN format can be provided.

The detailed structure of the Certificate subject attributes is provided in section 7.1 of the present CP (including X.500 distinguished names and RFC-822 names).

Code Signing Certificates

The rules concerning the naming and identification of the organisation owning the server to be certified are such that:

- Country (C) is the Country in which the organisation's registered office is established (as specified in the memorandum and articles of association)
- Locality (L) is the location in which the organisation's registered office is established (as specified in the memorandum and articles of association).
- Organisation (O) is the official name of the organisation, as published in the memorandum and articles of association of the organisation, including the legal form (optional)
- Common Name (CN) is the official name of the organisation, as published in the memorandum and articles of association of the organisation, including the legal form
- Rfc822Name is the Subject's e-mail address.

The detailed structure of the Certificate subject attributes is provided in section 7.1 of the present CP (including X.500 distinguished names and RFC-822 names).

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

LuxTrust Root CA Certificates	
Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust Root CA
LuxTrust Qualified CA Certificate (issued by the LuxTrust Root CA)	
Country (C)	LU
Organization (O)	LuxTrust S.A.
Common Name (CN)	LuxTrust Qualified CA

3.1.2 Need for names to be meaningful

As far as prescriptions described in 3.1.1 are followed, names may not be meaningful.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable as not allowed.

3.1.4 Rules for interpreting various name forms

RFC-822 names shall be used as Alternate Subject Names by indicating the email address of the Certificate's Subject.
In addition, Subject Alternative Names for the CN may be added.

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 insure this uniqueness.

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

The initial identity validation procedures for PKI participants or organisation of PKI participants other than Subscribers are described in the LuxTrust CPS [6] covering the present CP.

The initial identity validation procedures details for Subscribers/Subjects are detailed in the next sub-sections.

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 when registering to the CRA. The key generation process should be in compliance with the technical standard ETSI TS 102 042 LCP certificate policy [5].

As prescribed by PKCS, PKCS#10 requires that the request is signed by the 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.

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

1. Recent constitutive act, or recent extract of the commercial register (or the foreign equivalent for foreign companies registered under foreign law), or a copy of the publication in Memorial C (or its foreign equivalent) referring the creation of the legal person;

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 residence permit issued by the Luxembourg government) of one of the physical persons who are legal representative of the legal person. This copy must be certified by a competent authority (embassy, consulate, notary, municipality, police office, bank from the first order) and be accompanied by a legalisation of the signature of this authority. In addition, the Subscriber shall provide for verification a certified and legalized copy of a valid and authentic identity card or identity passport or residence permit issued by the Luxembourg government. The Subscriber shall also provide a signed statement from the above legal representative certifying his/her link with the organisation and authorizing the Certificate subscription;
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 a explanatory description of structure of the proposed company.
7. In case the membership of a physical person within a legal person is to be validated and certified in the Certificate, the person identified in (4) shall sign the appropriate guarantee as provided in the applicable Certificate application form (Purchase Order).

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

3.2.3 Authentication of individual identity

See section 3.2.2 (point 4).

3.2.4 Non-verified subscriber information

Subject's E-mail address is the only non-verified Subscriber information.

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 the LuxTrust CPS [6] covering the present CP.

The whole processes associated to suspension, revocation and re-instatement are described in section 4.9.

The Subscriber, and if applicable the legal representative (or his duly appointed delegate) of the company/organisation from which the Subscriber is a member of, the CRA or LuxTrust S.A. may apply for suspension, reinstatement following suspension (un-suspension), or revocation of the Certificate. The Subscriber and, where applicable, the legal representative (or his duly appointed delegate) is notified of the suspension, reinstatement following suspension or revocation of the Certificate.

Applications and reports relating to a suspension, reinstatement following suspension or revocation are processed on receipt, in a timely manner[8], and are authenticated as described in section 4.9.3, 4.9.16 and 4.9.15 respectively.

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

The form to be used for applying for the suspension / reinstatement following suspension / revocation of the Certificate can be obtained from the CA on the LuxTrust repository website https://repository.luxtrust.lu and on https://sra.luxtrust.lu.

