# LuxTrust Certificates issued to Natural Persons by a Qualified CA

**Version number: 1.6**

**Publication Date: 13/04/2012**

**Effective Date : 11/04/2012**

**Document O.I.D : 1.3.171.1.1.2.4.0.*1(version).4(sub-version)***

CP oid : 1.3.171.1.1.2.4.1 (QCP+ certificates supporting Qualified Electronic Signatures)
CP oid : 1.3.171.1.1.2.4.2 (NCP+ certificates supporting Authentication & Encryption)
CP oid : 1.3.171.1.1.2.4.3 (QCP certificates supporting AdES with a Qualified Certificate)
CP oid : 1.3.171.1.1.2.4.4 (NCP certificates supporting Authentication & Encryption)
CP oid : 1.3.171.1.1.2.4.5 (NCP Signing Server certificates supporting Signature, Authentication & Encryption)

# Document Information

| | |
|---|---|
| **Document title:** | LuxTrust Certificates issued to Natural Persons by a Qualified CA |
| **Document Code** | |
| **Project Reference:** | LuxTrust S.A. |
| **Document Type** | Certificate Policy |
| **Document Distribution List** | All |
| **Document Classification** | Public |
| **Document Owner** | CSP Board |

# Version History

| Version | Who | Date | Reason of modification |
|---|---|---|---|
| 1.1 | PHI<br>GMU | 10/04/2009<br>20/05/2009 | modifications to conform to EDP audit requirements<br>corrected OID |
| 1.2 | PHI | 28/10/2009 | insertion of ILNAS logo including accreditation reference and technical standards reference |
| 1.3 | PHI | 15/12/2010 | modifications to conform to ILNAS requirements |
| 1.4 | MSC | 20/07/2011 | New template, annual review and changes to certificate validity |
| 1.5 | YNU | 27/03/2012 | Update Signing Server NCP Certificate issuing mode |
| 1.6 | YNU | 12/04/2012 | Typo update |
| | | | |
| | | | |
| | | | |
| | | | |

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

[3] RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

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

[5] ISO/IEC 9594-8|ITU-T Recommandation X.509:"Information technology – Open Systems Interconnection – The Directory : Public-key and attribute certificate frameworks".

[6] LuxTrust Certification Practice Statement oid 1.3.171.1.1.1.1.0 (latest version in force).

[7] 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.

[8] Law of 12 November 2004 on the fight against money laundering and terrorist financing.

[9] CSSF circular 05/211 on combating money laundering and terrorist financing and prevention of the use of the financial sector for the purpose of money laundering and terrorist financing.

[10] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[11] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[12] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[13] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

# 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.

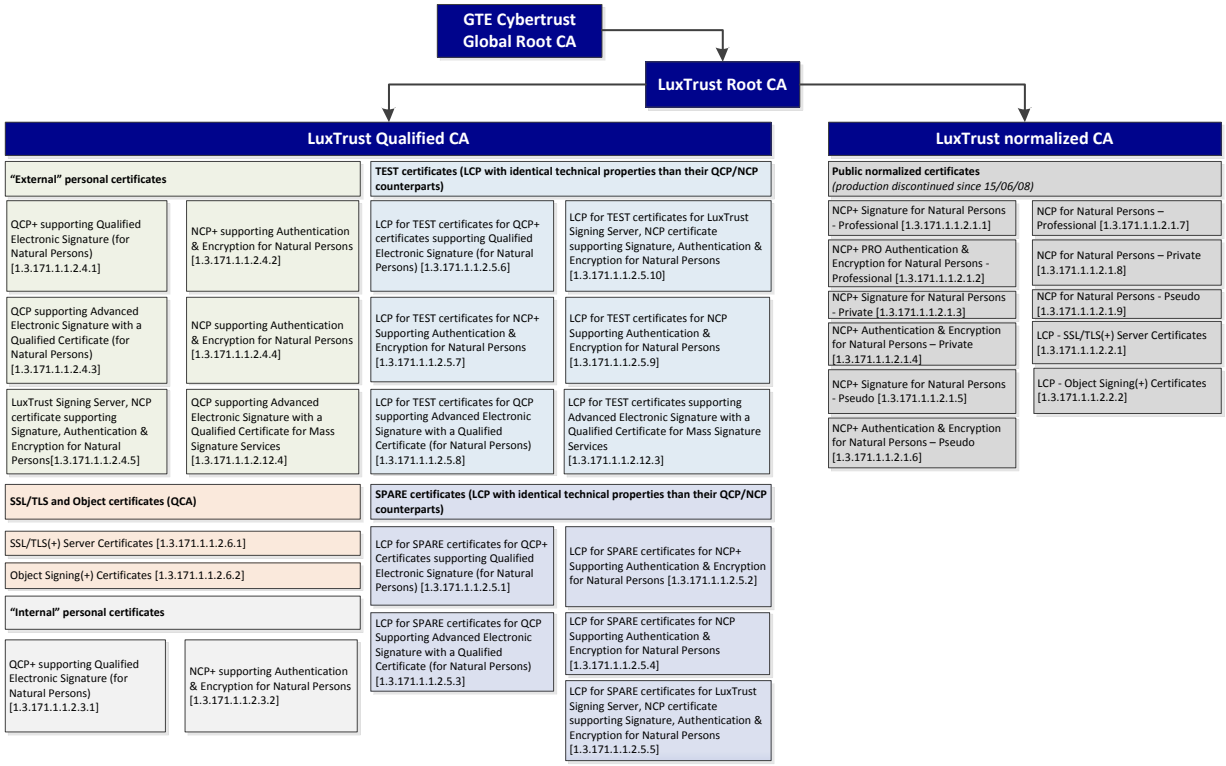


**Figure 1 - LuxTrust PKI CA hierarchy, related CPS/CPs and contractural documents**

### *1.1.4 The present document - LuxTrust Certificates issued to Natural Persons*

The present document is the Certificate Policy titled "LuxTrust Smart Card Certificates issued to Natural Persons". This Certificate Policy (CP) document indicates:

- the applicability of certificates in the form of *LuxTrust Certificates issued to Natural Person* (hereafter referred to as the "Certificates") issued by LuxTrust S.A. as Certification Service Provider (CSP) through its LuxTrust Qualified CA (LTQCA), 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 below defined Certificates.

The present CP is a set of rules, requirements and definitions determining the level of security reached by the LuxTrust Certificates issued to Natural Persons. Certificates issued in accordance with the present document include a LuxTrust Certificate Policy identifier which can be used by Relying Parties in determining the Certificates suitability and trustworthiness for a particular application. The present document specifies five types of Certificate Policies respectively issued to three types of end-user devices according to the following:

- **LuxTrust Smart Tokens that are considered as SSCD (e.g. Smartcards)**: These user devices contain two types of certificates according to two certificate policies:
  - **"LuxTrust QCP+ supporting Qualified Signature"**: ETSI TS 101 456 [2] QCP+ compliant Qualified Certificate on SSCD Hardware token (e.g. LuxTrust Smartcard), with creation of the keys by the CSP, three (3) years validity and 1024-bit key size, with a key usage limited to the support of qualified electronic signatures. This certificate policy is identified by the 1.3.171.1.1.2.4.1 oid.
  - **"LuxTrust NCP+ supporting Authentication & Encryption"**: ETSI TS 102 042 [4] NCP+ compliant Normalised Certificate on SSCD Hardware token (e.g. LuxTrust Smartcard), with creation of the keys by the CSP, three (3) years validity and 1024-bit key size, with a key usage limited to authentication purpose (to the exclusion of electronic signature)[1] and key & data encryption. This certificate policy is identified by the 1.3.171.1.1.2.4.2 oid.

  In addition to the specific LuxTrust requirements for Certificates stated in the present document, these Certificates meet the requirements for "QCP+" or "NCP+" certificate policies, respectively, as specified by ETSI TS 101 456 [2] or ETSI TS 102 042 [4] and include accordingly the respective ETSI certificate policy identifier (see section 1.2).
  These Certificates are covered by the ILNAS accreditation as registered under the reference N° 8/005 by the national registry of Accredited Certification Service Providers.

- **LuxTrust Smart Tokens that are not considered as SSCD (e.g. LuxTrust Signing Stick)**: These user devices contain two types of certificates according to two certificate policies:
  - **"LuxTrust QCP supporting Advanced Electronic Signature with a Qualified Certificate"**: ETSI TS 101 456 [2] QCP compliant Qualified Certificate on a non SSCD Hardware token (e.g. LuxTrust Signing Stick), with creation of the keys by the CSP, three (3) years validity and 2048-bit key size, with a key usage limited to the support of qualified electronic signatures. This certificate policy is identified by the 1.3.171.1.1.2.4.3 oid.
  - **"LuxTrust NCP supporting Authentication & Encryption"**: ETSI TS 102 042 [4] NCP compliant Normalised Certificate on a non SSCD Hardware token (e.g. LuxTrust Signing Stick), with creation of the keys by the CSP, three (3) years validity and 1024-bit key size, with a key usage limited to authentication purpose (to the exclusion of electronic signature)[2] and key & data encryption. This certificate policy is identified by the 1.3.171.1.1.2.4.4 oid.