[8] 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.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The general requirements imposed upon issuing CA, subject CAs, RA, SRA, Subscribers and other PKI Participants with respect to the life-cycle of Certificates are described in the LuxTrust CPS [6] covering the present CP.

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

- 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 LTQCA, shall then take appropriates measure 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.

The LTQCA shall issue, suspend 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 LTQCA 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 CPS [6] and by strictly following the “LuxTrust Central Registration Authority – Procedures & Guidelines for the registration of a new LuxTrust user via RA Software”. 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 his 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 LTQCA). 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.

As a post-registration step, the CRAO prepares to the attention of LuxTrust S.A. a paper copy of the full paper-based registration file of the subscriber. Once a month (or at another frequency indicated by LuxTrust S.A.), all these copies of subscribers' paper files are securely sent to LuxTrust S.A. according to its PSF status and to the law against money bleaching.

4.1.2.1 Subscriber enrolment process

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 Subscriber Order Form for the selected Certificate type (either Server or Code Signing 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 LTQCA.
   ii. Via this Order Form, the Subscriber selects his Suspension/Revocation password online together with reminder facilities.
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 (hereafter referred to as "the Order Form" and "the General Terms and Conditions"), together with the present CP and the LuxTrust CPS [6], 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 CP and the CPS [6].

Offline registration

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

a. the printed LuxTrust **Order Form** correctly and duly filled in,
b. the required **registration supporting documents** and,
c. the signed **print-out of the public key** (hexa or PEM format of the public key within the PKCS#10 electronic request).

The Order Form falls into two parts:

a. The "Subscriber Part" must be duly completed and signed by the Subscriber.
b. The "Subscriber Organisation Part" must be duly filled in and signed by a legal representative (or his/her duly appointed delegate) of the organisation to which the Subscriber belongs. In case of Web Server Certificates, a particular care will be put in the spelling of the URL(s) to be certified.

4.1.2.1.1 Supporting registration documents

The Subscriber applying for the LuxTrust Server or Code Signing Certificate(s) must provide the following documents (via postal mail and/or fax to the CRA) proving that:

A. The Subscriber is administrator or legal representative of the organisation applying for the Certificate

- A (two-sided) copy of the Subscriber's valid identity card, passport or residence permit issued by the Luxembourg government. The copy must be signed by the Subscriber, and the signature certified and legalised (see section 3.2.2);
- A copy of the current memorandum and articles of association of the company (or organisation) from which it can be clearly derived the exact representation of the Subscriber as claimed legal representative or duly appointed delegate.

The rules and documents required for the identification of the Subscriber's organisation (legal person) and/or to validate his membership within a legal person are listed in section 3.2.2 of the present CP;

- Official or appropriate documents establishing the formal link or ownership of the Subject name and identification to the Subscriber or the Subscriber's organisation.

OR

B. The Subscriber is an employee or a member of the organisation applying for the Certificate;

- A (two-sided) copy of the Subscriber's valid identity card, passport or residence permit issued by the Luxembourg government. This copy must be signed by the Subscriber, and the signature certified and legalised (see section 3.2.2);
- A (two-sided) copy of a valid identity card, passport or residence permit issued by the Luxembourg government of the legal representative (or duly appointed delegate of the organisation) from which the Subscriber is an employee or a member. The copy must be signed by the legal representative of the organisation (or by his/her duly appointed delegate), and the signature certified and legalised (see section 3.2.2);
- A copy of the current memorandum and articles of association of the organisation from which it can be clearly derived the exact representation of the claimed legal representative or duly appointed delegate;
- If the person (co-)signing the Order Form is a duly appointed delegate of a legal representative, the Subscriber must provide evidence that this person has the authority to sign on behalf of the legal representative;
- Official or appropriate documents establishing the formal link or ownership of the Subject name and identification to the Subscriber or the Subscriber's organisation.

4.1.2.1.2 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 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 the receiving back the certificate once issued by the LTQCA.
        ii. Via this Order Form, the Subscriber selects his Suspension/Revocation password online together with reminder facilities.
    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 print 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,
    b. the required registration supporting documents and,
    c. the signed print-out of the public key.
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.
    c. The public key in the electronic request has been signed by the corresponding private key
    d. The mapping between the public key within the electronic request and the signed print-out received by postal mail and/or fax.
4. To confirm the accuracy of the information provided in the customer's Registration File 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 LTQCA for Certificate issuing. When the application for the Certificate is rejected by the CRAO, the latter must inform the Subscriber and set out the grounds for this rejection.

6. The LTQCA generates the Certificate, and, in case the Subscriber has agreed so, publishes them on the LuxTrust Directory Server.
7. The LTQCA responds with the Certificate to the Central RA.
8. The Central RA will send the Certificates back to the Subscriber
9. 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 CP. This archiving is done on both paper-based and electronic collected information.
10. The subscriber will add the Certificates to the server.

As a post-registration step, the CRAO prepares to the attention of LuxTrust S.A. a paper copy of the full paper-based registration file of the subscriber. Once a month (or at another frequency indicated by LuxTrust S.A.), all these copies of subscribers' paper files are securely sent to LuxTrust S.A. according to its PSF status and to the law against money bleaching.

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". 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 CPS.

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 CP, and the LuxTrust CPS [6].

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 CP, and in particular with the corresponding enrolment (registration) procedures. The Subscriber is responsible for the accuracy of the data provided during enrolment process.
- The Subscriber must agree to the retention - for a period of 10 years from the date of expiry of the last Subscriber Certificate - by the CSP and CRA of all information used for the purposes of registration, for the provision of a certificate or for the suspension or 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 CP.
- The Subscriber hereby acknowledges the rights, obligations and responsibilities of the CSP, and other PKI participants. These are set out in the LuxTrust CPS [6] currently in effect, in the Order Form and in the General Terms and Conditions relating thereto, and in the present CP.

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 CPS [6] 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 represent, as indicated in Sections 3.2.2, and 7.1 of the present CP.
- 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 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.
- As a post-registration step, the CRAO prepares to the attention of LuxTrust S.A. a paper copy of the full paper-based registration file of the subscriber. Once a month (or at another frequency indicated by LuxTrust S.A.), all these copies of subscribers' paper files are securely sent to LuxTrust S.A. according to the law against money bleaching.
- 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 CP.

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 P.O. 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 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 CA actions during certificate issuance

Actions performed by the CA during the issuance of the Certificate are described within and ruled by the LuxTrust CPS [6].

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

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

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 publication in the LuxTrust CSP Public Repository of Certificates or its first use by the Subscriber, whichever occurs first. In the intervening period, the Subscriber is responsible for 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 CP. This is the sole recourse available to the Subscriber in the event of non-acceptance on Subscriber's part.

4.4.2 Publication of the Certificate by the CA

Once the Certificate has been issued by the LTQCA, unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Certificate is immediately published in the LuxTrust Public Repository of Certificates (Directory). This repository is in the public domain and is accessible at all times as stated in Section 4.10 of the present CP.

Unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Subscriber agrees to the publication of the digital Certificate in the LuxTrust Public Repository of Certificates immediately on creation. The Subscriber is made aware by the CSP that refusal to publish his Certificates may lead to usage difficulties if his counterpart expects to get the Subscriber's Certificates from the Certificates publishing services of LuxTrust.

4.4.3 Notification of Certificate issuance by the CA to other entities

The Certificate issuance is notified by the LTQCA to other entities through the publication of the Certificate in the LuxTrust Public Repository of Certificates (Directory), available in the public domain and accessible at all times as stated in Section 4.10 of the present CP.

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 CP or in applicable contractual agreements.
- In accordance with the LuxTrust CPS [6] and with the present CP, the Subscriber must protect the Private Key and its Activation Data at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. Once the Private and Public key pair has been delivered to the Subscriber, the Subscriber is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Subscriber is deemed the sole user of the Private Key. The Private Key Activation Data (e.g., PIN-code or password(s)) used to prevent unauthorized use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without adequate protection. The Subscriber must never leave the Private Key or the Private Key Activation Data unsupervised when it is not locked (e.g., leave it unsupervised in a work station when the PIN code or password has been entered).
- The Subscriber has sole liability for the use of the Private Key. LuxTrust S.A. acting as CSP is not liable for the use made of the Key Pair belonging to the Subscriber or for any damage resulting from misuse of the Key Pair.
- The Subscriber shall refrain from tampering with a Certificate.
- The Subscriber shall only use Private Key and Certificate for legal and authorised purposes in accordance with the present CP, the Subscriber Agreement and the LuxTrust CPS [6], 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 CPS [6], and in particular if:
  - The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
  - The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data (e.g. PIN code) has been compromised or for any other reason[9]; and/or,