  In addition to the specific LuxTrust requirements for Certificates stated in the present document, these Certificates meet the requirements for "QCP" or "NCP" certificate policies, respectively, as specified by ETSI TS 101 456 [2] or ETSI TS 102 042 [4] and include accordingly the respective ETSI certificate policy identifier (see section 1.2).
  These Certificates are covered by the ILNAS accreditation as registered under the reference N° 8/005 by the national registry of Accredited Certification Service Providers.

- **LuxTrust Signing Server (i.e. virtual smartcard) that is not considered as SSCD**: These centralised user devices contain one type of certificate according to one certificate policy:
  - **"LuxTrust NCP supporting Signature, Authentication & Encryption"**: ETSI TS 102 042 [4] NCP compliant Normalised Certificate on a non SSCD centralised hardware token (e.g. LuxTrust Signing Server), with creation of the keys by the CSP, three (3) years validity and 1024-bit key size, with a key usage limited to signature, authentication and key & data encryption purposes. This certificate policy is identified by the 1.3.171.1.1.2.4.5 oid.

  In addition to the specific LuxTrust requirements for Certificates stated in the present document, these Certificates meet the requirements for "NCP" certificate policies, as specified by ETSI TS 102 042 [4] and include accordingly the corresponding ETSI certificate policy identifier (see section 1.2).

These certificates are collectively called the Certificates unless they are more clearly identified.

[1] Please refer to section 1.4 of the present CP, in order to take knowledge of the usage restriction(s) 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.

[2] Please refer to section 1.4 of the present CP, in order to take knowledge of the usage restriction(s) 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.

These types of Certificates provide a high 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 can either be a physical private person identity (citizen) or a physical person identity with professional qualities/attributes.

The Certificate provides the highest degree of assurance of proper Certificate Subject authentication since in order to obtain the Certificate, unless the subscriber has already been identified according to the KYC (Know Your Customer) CSSF rules ([8], [9]) of the legal entity within which the LRA is set[3], the physical person applying (subscribing) for the Certificate must:

- be present in person when his/her application is registered by a Local Registration Authority (LRA), and
- present, for verification, his/her identity card or passport or Luxembourg residency card and, in case the professional quality should be certified, proof of his/her professional quality (e.g., representation power with regard to the associated legal person), together with any information required to support the certification process.

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 Certificate types described in the present document.

## 1.2 Document name and identification

The present document is identified by the following identifier:

*1.3.171.1.1.2.4.0.1(version).4(subversion)*

Depending on the type of token in which the private key(s) are stored and secured, this document sets out and identifies several Certificate Policies within one global Certificate Policy document titled **LuxTrust Certificates issued to Natural Persons**. In addition to the specific LuxTrust requirements stated in the present document, these Certificates meet respectively the requirements for "QCP+" or "NCP+" or "QCP", or "NCP" certificate policies, as specified respectively by ETSI TS 101 456 [2] by ETSI TS 102 042 [4] and include accordingly the respective applicable certificate policy identifier.

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

- **"LuxTrust QCP+ supporting Qualified Electronic Signature"**:
  - ETSI 101 456 QCP+ oid: **0.4.0.1456.1.1**
  - **LuxTrust oid**: 1.3.171.1.1.2.4.1
- **"LuxTrust NCP+ supporting Authentication & Encryption"**:
  - ETSI 102 042 NCP+ oid: **0.4.0.2042.1.2**
  - **LuxTrust oid**: 1.3.171.1.1.2.4.2
- **"LuxTrust QCP supporting Advanced Electronic Signature with Qualified Certificate"**:
  - ETSI 101 456 QCP oid: **0.4.0.1456.1.2**
  - **LuxTrust oid**: 1.3.171.1.1.2.4.3
- **"LuxTrust NCP supporting Authentication & Encryption"**:
  - ETSI 102 042 NCP oid: **0.4.0.2042.1.1**
  - **LuxTrust oid**: 1.3.171.1.1.2.4.4
- **"LuxTrust Signing Server NCP supporting Signature, Authentication & Encryption"**:
  - ETSI 102 042 NCP oid: **0.4.0.2042.1.1**

[3] Subscriber enrolment process for "Identified Clients" is further described in section 4.1.2.2 of the present CP. Default and other specific enrolment processes are described in section 4.1.

- **LuxTrust oid**: 1.3.171.1.1.2.4.5

## 1.3 PKI participants

The LuxTrust PKI Participants are the legal entities or set of legal entities filling the role of a participant within the LuxTrust PKI 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 Qualified Certification Authority
- Central & Local Registration Authorities
- Subscribers
- Relying Parties
- And other participants as:
  - CA Factory Services Provider
  - (Secure) Signature Creation Device 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].

### *1.3.1 Certification Authorities*

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

**Three-level CA hierarchy**

The top level root is the GTE Cybertrust Global Root managed by Cybertrust.

Within the LuxTrust PKI, the "LuxTrust Qualified CA" is used by LuxTrust S.A. acting as CSP to issue the LuxTrust 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 to Natural Persons under the present CP. This grant has been provided by the "LuxTrust Root CA" (hereafter 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 otherwise indicated, when referring to "the CA", it is expressly meant "the LuxTrust Qualified CA granted to issue LuxTrust Certificates issued to Natural Persons 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.

[4] Or "component services" as defined by [2] and [4] in their section 4.2 as the break downed services constituting the service of issuing public key certificates.

The LTQCA, as well as all supporting component services, are accredited against ETSI TS 101 456 [2] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. ILNAS is 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 the 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 [6] 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.

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

[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).

[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.

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://helpdesk.luxtrust.lu.
- By registering Subscribers for certification services
- By setting up facilities
  - For notification of changes in certified information or in information supporting certification. Note that any change to certified information shall lead to the 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://helpdesk.luxtrust.lu and https://sra.luxtrust.lu.

The provision of Central Registration Services is ensured by U-Trust consortium under 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.

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 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 Certificates related certification services in the LuxTrust Qualified CA (LTQCA) domain are either:

- physical persons identified as private persons, or
- physical persons identified as private persons entitled to represent a legal person or qualified by professional attributes (e.g., self-employed, employee, legal representative).

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 (Secure) Signature Creation Device Provider

The provision of LuxTrust Signing Server provisioning facilities, under the LuxTrust CPS [6] and in compliance with the relevant LuxTrust CPs and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured:

- by LuxTrust S.A. and Clearstream Services S.A. from the u-trust consortium for the provision of the Signing Server Services related to the operations of the Subscriber's Signature Creation (or decryption, or authentication) Device, and
- by Clearstream Services S.A. from the u-trust consortium for the provision of the Signing Server Authentication Services related to the validation of the User Activation Data allowing use of the Subscriber's Signature Creation Device.

The above mentioned companies from the u-trust consortium are constituted by legal persons that are different and independent from each other.

The provision of physical end-user (Secure) Signature Creation Device ((S)SCD) Services, namely the LuxTrust Smartcard and other smart token provisioning facilities, under the LuxTrust CPS [6], and in compliance with the relevant LuxTrust CPs and under a signed contractual agreement with LuxTrust S.A. acting as CSP, is ensured by U-Trust consortium.

#### 1.3.5.3 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.

#### 1.3.5.4 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.

#### 1.3.5.5 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*

Certificates covered by the present CP provide assurance of the personal and optionally of the professional electronic identity of a physical person.

Such a Certificate can be used to protect highly secured applications with security features such as qualified electronic signature (QCP+ Certificate with LuxTrust oid 1.3.171.1.1.2.4.1), or encryption and/or authentication (NCP+ Certificate with LuxTrust oid 1.3.171.1.1.2.4.2 or NCP Certificate with LuxTrust oid 1.3.171.1.1.2.4.4), or advanced electronic signature supported by a qualified certificate (QCP Certificate with LuxTrust oid 1.3.171.1.1.2.4.3), or a combination of signature, encryption and/or authentication (NCP Certificate with LuxTrust oid 1.3.171.1.1.2.4.5).

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 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].

Key usage and the applicability of the Certificate are certified (see the description of the Certificate content in Section 7 of the present CP) respectively as follows:

- **"LuxTrust QCP+ supporting Qualified Electronic Signature" Certificate on LuxTrust SSCD (e.g. smartcard)**: It is an ETSI TS 101 456 [2] QCP+ compliant Qualified Certificate whose key usage is limited to the support of qualified electronic signature. The keyUsage is exclusively set to nonRepudiation to the exclusion of any other usage. Electronic signatures supported by such a Certificate are Qualified 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[7].

- **"LuxTrust NCP+ supporting Authentication & Encryption" Certificate on LuxTrust SSCD (e.g. smartcard)**: It is an ETSI TS 102 042 [4] NCP+ compliant Normalised Certificate with a key usage limited to authentication purpose and key & data encryption. The keyUsage bits "digitalSignature", "dataEncryption" and "keyEncryption" are set to the exclusion of any other usage. It shall be explicitly stated in the Certificate that Electronic Signatures are **not** authorised to be computed as supported by such a Certificate, and that Relying Parties **shall not** accept such a Certificate to support valid Electronic Signatures. The only appropriate usages for such a Certificate are the strong (entity or data) authentication via non-meaningful challenge-response mechanisms, key encryption and data encryption to the exclusion of any other security mechanism, and in particular Electronic Signatures.