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

- The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part)

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

- The Subscriber must inform the CSP of any changes to data not included in the Certificate but submitted during the enrolment process. The CSP then rectifies the 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 CP 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 the present CP, taking into account all the limitations on the use of the Certificate specified in the Certificate, the applicable contractual documents and the present CP (in particular in section 1.4).
- Take all other precautions with regard to the use of the Certificate as set out in this CP or elsewhere, and rely on a Certificate as may be reasonable under the circumstances.
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on a Certificate.

4.6 Certificate renewal

Not applicable 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 CP.

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, §2 of the present CP).

4.9 Certificate revocation

The revocation processes are managed by the Suspension and Revocation Authority (SRA), through the CRA towards the LTQCA who technically suspends or revokes a Certificate. In any cases, CRA, and SRA functions shall be functionally separated to ensure separation of duties. 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). It is an obligation for all entities subject to PSF regulation. 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 CPS [6].

The Certificate Subscriber, the legal representative (or his 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 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 CPS [6].

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 the applicable CP, and CPS [6]. 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 CPS [6].

The form and/or 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 ask the CSP to revoke the Certificate as required pursuant to the LuxTrust CPS [6], and in particular if:

- The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
- The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data (e.g. PIN code) has been compromised or for any other reason; or,
- The certified data is not reflecting the certificate request as verified by the Subscriber in the acceptance period following the issuance (see section 4.4.1 of the present CP); 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 SRA request promptly to the LTQCA 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 CP 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.

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 CP and the LuxTrust CPS.

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 LTQCA 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)-266815-1 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". This document is an internal document as part of the LuxTrust CPS [6].

The revocation of a Certificate is definitive.

4.9.4 Revocation request grace period

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 and does not exceed four(4) 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 as prompt as possible suspension prior 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 CP.

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 LTQCA updates OCSP, CRLs and the Web based interface Certificate status validation service accordingly. Relying Parties are made aware of 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 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 https://ocsp.luxtrust.lu. Web interface for Certificate status checking services is available from https://status.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

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

LuxTrust S.A. makes available all CRLs issued by the LTQCA in the previous [*12*] months available on its repository. 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 CP.

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 LTQCA including CRLs, OCSP and appropriate web interfaces. See section 2.4 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

Alternative, out-of-band, revocation advertisements available for the advertising of revocation, especially in case of revocation of the LTQCA Signature Certificate are stipulated in the LuxTrust CPS [6].

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 Qualified 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 CPS [6].

6 TECHNICAL SECURITY CONTROLS

The security measures taken by LuxTrust S.A. for its LTQCA 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 LTQCA 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 CPS [6].

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

X.509 v3 is supported and used.

7.1.1.1 LuxTrust Server Certificates

LuxTrust Server Certificates are ETSI TS 102 042 LCP Certificates [5] not certified as generated on SSCD, with creation of the keys by the Subscriber, with a 1024-bits key size for one (1) year certificates or 2048-bit key size and one (1) or three (3) years validity from issuing start date.

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

The usage purpose of these LuxTrust Server Certificates is the combined purpose of digital signature, key and data encryption. The LuxTrust LCP Server Certificates include the corresponding LuxTrust LCP OID for SSL/TLS server certificates, i.e., ***<1.3.171.1.1.2.6.1>.***

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

*Items marked **Green** have to be provided by the requesting company; items marked **Red** can be provided optionally.*

LuxTrust LCP Server Certificate Profile						
Attribute	**Field**	**IN** [10]	**CE** [11]	**O/M** [12]	**CO** [13]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = “2”
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			
	algorithm				S	OID = “1.2.840.113549.1.1.5” - SHA-1 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Qualified CA

[10] IN = Included: Attribute / field included within the certificate profile.
[11] CE = Critical Extension.
[12] O/M: O = Optional, M = Mandatory.
[13] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