  ***Note**: As the usage of such a Certificate in an "authentication" mode is technically a digital signature providing data integrity and authentication of the data origin (i.e., the Subscriber whose identity is certified in the Certificate), if it is used in a process that can be legally considered as a contract establishment process, the result may lead to an Advanced Electronic Signature against neither the "signatory" nor the receiving or relying party could deny being linked to. It is not sufficient to restrict the usage to "Authentication" as it is only confirming the above. It is explicitly forbidden to "electronically sign" with such a Certificate and/or to rely on such a Certificate as supporting an Electronic Signature.*

- **"LuxTrust QCP supporting Advanced Electronic Signature with a Qualified Certificate" Certificate not on LuxTrust SSCD**: It is an ETSI TS 101 456 [2] QCP compliant Qualified Certificate whose key usage is limited to the support of advanced electronic signature supported by a qualified certificate. The keyUsage is exclusively set to nonRepudiation to the exclusion of any other usage. Electronic signatures supported by such a Certificate are

[7] The expiration of the Certificate, the cryptanalysis of the private key or of the hash function used in the digital signature process are circumstances that can no longer provide such a guarantee, unless appropriate measures have been taken, such as for example the use of timestamping services.

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[8].

- **"LuxTrust NCP supporting Authentication & Encryption" Certificate not on LuxTrust SSCD**: It is an ETSI TS 102 042 [4] NCP compliant Normalised Certificate with a key usage limited to authentication purpose and key & data encryption. The keyUsage bits "digitalSignature", "dataEncryption" and "keyEncryption" are set to the exclusion of any other usage. It shall be explicitly stated in the Certificate that Electronic Signatures are **not** authorised to be computed as supported by such a Certificate, and that Relying Parties **shall not** accept such a Certificate to support valid Electronic Signatures. The only appropriate usages for such a Certificate are the strong (entity or data) authentication via non-meaningful challenge-response mechanisms, key encryption and data encryption to the exclusion of any other security mechanism, and in particular Electronic Signatures.
  ***Note**: the above note is applicable.*

- **"LuxTrust NCP supporting Signature, Authentication & Encryption" Certificate on a non SSCD LuxTrust Signing Server**: It is an ETSI TS 102 042 [4] NCP compliant Normalised Certificate with a key usage limited to signature, authentication and/or key & data encryption purposes. The keyUsage bits "digitalSignature", "dataEncryption" and "keyEncryption" 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. 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.

### *1.4.2 Prohibited certificate uses*

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

In particular, it is explicitly **prohibited** to compute Electronic signatures as supported by a "LuxTrust NCP(+) supporting Authentication and Encryption" Certificate and Relying Parties **shall not** accept such a Certificate to support valid Electronic Signatures. The only appropriate usages for such a Certificate are the strong (entity) authentication via non-meaningful challenge-response mechanisms, key encryption and data encryption to the exclusion of any other security mechanism, and in particular Electronic Signatures.

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 in accordance with the restrictions stated in the present CP.

## 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.

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

It can be contacted via the coordinates using the following coordinates:

[8] The expiration of the Certificate, the cryptanalysis of the private key or of the hash function used in the digital signature process are circumstances that can no longer provide such a guarantee, unless appropriate measures have been taken, such as for example the use of timestamping services.

| LuxTrust contact information | |
|---|---|
| **Contact Person:** | **CSP Board Contact** |
| **Postal Address:** | LuxTrust CSP Board<br>LuxTrust S.A.<br>IVY Building<br>13-15, Parc d'Activités<br>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:<br>– It is uniquely linked to the signatory;<br>– It is capable of identifying the signatory;<br>– It is created using means that the signatory can maintain under his sole control; and<br>– 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.<br>– 14/08/2000 Luxembourg Law [7]:<br>Art. 6. « Signature » - Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé :<br>"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.<br>Elle peut être manuscrite ou électronique.<br>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:<br>– It is computationally unfeasible to find for a given output an input which maps to this output;<br>– 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:<br>– CETREL S.A.;<br>– Clearstream Services;<br>– G4S (SRA) |
| **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 |
| **ITU** | International Telecommunications Union | **SRA** | Suspension and Revocation Authority |
| **KYC** | Know Your Customer | **SRAO** | Suspension and Revocation Authority Officer |

| Acronym | Definition | Acronym | Definition |
|---|---|---|---|
| **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, are accredited against ETSI TS 101 456 [2] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. ILNAS is the accreditation entity. For further details please refer to section 8 of the present CP.

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

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

Electronic signatures supported by a certificate covered by the "**LuxTrust NCP supporting Signature, Authentication and Encryption**" Certificate Policy 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 authorised and prohibited usages of these certificates.

# 2 Publications and Repository Responsibilities

## 1.1. 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 LuxTrust CPS [6];
- 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.

## 2.1 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.

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

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

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

The CA publishes CRLs at regular intervals at https://www.luxtrust.lu/faq/crl/crl.

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

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

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

The LTQCA publishes CRLs at regular intervals at https://www.luxtrust.lu/faq/crl/crl as indicated in the LuxTrust CPS [6].

LuxTrust S.A. makes available an OCSP responder server at http://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 in force, 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://test.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

## 2.2 Time of Frequency of Publication

### *2.2.1 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.

### *2.2.2 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.

### *2.2.3 Frequency of Publication of Terms & Conditions*

An update of all relevant Terms & Conditions (including the LuxTrust CPS [6], the General Terms and Conditions and the Purchase Order) is published whenever a change occurs.

## 2.3 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.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### *3.1.1 Types of names*

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

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

The rules concerning the naming and identification of professional attributes of physical persons are the same as the legal rules applied to naming and identification of professional attributes in the Grand-Duchy of Luxembourg and of equivalent international professional attributes. More specifically, the following professional attributes values shall be used to the exclusion of any other professional naming convention:

- *Professional person (default)*
- *Professional Administrator*
- *Other titles are possible for special purpose certificates; the following may be considered:*
  - *"Employee"*
  - *"Administrator"*
  - *"CEO"*
  - *"Manager"*
  - *"Civil Servant"*

Certificates issued to private persons shall carry the following naming convention:

- *"Private Person"*

The detailed structure of the Certificates 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:

*For the LuxTrust Root CA Certificates:*

| | |
|---|---|
| **Country (C)** | LU |
| **Organization (O)** | LuxTrust S.A. |
| **Common Name (CN)** | LuxTrust Root CA |

*For the LuxTrust Qualified CA Certificates (issued by the LuxTrust Root CA):*

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

### *3.1.2 Need for names to be meaningful*

Unless pseudonyms are used, the names used under this CP shall be meaningful as identifying physical persons and as identifying optional professional attributes.
RFC 822 names may not be meaningful.

### 3.1.3 Anonymity or pseudonymity of subscribers

Subscribers may choose to receive a Certificate certifying their identity as a pseudonym. The Certificate shall clearly identify this choice by indicating the mention "Pseudonym :" before the allocated pseudonymUniqueIdentifier in the appropriate subject attributes as specified in section 7.1 of the present CP. The pseudonymUniqueIdentifier shall be uniquely determined at registration by the Local Registration Authority according to the following scheme:

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

In case the Subscriber chooses to receive a Certificate certifying his identity as a pseudonym, the LRAO registering the Subscriber shall retain full identification of the Subscriber with regards to his/her allocated pseudonymUniqueIdentifier. The LRAO shall retain this information as confidential and shall never disclose this information to third parties unless as foreseen by law.

### 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 Subject.

### 3.1.5 Uniqueness of names

The full combination of the Subject Attributes (Distinguished name) has to be unique.

### 3.1.6 Recognition, authentication, and role of trademarks

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

## 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 are detailed in the next sub-sections. Revalidation of these identities shall occur every three (3) years for "LuxTrust QCP+" labelled Certificates, and for "LuxTrust NCP+" labelled Certificates. The same procedure as for the initial identity validation shall be followed at that time, unless online re-key is performed (see section 4.6 to 4.9).

### 3.2.1 Method to prove possession of private key

The key generation process is ensured by the CSP in compliance with the ETSI TS 101 456 QCP(+) and ETSI TS 102 042 NCP(+) technical specifications respectively. The (Secure) Signature Creation Device and/or the private key activation data may be sent to the Certificate Subject by postal mail or delivered to the Certificate Subject according to a physical presentation based procedure that is strictly followed by the LRAO registering the Subscriber (Certificate Subject) and that is provided by LuxTrust S.A. as an internal and auditable document. When both SSCD and Activation Data are delivered to the Subscriber, these items are delivered securely using two separated channels.

The method used to prove possession of the private key by the Subscriber is thus ensured by a combination of a key generation process ensured by the CSP and the secure delivery of the SSCD and/or the Activation Data to the Subscriber using two separated channels. Face-to-face based procedure is by default mandatory unless otherwise authorised. See section 4 of the present CP for further details.
As stated in section 4.12, Subscriber's key back-up and key recovery are not allowed except for the sole purpose of and in the context of LuxTrust Signing Server Account disaster recovery as stated and ruled by the LuxTrust CPS [6]. **Subscriber's key escrow is never allowed**.

### 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).
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 or passport or Luxembourg residency card) of one of the physical persons who are a legal representative of the legal person; in case this person cannot be physically present at the LRA, the copy must be certified by a competent authority (embassy, consulate, notary, municipality, police office, bank from the first order) and be accompanied by a legalisation of the signature of this authority.
5. The information about their legal address, civil state, and profession;
6. In case a company established in a non-Luxembourg jurisdiction is found as founder or administrator or signatory in the LuxTrust registration process, LuxTrust S.A. reserves right to ask for constitutive documents of this company (points 1 & 2 above), the declaration of the commercial beneficiary and the origin of the funds of the company, as well as 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

Unless the Subscriber has already been identified by the legal person, within which the RA network operates, through a face-to-face identification following the "Know Your Customer" (KYC) rules set by the CSSF ([8], [9]), identification and authentication requirements for an individual Subscriber shall include the following:

- The Subscriber shall be present in person in front of an LRAO during registration process;
- The Subscriber shall provide for verification a valid and authentic identity card or identity passport or Luxembourg residency card;
- The LRAO shall verify the authenticity and validity of the provided identity proof according to (legal) procedures provided by LuxTrust S.A. and against stolen identity proof lists.

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

### 3.2.4 Non-verified subscriber information

Subscriber's E-mail address of physical private persons 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 un-suspension 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 LRA, the CRA or LuxTrust S.A. may apply for revocation, suspension or un-suspension following suspension, of the Certificate. The Subscriber and, where applicable, the legal representative (or his duly appointed delegate) is notified of the suspension or un-suspension following suspension of the Certificate.

Applications and reports relating to a revocation, suspension or un-suspension following suspension are processed on receipt, in a timely manner[9], and are authenticated as described in section 4.9.3, 4.9.16 and 4.9.15 respectively.

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

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

[9] 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 appropriate measures to make sure that the situation is corrected (including revocation of the Certificate if applicable).

## 4.1 Certificate Application

### *4.1.1 Who can submit a certificate application*

Unless otherwise specified by law, LuxTrust applicable standards, or the applicable CP, any physical person can submit a Certificate application.

The 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 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 LRA mission, in the context of Subscriber registration, is to verify that the Subscriber is indeed the person (s)he claims to be and to validate the information that is requested to be certified 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 Local 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 as described in section 3.2 and, accordingly, in case the professional quality should be certified, to prove his/her professional quality, together with any information supporting his/her registration.

As detailed in the next sub-sections hereafter, we can distinguish the following scenarios for enrolment process of the Subscribers:

- Default Subscriber enrolment process with face-to-face presentation of the Subscriber at an LRA;
- "Identified client" enrolment process inheriting from a previous KYC compliant banking client identification process;
- "New foreign client" enrolment process.

The LRA guarantees the accuracy, at the time of registration, of all information contained in the certificate request as sent to the Central Registration Authority, and that the Certificate Subscriber (identified in the certificate request as the "to be certified entity",

and thus the Subject of the Certificate) has 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 LRAO collates and securely archives all the submitted documents and uses the RA Graphical User Interface to send the request for the LuxTrust Certificates (including the related end-user signature creation device, either SSCD, non SSCD or Signing Server) to the Central Registration Authority (CRA). The CRA then performs a final validity check, on receipt of the Subscriber's registration information received from the LRAO. In case the request is accepted by the CRA, the CRA requests the Signature Creation Device Issuing Authority for the creation of the key-pair(s) and Certificate(s) by 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 (via his/her LRAO in case of pseudonym Subscriber) and set out the grounds for this rejection.

The LuxTrust Certificates are generated in a suspended mode by the LuxTrust LTQCA (Factory). This suspension notification is immediately available in the related CRL and via the LuxTrust Validation Services. By default, the requested LuxTrust Signature Creation Device (SSCD or non SSCD) and its related Activation Data will be sent per postal mail to the Subscriber using delayed channels according to procedures used in the banking sector and in compliance with the CSSF recommendations. Re-activation of the suspended Certificates can be performed online by the Subscriber through a web based activation and test module provided on the LuxTrust website. The activation step is secured through mutual authentication based SSL connection and presentation of the Subscriber activation code selected by the Subscriber during registration process.

#### 4.1.2.1 Default Subscriber enrolment process

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

Registration preparation

The Subscriber must obtain the Order Form and the General Terms and Conditions for the Certificate (hereafter referred to as "the Order Form" and "the General Terms and Conditions") from LuxTrust S.A. acting as CSP. These, together with the present CP and the LuxTrust 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 or to obtain the documents from an LRA approved by the CSP. The correct versions of these documents are deemed to be available on: https://repository.luxtrust.lu.

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

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

By signing the Order Form, the Subscriber and, if applicable, the Subscriber's organisation accept the General Terms and Conditions, the present CP and the LuxTrust CPS [6].

*Online Registration Preparation*

In order to facilitate the Subscriber registration preparation, to reduce the amount of errors, an end-user web-based registration preparation interface is available. This interface will present the Subscriber with a convenient & intelligent electronic form to collect information needed for registration. This form will dynamically present appropriate fields in function of the choices of the Subscriber: Subscriber's data, type of registration process (e.g., default, identified client), type of requested LuxTrust product ((secure) signature creation device), data for (secure) signature creation device and PIN-mailer delivery, etc. Once the Subscriber's registration information filled in, the intelligent form will provide the Subscriber with a printer friendly version of the LuxTrust Subscriber Order Form and will remind him/her the supporting registration documents that the Subscriber must collect and bring to the LRA in order to validate his/her registration.

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

*Supporting registration documents*

The Subscriber applying for the LuxTrust Certificate(s) must[10] present himself, in person, to one of the LRAs authorised under the present CP. The Subscriber may arrange a meeting with an LRA Officer (LRAO) and go there in person, bringing with him/her the following documents:

**a. The Subscriber is an employee or a member of an organisation**

- The order form, duly filled in and signed;
- A (two-sided) copy of the Subscriber's valid identity card or passport or Luxembourg residency card. This copy must be signed by the Subscriber;
- A (two-sided) copy of a valid identity card or passport or Luxembourg residency card, 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;
- 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.

**b. The Subscriber is self-employed or is private physical person**

- The order form, duly filled in and signed;
- A (two-sided) copy of the Subscriber's valid identity card or passport or Luxembourg residency card. The copy must be signed by the Subscriber;

If the Subscriber would want to have his self-employed professional identity certified:

- A proof of his professional status as legally acceptable in Grand-Duchy of Luxembourg.

**c. The Subscriber is an organisation administrator or legal representative**

- The order form, duly filled in and signed;
- A (two-sided) copy of the Subscriber's valid identity card or passport or Luxembourg residency card. The copy must be signed by the Subscriber;
- 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.

Unless identified as stated in section 1.1.3 of the current CP, the Subscriber must make an appointment with the LRAO at the LRA of his/her choice provided it is an authorised LRA(O) under the present CP.

**Enrolment of a new LuxTrust Certificate Subscriber: high level overview**

The following process is applicable in the context of a non Virtual Smartcard product (Signing Server), i.e., when having requested a physical end-user signature creation device, being either an SSCD Smartcard (e.g., smartcard or any compliant token) or a non SSCD Signing Stick (e.g. Signing Stick or any compliant token).

[10] This physical presentation is not required in the context of "Identified client" enrolment process as described in section 4.1.2.2.

0. Registration Preparation step: As indicated above, the Subscriber connects on the LuxTrust RA website, fills in his Subscriber Order Form (either from own initiative, either upon invitation), and collates necessary registration supporting documents.
1. Unless the Subscriber has already been identified according to the KYC (Know Your Customer) CSSF rules ([8], [9]) of the legal entity within which the LRA is set, the Subscriber presents himself to the LRA Officer (LRAO) with the LuxTrust Order Form correctly and duly filled in accompanied with the required registration supporting documents when applicable.[11]
2. The LRAO will be able to register the personal details and perform a face-to-face identification and authentication, and request the Subscriber Certificate (either SSCD, non SSCD or Virtual as being Signing Server conformant to the requested instance of (secure) signature creation device).
3. The LRAO forwards to the Central RA only:
    a. The required information that is deemed to be certified as required by the Certificate Profile (see section 7.1 of the present CP), and
    b. Details for sending the "Certificate PIN/PUK-Letter" to the Subscriber (so called Shipping Data).
4. The Central RA will initiate the creation of a LuxTrust Certificate for the Subscriber's profile to the LuxTrust Certificate Issuing Authority.
5. The (S)SCD Issuing Authority will generate the Subscriber key-pairs on a Non-personalised card, and extract the public keys.
6. The (S)SCD Issuing Authority responds to the CRA with the Public Keys to be certified.
7. The Central RA will request the Certificates from the Certificate Factory (CA).
8. The CA generates the Certificate (in a suspended mode), and, in case the Subscriber has agreed so, publishes them on the LuxTrust Directory Server.
9. The CA responds with the Certificate to the Central RA.
10. The Central RA will send the Certificates back to the (S)SCD Issuing Authority
11. The (S)SCD Issuing Authority will add the Certificates to the physical (Secure) Signature Creation Device, and send it together with the corresponding "(S)SCD PIN/PUK-Letter" securely to the Central RA.
12. The Central RA sends the PIN/PUK-Letter to the Subscriber's Shipping Data coordinates, and the (S)SCD through two separate and delayed sendings[12].
13. Change initial PIN: Right after reception of the (S)SCD and the related PIN-PUK Letter, the Subscriber must first change its initial PIN-code. For that purpose, the Subscriber must install the LuxTrust Middleware and, in case of a smartcard, a smartcard reader on its computer.
14. Certificates un-suspension, testing and selection of Suspension/Revocation password: A last step is requested to the Subscriber by browsing to a URL link provided by the LRAO on which the Subscriber can un-suspend (re-activate) the Certificates by making use of the activation code selected at establishment of the Purchase Order, test his Certificates and select his Suspension/Revocation password online together with reminder facilities. This step can be performed by the Subscriber when back home or at office.