LuxTrust LCP Server Certificate Profile						
Attribute	**Field**	**IN** [10]	**CE** [11]	**O/ M** [12]	**CO** [13]	**Value**
	organizationName	✓			S	LuxTrust S.A.
validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12;36** months **(1or 3 years validity)**
subject		✓	False			
	countryName*	✓		M	D	*Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)*
	stateOrProvinceName*	✓		O	D	
	localityName	✓		M	D	*Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)*
	organizationName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	organizationalUnitName1	✓		O	D	*As provided by Subscriber or, if commonName does not contain a Fully Qualified Domain Name (FQDN), this field (OU1) must contain the text: INTERNAL USE ONLY*
	organizationalUnitName2	✓		O	D	*As provided by Subscriber*
	commonName	✓		M	D	*FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or IP address or unique name of server.*
	serialNumber	✓		O	D	*Serial Number as provided by subscriber*
	emailAddress	✓		O	D	*Subject's email address*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				*Public Key: Key length: 1024bits (RSA) for one (1) year certificates or 2048bits (RSA) for one (1) or three (3) years certificates;* *public exponent: Fermat-4 (=010001).*
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInfoAccess		✓	False			

LuxTrust LCP Server Certificate Profile						
Attribute	**Field**	**IN** [10]	**CE** [11]	**O/ M** [12]	**CO** [13]	**Value**
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				https://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				https://ca.luxtrust.lu/LTQCA.crt
CRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				"https://crl.luxtrust.lu/LTQCA.crl"
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject's email address*
	SubjectAltName-dNSName	✓		O		*Up to ten FQDN (Fully Qualified Domain Name) of application/server – Exact and full second URL for a Web Server or IP address or unique name of server.*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	*The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).*
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓			S	1.3.171.1.1.**2.6.1**
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	LuxTrust Server Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on

LuxTrust LCP Server Certificate Profile						
Attribute	**Field**	**IN**[10]	**CE**[11]	**O/M**[12]	**CO**[13]	**Value**
						https://repository.luxtrust.lu. Signed by a Qualified CA.
	PolicyIdentifier	✓			S	0.4.0.2042.1.3
Extended Key Usage		✓	False			
	serverAuth	✓			S	True
	clientAuth	✓			S	True
	emailProtection	✓			S	True
Netscape Proprietary						
NetscapeCertificateType		✓	False			
	SSL Client	✓			S	Set
	SSL Server	✓			S	Set
	S/MIME	✓			S	Set

7.1.1.2 LuxTrust Object (or code) Signing Certificates

LuxTrust Code Signing Certificates are ETSI TS 102 042 LCP Certificates [5] not certified as generated on SSCD, with creation of the keys by the Subscriber, with a 2048-bit key size and one (1) or three (3) years validity from issuing start date.

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

The usage purpose of these LuxTrust Code Signing Certificates is the purpose of digital signature. The LuxTrust LCP Code Signing Certificates include the corresponding LuxTrust LCP OID, i.e., ***<1.3.171.1.1.2.6.2>.***

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

*Items marked **Green** have to be provided by the requesting company; items marked **Red** can be provided optionally.*

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN**[14]	**CE**[15]	**O/M**[16]	**CO**[17]	**Value**
Base Profile						
Version		✓	False			
					S	Version 3 Value = "2"
SerialNumber		✓	False			
					FDV	Validated on duplicates.
signatureAlgorithm		✓	False			

[14] IN = Included: Attribute / field included within the certificate profile.
[15] CE = Critical Extension.
[16] O/M: O = Optional, M = Mandatory.
[17] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [14]	**CE** [15]	**O/M** [16]	**CO** [17]	**Value**
	algorithm				S	OID = "1.2.840.113549.1.1.5" - SHA-1 with RSA Encryption.
signatureValue		✓	False			
					D	Issuing CA Signature.
issuer		✓	False		S	
	countryName	✓			S	LU
	commonName	✓			S	LuxTrust Qualified CA
	organizationName	✓			S	LuxTrust S.A.
validity		✓	False			
	NotBefore	✓			D	Certificate generation process date/time.
	NotAfter	✓			D	Certificate generation process date/time + **12; 36** months **(1 or 3 years validity)**
subject		✓	False			
	countryName*	✓		M	D	*Country in which the company's registered office is established (as specified in the memorandum and articles of association). (ISO3166)*
	stateOrProvinceName*	✓		O	D	
	localityName	✓		M	D	*Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)*
	organizationName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	organizationalUnitName1	✓		O	D	*As provided by Subscriber*
	organizationalUnitName2	✓		O	D	*As provided by Subscriber*
	commonName	✓		M	D	*Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)*
	serialNumber	✓		O	D	*NA or Serial Number as provided by subscriber*
	emailAddress	✓		O	D	*Subject's email address if available*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				*Public Key: Key length: 2048 (RSA); public exponent: Fermat-4 (=010001).*
	subjectPublicKey	✓		M		
Extensions						

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [14]	**CE** [15]	**O/M** [16]	**CO** [17]	**Value**
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Qualified CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				https://ocsp.luxtrust.lu
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				https://ca.luxtrust.lu/LTQCA.crt
CRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				"https://crl.luxtrust.lu/LTQCA.crl"
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		O	D	*Subject's email address*
subjectKeyIdentifier		✓	False			
	keyIdentifier	✓			Fixed	*The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).*
Policy Properties						
keyUsage		✓	True			
	digitalSignature	✓			S	True
	nonRepudiation	✓			S	False
	keyEncipherment	✓			S	False
	dataEncipherment	✓			S	False
certificatePolicies		✓	False			
	PolicyIdentifier	✓			S	1.3.171.1.1.**2.6.2**
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	https://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					

LuxTrust LCP Code Signing Certificate Profile						
Attribute	**Field**	**IN** [14]	**CE** [15]	**O/M** [16]	**CO** [17]	**Value**
	DisplayText	✓			S	LuxTrust Code Signing Certificate. Not supported by SSCD, Key Generation by Subscriber. GTC, CP and CPS on https://repository.luxtrust.lu. Signed by a Qualified CA.
	PolicyIdentifier	✓			S	0.4.0.2042.1.3
Extended Key Usage		✓	False			
	Object Signing	✓			S	Set
Netscape Proprietary						
NetscapeCertificateType		✓	False			
	Object Signing	✓			S	Set

7.1.2 Certificate extensions

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

7.1.3 Algorithm object identifiers

Algorithms OID are conforming to IETF RFC 3279 and RFC 3280.

7.1.4 Name forms

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

7.1.5 Name constraints

Name constraints are supported as per RFC 3280.

7.1.6 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

7.1.7 Usage of Policy Constraints extension

Usage of Policy Constraints extension is supported as per RFC 3280.

7.1.8 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 3280 is supported.

7.1.9 Processing semantics for the critical Certificate Policies

Not applicable.

7.2 CRL profile

In conformance with the IETF PKIX RFC 2459, LuxTrust S.A., through its LTQCA supports CRLs compliant with:

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

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

LuxTrust CRL Profile	
Field	**Comments**
Version	v2
Signature	Sha1RSA
Issuer	<subjectCA>
thisUpdate	<creation time>
nextUpdate	<creation time + 100 days for Root CA> <creation time + 4,5 hours (4 hours and 30 minutes) for NCA & QCA>
revokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
reasonCode	*<Insert List of used revocation reason code>*
crlExtensions	
cRLNumber	Non-critical <subject key identifier CA>
authorityKeyIdentifier	Non-critical <CA assigned unique number>

7.2.1 Version number(s)

See section 7.2.

The LTQCA will support X.509 version 2 CRLs, retrievable by LDAP on the LuxTrust Certificate Public Registry.
As an alternative to CRLs, LuxTrust S.A. may provide Web based or “other” revocation checking services for Certificates issued by its LTQCA.

7.2.2 CRL entry extensions

See section 7.2.

7.3 OCSP profile

The OCSP profile follows IETF PKIX RFC 2560 OCSP v1 and v2. No OCSP extensions are supported. The LTQCA supports signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA. The OCSP response is signed as described and ruled in the LuxTrust CPS.

7.3.1 Version number(s)

See section 7.3.