The Shipping Data, mentioned here above, are (detailed) coordinates of the Subscriber needed to send per postal mail the Subscriber's Hardware token and the related PIN/PUK-Letter.

**Enrolment of a LuxTrust Signing Server Account Subscriber: high level overview**

0. Registration Preparation step: As indicated above, the Subscriber connects on the LuxTrust RA website, fills in his Subscriber Order Form (either from own initiative, either upon invitation), and collates necessary registration supporting documents.

[11] If the Subscriber is an identified person as stated in section 1.1.3 of the current CP the Subscriber can forward the above mentioned documents via postal mail to the LRA.

[12] The physical (S)SCD and, with two days delay, the related PIN-PUK Letter will be sent to the Subscriber within 5 working days (postal date) from the validation of the application by the LRA.

15. Unless the Subscriber has already been identified according to the KYC (Know Your Customer) CSSF rules ([8], [9]) of the legal entity within which the LRA is set, the Subscriber presents himself to the LRA Officer (LRAO) with the LuxTrust Order Form correctly and duly filled in, accompanied with the required registration supporting documents when applicable.[13]

1. The LRAO will be able to register the personal details and perform a face-to-face identification and authentication.[14]
2. The LRAO will be able to hand-over a pre-generated OTP-Credential (One Time Password Credential, e.g. a Token) to the Subscriber. The Serial number of this OTP-Credential is noted by the LRA and will be communicated to LuxTrust CRA.[15]
3. The LRAO forwards to the Central RA (CRA) only the information:
    a. That is deemed to be certified in the Certificate as required by the Certificate Profile (see section 7.1 of the present CP),
    b. The Serial Number of the OTP-Credential issued to this Subscriber by the LRAO, and
    c. Details for sending the "Signing Server Account PIN-Letter" to the Subscriber (so called Shipping Data).
4. The Central RA will initiate the creation of the Subscriber's profile by the LuxTrust Signing Server Authority on the LuxTrust Signing Server.
5. The LuxTrust Signing Server responds to the CRA with the User-ID & Public Key which was generated for this Subscriber.
6. The Central RA will request the Certificate from the Certificate Factory (CA).
7. The CA generates the Certificate, and, in case the Subscriber has agreed so, publishes it on the LuxTrust Directory Server.
8. The CA responds with the Certificate to the Central RA.
9. The Central RA will send the Certificate back to the Signing Server.
10. The Signing Server generates the Static Password, and sends the User-ID & Static Password ("Signing Server Account PIN-Letter") securely to the Central RA.
11. The Central RA sends the "Signing Server Account PIN-Letter" securely to the Subscriber's shipping data under secure envelope.
12. The CRA sends the UID / OTP-Credential Serial Number information to the LuxTrust Signing Server Authentication Service Provider.
13. Certificate testing and selection of Suspension/Revocation password: A last step is requested to the Subscriber by browsing to a URL link provided by the LRAO on which the Subscriber can test and activate his Certificate and select his Suspension/Revocation password online together with reminder facilities. This step can be performed by the Subscriber when back home or at office.

The OTP-Credential, mentioned here above, refers to the Authentication Token as provided by the Signing Server Authentication Service Provider. These authorised OTP-Credentials under the present CP are the authorised OTP-Credentials as specified by the LuxTrust CPS [6].

The Shipping Data, mentioned here above, are detailed coordinates of the Subscriber needed to send the Subscriber's PIN-Letter per postal mail. This sending can, if required, be anonymised with regards to the Subscriber's coordinates (to protect Subscriber delivery information, in case of pseudonym for example) in the sense that the shipping coordinates that are sent to the CRA can be the LRA(O) coordinates. In that case, the LRAO will then be in charge of delivering the un-tampered secured envelope containing the applicant's PIN-Letter to the identified and authenticated corresponding Subscriber.

[13] If the Subscriber is an identified person as stated in section 1.1.3 of the current CP the Subscriber can forward the above mentioned documents via postal mail to the LRA.

[14] If the Subscriber is an identified person as stated in section 1.1.3 of the current CP the Subscriber can forward the above mentioned documents via postal mail to the LRA.

[15] In case of a registration of an already identified person as stated in section 1.1.3 of the current CP the pre-generated OTP-Credential (One Time Password Credential, e.g. a Token) will be sent to the Subscriber shipping address via postal mail.

Post-registration steps

The archival of the registration related information is the closing task of the LRAO once registration of a new Subscriber is performed. It means for the LRAO 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.

The detailed procedures and guidelines for LRA Officers are collected in the document "LuxTrust Local 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].

#### 4.1.2.2 Subscriber enrolment process for "Identified Clients"

Identified Clients are defined as clients who have already been previously identified according to the "Know Your Customer" (KYC) rules imposed by the CSSF to the Luxembourgian financial institutions, thus in principle every person who owns a banking account in a financial institution in the Grand-Duchy of Luxembourg.

Those KYC identification rules being even stricter than LuxTrust requirements, have been accepted by LuxTrust as a substitution to the mandatory physical presence requirement of Subscribers during initial enrolment process. Those KYC identification rules are also compliant with ETSI 101 456 identification requirements [2].

Identified Clients are not required to present in person to a LRA in order to validate their enrolment. They only need to send their Purchase Order and the requested annexes per postal mail to their financial institution acting as LuxTrust LRA under a signed agreement with LuxTrust S.A. This financial institution will validate the Subscriber application against the KYC identification data available in its organisation in order to validate the LuxTrust Certificate enrolment.

This procedure can be implemented by a LRA that has a financial institution status in the Grand-Duchy of Luxembourg and that has already identified its customers according to a strong (KYC) procedure endorsed by the CSSF.

The Identified Client must however provide its explicit agreement to such a reuse of its KYC identification data. The Subscriber must therefore explicitly opt in for this option in its Purchase Order in order to initiate this enrolment process. This explicit agreement is also repeated on the Purchase Order where the Subscriber's handwritten signature is requested.

From the financial institution LRA point of view, this procedure is initiated by its client who sends in the Purchase Order and its annexes. The Subscriber must also annex a proof of payment according to the instructions available on the LuxTrust website (https://ra.luxtrust.lu). From the reception of this postal mail, the LRAO validates that all requested documents are provided, duly filled in, dated and signed. The LRAO then verifies the claimed identity of the client against the KYC client identification stored in the financial institution systems. Subscriber's name, date and place of birth must match. Photo comparison and validation of other identification information are optional but recommended by LuxTrust. The LRAO checks whether the payment has been done. The LRAO then uses its LRAO tool to forward the enrolment data to the CRA as described from step 3 in the default enrolment process (see above section 4.1.2.1).

The archival of the registration related information is the closing task of the LRAO once registration of a new Subscriber is performed. It means for the LRAO 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.

The detailed procedures and guidelines for LRA Officers are collected in the document "LuxTrust Local 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].

#### 4.1.2.3 Subscriber enrolment process for "New Foreign Clients"

**Identification according to KYC rules**

The identification of new foreign clients or employees of new foreign clients, who cannot present themselves in person to a LuxTrust LRA and who are not registered as existing clients within a LuxTrust LRA can be performed according to the same remote identification rules used by the financial institution LRAs for entering in traditional business relations with its foreign customers.

These remote identification rules must have been previously validated by the CSSF in the context of the KYC rules [8], [9].

The financial institution that wish to make use of this type of remote identification in the context of the present CP, must inform LuxTrust in advance. In addition, it must provide LuxTrust, on demand, with the internal KYC rules that has been used in the context of any remote identification.

Enrolment process is then similar to the one described in section 4.1.2.2.

**Identification by a Notary and Apostille**

LuxTrust allows the remote identification of foreign Subscribers through a notary and apostille in conformance with the international regulations in this area. This procedure can be implemented by any LRA authorised to act in the context of the present CP. This procedure requires the production of the following documents:

- A copy of the identity card or passport or Luxembourg residency card of the related Subscriber, duly legalised by a notary;
- This copy must be accompanied by an Apostille[16]. This Apostille will attest the authenticity of the signature of the person who has signed the document (i.e. the notary), the quality in which he has acted, and when applicable of the seal or stamp placed on the document.

The copy of the identity document and of the Apostille must be readable according to standards applicable in the Grand-Duchy of Luxembourg (e.g., alphabet, language, etc.).

The foreign Subscriber must add these documents instead of the signed copy of the identity document required in the default procedure and send its registration file, including these documents and all other requested documents to a LuxTrust LRA authorised under the present CP that accepts this identification mode.

Enrolment process is then similar to the one described in section 4.1.2.2.

#### 4.1.2.4 Other PKI Participants enrolment process

The enrolment process for PKI Participants other than Subscribers is described and ruled in the LuxTrust CPS [6].

#### 4.1.2.5 PKI Participants responsibilities related to enrolment process

***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

[16] **Apostille** is a French word which means a *certification*. It is commonly used in English to refer to the legalisation of a document for international use under the terms of the 1961 Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents. Documents which have been notarised by a notary public, and certain other documents, and then certified with a conformant apostille are accepted for legal use in all the nations that have signed the Hague Convention.

the corresponding enrolment (registration) procedures. The Subscriber is responsible for the accuracy of the data provided during enrolment process.

- The Subscriber must agree to the retention - for a period of 10 years from the date of expiry of the last Subscriber Certificate - by the CSP and LRA of all information used for the purposes of registration, for the provision of a (S)SCD[17] 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 force, in the Order Form and in the General Terms and Conditions relating thereto, and in the present CP.

***LRA – CRA responsibilities***

The LRA is under a contractual obligation to comply scrupulously with the registration procedures described in the LuxTrust CPS [6] and within related LuxTrust internal LRA procedures.

The LRA 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 any optional information about optional professional status;
- Any application for Certificates submitted to the CA is complete, accurate, valid and duly authorised.
- The LRA Officer (LRAO) 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 LRAO checks the identity of the Subscriber, and when applicable Subscriber's organisation representative(s), on the basis of valid identity documents recognised under Grand-Duchy of Luxembourg law. These identity documents (identity card, passport, Luxembourg residency card) must indicate the full name (last name and first name(s)), date and place of birth of its legitimate owner.
- The LRAO also verifies any optional information relating to the Subscriber's professional status for the purposes of certification, 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 LRAO validates the documentation supplied as proof of the existence of this relationship.
- The LRAO 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 professional status, including any reference numbers on documentation used for this verification as well as any limitations on its validity.
  - A copy of the contractual agreement signed by the Subscriber, including the latter's agreement to all obligations incumbent on him/her.
  - This information is retained by the LRA for a period of 10 years from the date of expiry of the last Certificate linked to the Subscriber's registration by the LRA.
- The LRAO 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 LRA 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;

[17] LuxTrust Virtual Smart Cards or Signing Server Accounts are not considered as SSCD but SCD.

- Logical access to any software;
- LRAOs 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 LRA 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.

Similar responsibilities are applicable to the CRA(O) with regards to the registration procedures as described in the LuxTrust CPS [6] and within related LuxTrust internal CRA procedures as part of the LuxTrust CPS [6].

*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*

Unless the Certificate Subscriber has already been identified, by the RA Network, as described in section 3.2 of the present CP, validation of Certificate requests will require the Certificate Subscriber to present him-/herself to a Local Registration Authority (LRA) when face-to-face registration is required by the applicable CP. The LRA performs the Subscribers identification and authentication and guarantees the accuracy, at the time of registration, of all information contained in the certificate request as sent to the Central Registration Authority, and that the certificate holder (Subscriber identified in the certificate request as the to be certified entity, and then as the Subject of the Certificate) has 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 LRAO sends the Certificate request to the Central Registration Authority (CRA). The CRA then performs a final validity check, on receipt of the Subscriber's registration information received from the LRAO. In case the request is accepted by the CRA, the CRA requests the Signature Creation Device Issuing Authority for the creation of the key-pair(s) and Certificate(s) by the Certificate Factory (CA).

When the application for the Certificate is rejected by the CRA, the latter must inform the Subscriber (via its LRAO in case of pseudonym 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 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 LRA, or SRA to the CRA in order to request the CA to revoke the Certificate and take the appropriate measures to enable the reissuing of a Certificate. The procedure used for this purpose is described in Section 4.9 of the present 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 CA, unless specifically otherwise chosen by the Subscriber in the Subscriber Agreement, the Certificate is not published in the LuxTrust Public Repository of Certificates (Directory). This repository is in the public domain and is accessible at all times as stated in Section 2 of the present CP.

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

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

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

## 4.5 Key pair and certificate usage

The responsibilities relating to the use of keys and Certificates are defined in the next sub-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[18] 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

[18] Unless in the context of LuxTrust Virtual Smart Cards (Signing Serve Accounts).

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., Activation Code, PIN-code or password(s)) used to prevent unauthorised use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without adequate protection. The Subscriber must never leave the Private Key or the Private Key Activation Data unsupervised when it is not locked (e.g., leave it unsupervised in a workstation 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[19]; and/or,
  - The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part)

  The Certificate revocation process is then started immediately. The suspension and revocation process and procedures are set out in Section 4.9 of the present 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 shall ensure the destruction of the (S)SCD or shall give it back to a LuxTrust LRA for destruction once all Certificates on the (S)SCD are either revoked or expired.[18]
- The LuxTrust Signing Server Account Subscriber accepts that his certified private key shall be destroyed once expired or revoked.

### *4.5.2 Relying Party public key and Certificate usage*

Relying Parties 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 the present 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.

[19] 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).

## 4.7 Certificate re-key

**Certificate online re-key** is authorised under the condition that the initial Certificate is still valid (not suspended, not revoked and not expired), and that the certified information is still valid, and that the Subscriber electronically signs (supported by a LuxTrust valid certificate) an electronic certificate on-line re-key contract with the CSP for processing the request. The CSP shall take care of the re-key process:

- either on a new physical LuxTrust (S)SCD and of the secure delivery of this new (S)SCD and associated Activation Data (via two separated channels),
- or on a new LuxTrust Signing Server Account and of the secure delivery of the associated OTP Token and the associated LuxTrust Signing Server Account information and Activation Data.

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

The only data which can be updated by the subject is the email address(es). The others subject data contain the same values as the certificate on which the re-key is based on.

In case of Certificates (online) re-key on LuxTrust (S)SCD, and when Subscriber key generation is done by the CSP, a new (S)SCD is issued while the revoked or expired (S)SCD or the (S)SCD that contains only revoked Certificates shall be destroyed according to the LuxTrust CPS [6]. In case of Certificates re-key on LuxTrust Signing Server Account, old keys related to revoked Certificates shall be destroyed according to the LuxTrust CPS [6].

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

## 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 and suspension

The suspension, un-suspension and 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, LRA and SRA functions shall be functionally separated to ensure separation of duties.

LRAs shall in any case intervene in the process of un-suspension of Certificates, and in revocation of Subscriber's Certificate(s) when the physical presence of the requestor is demanded. 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 and LRA may initiate a suspension or revocation process in case of doubt on the *sanity* of a Subscriber. It is an obligation for all entities subject to PSF regulation. The CRA shall be a PSF and will thus be in possession of specific blacklists. As a consequence, it is an obligation for CRA to initiate suspension and/or revocation whenever necessary.

For the sake of clarity, a Certificate status can be either valid, or suspended or revoked. Suspension is a temporary and reversible status. A Certificate can be un-suspended to become valid again. The revocation process is irreversible. Once revoked, the Certificate cannot be unrevoked. Once the LuxTrust Certificate is revoked (or expired), the corresponding private key is destroyed in accordance with the LuxTrust CPS [6]. The Smartcard whose both Certificates have been revoked shall be destroyed by the Certificate Subscriber itself or brought back by the Subscriber to a LuxTrust LRA for destroying in accordance with the LuxTrust CPS [6].

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

Detailed procedures related to the suspension, un-suspension, and 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].

### *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 LRA and SRA request promptly to the LTQCA the suspension of a Certificate (or a pair of Certificates in case of a LuxTrust physical (S)SCD Subscriber) 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 LRA 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.

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

### *4.9.2 Who can request revocation*

Revocation can be requested to the SRA by the Subscriber, by the Subscriber's organisation if applicable, by the LRA, and/or directly initiated by the CRA under the circumstances and conditions as set forth in the present CP and the LuxTrust CPS [6].

Under specific circumstances, LuxTrust S.A. acting as CSP may request revocation to the SRA of any Certificate in accordance with the LuxTrust CPS [6]. E.g. specific circumstances may be that a LuxTrust Certificate Subscriber appears in a Blacklist as defined and in accordance with the PSF rules.

The suspension, un-suspension and revocation processes are managed by the Suspension and Revocation Authority (SRA), through the CRA towards the LTQCA who technically suspends or revokes a Certificate. 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 form and/or procedure to be used for applying for the (suspension, un-suspension or) revocation of a Certificate can be obtained from the LuxTrust SRA webpage available at the following url: https://sra.luxtrust.lu.