7.3.2 OCSP extensions

See section 7.3.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

With regard to the provision of LuxTrust Qualified Certificates, LuxTrust S.A. through its LuxTrust Qualified 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 [8],
- According to the ETSI technical standard TS 102 042 “Policy requirements for certification authorities issuing public key certificates”,[5]
- According to the present CP and the LuxTrust CPS [6].

As described and ruled in the LuxTrust CPS [6], LuxTrust S.A. acting as CSP accepts for its LTQCA and all its supporting certification services compliance audit to ensure they meet, within 18 months following services set-up, the ILNAS requirements for the voluntary “Accreditation of Certification Service Providers issuing certificates or providing other services related to electronic signatures” as described and available on the official ILNAS website, www.ilnas.lu.

Any PKI Participant supporting the LuxTrust CSP activities under the present CP, 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 CPS [6] for further details on compliance audit and other assessments requirements.

9 OTHER BUSINESS AND LEGAL MATTERS

See LuxTrust CPS [6] for further details.

9.1 Fees

LuxTrust S.A. may charge fees for the provision, usage and validation of LuxTrust Server and Code Signing 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 CP, 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.

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 CPS [6] 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 CPS [6].
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 CPS [6] 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 CPS [6] 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 title, copyrights, trademarks, service marks, patents, patent applications and all other intellectual proprietary rights now known or hereafter recognised in any jurisdiction (the IP Rights) in and to LuxTrust's technology, web sites, documentation, products and services (the Proprietary Materials) are owned and will continue to be exclusively owned by LuxTrust S.A. and/or its licensors. LuxTrust's contractors and / or subcontractors agree to make no claim of interest in or to any such IP Rights. LuxTrust's contractors and / or subcontractors acknowledge that no title to the IP Rights in and to the Proprietary Materials is transferred to them and that they do not obtain any rights, express or implied, in any Proprietary Materials other than the rights expressly granted in the CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

LuxTrust S.A., through its LTQCA issues X509 v3-compatible Certificates (ISO 9594-8).

LuxTrust S.A., through its LTQCA issues Certificates compliant with ETSI TS 102 042 Qualified 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 CP (and indicated in the Certificate in accordance with Section 7.1) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with the LuxTrust CPS [6].

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

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 CP, the verification procedures, and the LuxTrust CPS as applicable at the time of issuance. In addition other warranties may be implied in this CP definition by operation of law.

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

In certain cases described in the CPS [6], 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 CP 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 LTQCA.

Please refer to the LuxTrust CPS [6] for further details.

9.6.2 RA representations and warranties

The CRA is under a contractual obligation to comply scrupulously with the LuxTrust CPS, with the relevant section of the present CP (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 CP and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the present CP (e.g., but not limited to, 1.3.3, 1.4, 4, 4.1.2.3, 4.5.1, 9).

In particular, the Subscriber is liable towards Relying Parties for any use that is made of his/her 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 CPS [6] 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 CP and of the LuxTrust CPS and associated conditions for Relying Parties (in particular section 4.5.2 and 4.9.6 of the present CP).
- 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 section 4.5.2 and 4.9.6 of the present CP.
- Without prejudice to the warranties provided in the present CP or in the LuxTrust CPS, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- If a Relying Party relies on a Certificate without following the above rules, 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 otify LuxTrust S.A. acting as CSP.

Please refer to the LuxTrust CPS [6] 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 CP and in the applicable legislation, LuxTrust S.A. acting as CSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. LuxTrust S.A. does not warrant "non repudiation" of any Certificate or message. LuxTrust S.A. does not warrant any software.

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

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

c) 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, suspends or revokes, or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim.

d) 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 CPS [6] 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 CP (e.g., but not limited to section 9) and to the extent permitted by law.

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

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

9.9 Indemnities

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

9.10 Term and termination

The present CP 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 CP shall be in writing and shall be sent, except provided explicitly in the present CP, 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 CP.
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 CP 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 CP 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 CP 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 CP. 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 CP, 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 CP.
Minor changes to this CP do 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 CP 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 CP.

9.15 Compliance with applicable law

The present CP 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 Qualified CA, the following information in all Certificates it issues:

- Terms and conditions described in the present CP and in the LuxTrust CPS;
- 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 LTQCA uses computer-based and text based pointers that include URLs, OIDs, etc.