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

**Revocation of an existing LuxTrust Subscriber: process overview**

The revocation requestor may request revocation of its certificate using one of the following possibilities:

a. If the requestor is still in possession of the certificate he wants to revoke and if that certificate is still valid, the requestor can revoke the certificate 24/7 over the LuxTrust website under https://revoke.luxtrust.lu. The requestor will therefore have to validly login to the online revocation functionality using the certificate which should be revoked. He will then have to indicate the valid revocation challenge indicated on his PIN-Mailer and sign the request validly with the certificate which is to be revoked. If all elements are correct, the revocation is executed immediately.

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

c. Go to an RA (or CRA or LRA): The revocation requestor goes to an RA (or CRA, or LRA) with the request to revoke a Certificate. When the RA (or CRA, or LRA) receives the request, it will register the details of the revocation requestor and will validate his/her identity by validating his identity card, passport or Luxembourg residency card. The revocation requestor will need to fill a revocation request form and sign it. The requestor may also download this request form previously from the LuxTrust website https://sra.luxtrust.lu and fill it out before going to an RA. This form is incorporated in the requestor's file or, in case no such file exists in that RA, integrated into a newly created file.
   - If the revocation requestor can be properly identified and the revocation request form is properly filled out and signed, the RA will revoke the Certificate.
   - if the revocation requestor cannot be properly identified or the revocation request form is not properly filled out or signed, the RA performs no change on the validity status of the Certificate.

d. For professional products, LuxTrust offers the option that one or more persons of a company or institution can order a PRO certificate with the subject.Title "Professional administrator". This does allow this person to revoke (or suspend) any professional certificate issued to the same company or institution. In order to have a third person's certificate revoked, the holder of a "Professional administrator" certificate has to send a digitally signed document (e-mail, MS-Word, ...) to LuxTrust, within which he indicates the references of the certificate to be revoked. LuxTrust checks:
   - if requestors signature is valid
   - if the requestor does have the "Professional administrator" status
     if the company or institution indicated in the requestors certificate does match the company or institution indicated in the certificate to be revoked.

   If all checks are positive, the revocation request is executed.

(Note that un-suspension and suspension cases are detailed respectively in section 4.9.16 and 4.9.15 of the present CP).

As stated in section 4.5.1 and in accordance with the LuxTrust CPS [6]:

- The Subscriber having subscribed for a physical LuxTrust (S)SCD shall ensure the destruction of his (S)SCD or alternatively give it back to a LuxTrust LRA for destruction once all Certificates on this (S)SCD are either revoked or expired.
- The LuxTrust Signing Server Account Subscriber accepts that his certified private key shall be destroyed once expired or revoked.

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

**The revocation of a Certificate is definitive.**

Note that for a revocation request, when the revocation requestor is requested to present himself to an LRA, (s)he can do so with any LRA approved by LuxTrust CSP, however,

- Unless the pseudonym Subscriber proceeds through online revocation, the revocation requestor has to go to the LRA where the Subscriber initially performed the registration. Indeed, only this LRA is able to make the link between a physical person identity and the certified pseudonym.
- In case the selected LRA is not part of the same LRA network as the initial LRA and/or this LRA network does not allow affiliated LRAs to access a digitalised version of the end-user registration file, the revocation requestor shall be required to perform a full validation of his request using a process that is similar to the initial enrolment (registration) process to provide all the required proofs.

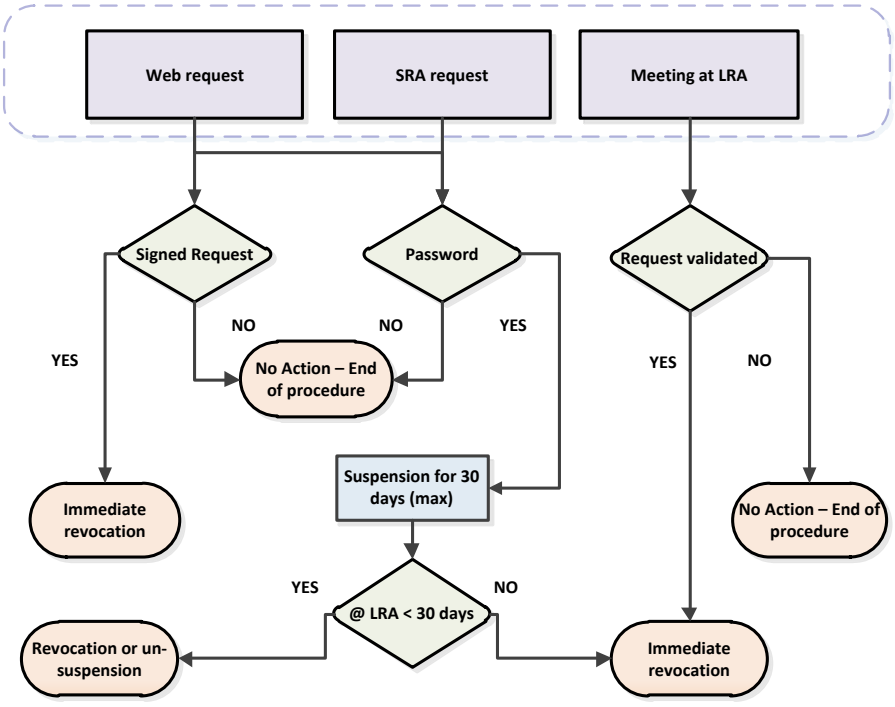


Figure 2 - Certificate revocation

The above picture summarises the process flow related to the revocation of a Certificate.

### 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 (updating the CRL) shall be as reduced as possible and does not exceed 24 hours.

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

To request the revocation of a Certificate, the revocation requestor must contact and present himself at an LRA for immediate revocation or use appropriately the SRA web-based interface or contact the SRA Hotline 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 LRA requests promptly, via the CRA towards 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.

While an LRA opening hours are limited, the SRA Hotline and web-based interface are available for at least prompt suspension (prior revocation) requests 24 hours a day, 7 days a week. The SRA Hotline requests promptly, via the CRA towards the CA, the suspension of the Certificate once the suspension request authenticated and validated. In case suspension is requested as a prior step towards revocation, the SRA informs promptly the CRA of this circumstance and the CRA contacts the Subscriber (via its LRAO in case of pseudonym Subscriber) to invite him to present himself at an LRA in order to proceed to the revocation of the suspended Certificate.

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 24 hours maximum as stated in section 4.9.4 of the present CP.

### 4.9.6 Revocation checking requirement for Relying Parties

Relying Parties must use online resources that the CA makes available through its repository to check the status of a Certificate before relying on it. 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 / OCSP response validity period

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://www.luxtrust.lu/faq/crl/crl. OCSP services are available from http://ocsp.luxtrust.lu. Web interface for Certificate status checking services is available from https://test.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

A CRL is issued each 4,5 hours (4 hours and 30 minutes), 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 (twelve) months available on its repository. Every CRL is stored, archived and available for retrieval for 10 (ten) years. Recovery of CRLs older than 12 (twelve) months may be subject to retrieval and administration fees as stated in section 9.1 of the present CP.

The fields “this update” and “next update” reflect the validity period of an OCSP response.

### 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

The LuxTrust Certificates covered by the present CP are generated in a suspended mode by the LuxTrust LTQCA (Factory). This suspension notification is immediately available in the related CRL and via the LuxTrust Validation Services.

In case of physical (S)SCD, unless the (S)SCD was sent directly to the Subscribers Shipping Data the Subscriber may be requested to present himself (herself) to the LRA to collect his/her (S)SCD and where his/her identity will be checked prior (S)SCD delivery and re-activation of Certificates.

If the (S)SCD is sent to the Subscriber by postal mail, or in case of LuxTrust Signing Server Account users (Virtual Smartcard), the activation and testing of the Certificates can be performed online through https://cmt.luxtrust.lu.

Initial suspension has a maximum duration of 60 (sixty) days. In case no un-suspension occurs within this period, the initially suspended Certificate(s) are revoked automatically. Un-suspension procedure is described in section 4.9.16 of the present CP.

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

### 4.9.14 Who can request suspension

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

### 4.9.15 Procedure for suspension request

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

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

Two types of suspensions are to be considered within LuxTrust:

- The initial suspension that is always performed by LuxTrust S.A. for the Certificates issued under the present CP, (certificates are kept suspended until hand-over of the card to the legitimate card owner).
- Requested suspension by an authorised party (see also section 4.9.14).

**Initial Suspension of LuxTrust Certificates issued under the present CP**

**The initial suspension** (related to the Certificates issuance) leads to a **60 (sixty) days** suspension period at a maximum. Two cases are then possible:

a. The Subscriber activates his Certificates before the end of the 60 (sixty) days period, and then the Certificates are un-suspended. This action is to be performed via the SRA Website.

b. If the Subscriber does not activate its Certificates before the end of the 60 (sixty) days period, the Certificates are automatically revoked.

**Suspension of Certificates from an existing LuxTrust Subscriber: process overview**

**A requested suspension** leads to a **30 (thirty) days period** suspension maximum.

The suspension requestor has two means to initiate the procedure:

a. **Contact the LuxTrust SRA Hotline**

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

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

b. **SRA Website based procedure**: The suspension requestor proceeds via the LuxTrust web-site (https://sra.luxtrust.lu):

- The suspension requestor electronically signs a suspension form-based request. If the signature is validated, then the suspension request is promptly sent to the CA for prompt processing and suspension of the certificate for a period of 30 (thirty) days and the SRA will inform the LuxTrust CRA of the event.
- The suspension requestor does not electronically sign his/her request, but provides a correct Challenge, then the certificate is promptly suspended by the SRA for a period of 30 (thirty) days maximum and the SRA will inform the LuxTrust CRA of the event.
- If the Challenge or the electronic signature is incorrect, the SRA performs no change on the validity status of the Certificate but raises an “alarm” towards the CRA.

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

- When no valid un-suspension is performed at an LRA within the 30 (thirty) days suspension period, the Certificate is automatically revoked.
- When an authorised requestor presents himself (herself) at an LRA before the end of the 30 (thirty) days suspension period:
  - (a) If the authorised requestor requests at an LRA the revocation of the Certificate, then the LRA, once the authorised requestor and his/her request are authenticated and validated, sends the revocation request to the CRA (using LRA software).
  - (b) If the authorised requestor requests at an LRA that (s)he wants to un-suspend the certificate, once the authorised requestor and his/her request are authenticated and validated, the LRA sends the un-suspension request to the CRA (using LRA software).

(c) If the claimed authorised requestor is not correctly authenticated at the LRA, the LRA performs no change on the validity status of the Certificate but raises an "alarm" towards the CRA.

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

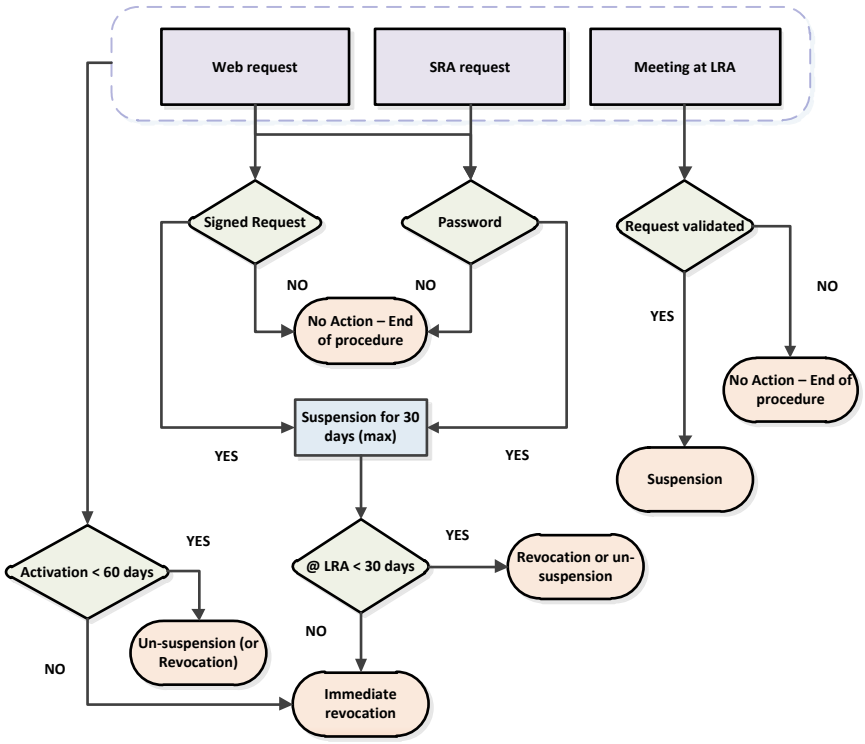


Figure 3 - Certificate suspension

### *4.9.16 Limits on suspension period*

The LuxTrust Certificates issued under the present CP are generated in a suspended mode by the LuxTrust CA (Factory). This initial suspension is set for a maximum period of 60 (sixty) days ; afterwards if not correctly un-suspended the Certificates are revoked.

In case of physical (S)SCD, unless the (S)SCD was sent directly to the Subscribers Shipping Data the Subscriber may be requested to present himself (herself) to the LRA to collect his/her (S)SCD and where his/her identity will be checked prior (S)SCD delivery and re-activation of Certificates. If the (S)SCD is sent to the Subscriber by postal mail, or in case of LuxTrust Signing Server Account users (Virtual Smartcard), the activation and testing of the Certificates can be performed online through https://cmt.luxtrust.lu.

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

Un-suspension procedure can occur during face-to-face delivery of Subscriber's LuxTrust Certificate during initial enrolment process or in a more general way as it is described hereafter.

**Un-suspension of a suspended existing Subscriber Certificate: process overview**

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

## 4.10 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 and key recovery are not allowed except for the sole purpose of and in the context of LuxTrust Signing Server Account disaster recovery as stated and ruled by the LuxTrust CPS [6].

**Subscriber's key escrow is never 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

This section is used to specify the Certificate format, CRL and OCSP format. This includes information on profiles, versions, and extensions used.

## 7.1 Certificate profile

Five types of LuxTrust Certificates can be issued under the present CP. They are respectively issued to three types of end-user devices according to the following:

- **LuxTrust SSCD Smartcards**: These physical user devices contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP+ [20] Qualified Certificate for Natural Persons for the purpose of creating qualified electronic signatures, under the Certificate Policy oid ***1.3.171.1.1.2.4.1***, and
  - One LuxTrust NCP+ [21] certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy oid ***1.3.171.1.1.2.4.2***.

- **LuxTrust non SSCD Signing Sticks**: These physical user devices that are not considered as SSCD according to [1] (e.g., SIM type chips unless they can be certified as SSCD) contain two certificates, associated to two different key pairs, according to two certificate policies
  - One LuxTrust QCP [22] Qualified Certificate for Natural Persons for the purpose of creating advanced electronic signatures supported by a qualified certificate, under the Certificate Policy oid ***1.3.171.1.1.2.4.3***, and
  - One LuxTrust NCP [23] certificate for Natural Persons for the purpose of data/entity authentication and encryption facilities, under the Certificate Policy oid ***1.3.171.1.1.2.4.4***.

- **LuxTrust Signing Server Accounts (Virtual Smartcards)**: These centralised virtual user signature creation devices contain one certificate, associated to one key pair, according to one specific certificate policy
  - One LuxTrust NCP [24] certificate for Natural Persons for the combined purposes of electronic signature, data/entity authentication and encryption facilities, under the Certificate Policy oid ***1.3.171.1.1.2.4.5***.

### *7.1.1 Version number(s)*

X.509 v3 is supported and used.

#### 7.1.1.1 LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures

LuxTrust SSCD QCP+ Certificates supporting Qualified Signatures are Qualified Certificates issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 1024-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD QCP+ Certificates are compliant with and include the oid reference of the QCP+ certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.1) [2].

The usage purpose of these LuxTrust SSCD QCP+ Certificates is limited to sole authorised usage of supporting the creation of qualified electronic signatures. The LuxTrust SSCD QCP+ Certificates include the corresponding LuxTrust QCP+ oid, i.e., < **OID 1.3.171.1.1.2.4.1**>.

[20] As defined by ETSI TS 101 456 [2].
[21] As defined in ETSI TS 102 042 [4].
[22] As defined by ETSI TS 101 456 [2].
[23] As defined in ETSI TS 102 042 [4].
[24] As defined in ETSI TS 102 042 [4].

The following table provides the description of the fields for LuxTrust SSCD QCP+ Certificates.

| LuxTrust SSCD QCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[25] | CE[26] | O/M[27] | CO[28] | 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 |
| | organizationName | ✓ | | | S | LuxTrust S.A. |
| Validity | | ✓ | False | | | |
| | NotBefore | ✓ | | | D | Certificate generation process date/time. |
| | NotAfter | ✓ | | | D | Certificate generation process date/time + 36 Months |
| Subject | | ✓ | False | | | |
| | serialNumber | ✓ | | M | D | *Serial Number as constructed by LRAO* |
| | commonName | ✓ | | M | D | ***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*<br>***PSEUDONYM products:***<br>*Concatenation: "PSEUDONYM: " & subject.pseudonym* |
| | givenName | ✓ | | M | D | ***PRO and PRIVATE products**: Given name(s) as on ID card*<br>*(not present in case of pseudonym)* |
| | surname | ✓ | | M | D | ***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*<br>*(not present in case of pseudonym)* |

[25] IN = Included: Attribute / field included within the certificate profile.

[26] CE = Critical Extension.

[27] O/M: O = Optional, M = Mandatory.

[28] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

| LuxTrust SSCD QCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[25] | CE[26] | O/M[27] | CO[28] | Value |
| | pseudonym | ✓ | | M | D | ***PSEUDONYM products only:*** *Pseudonym as provided by the holder* |
| | countryName | ✓ | | M | D | *Nationality of holder (ISO3166)* |
| | emailAddress | ✓ | | O | D | *Subject's email address* |
| | title | ✓ | | M | D | ***PRIVATE products:*** *Fixed value:* ***"Private Person"*** ***PRO products:*** ***"Professional Person"*** *(default) or* ***"Professional Administrator"*** *(Other titles possible for special purpose certificates)* ***PSEUDONYM products****:* *Fixed value:* ***"Private Person"*** |
| | organizationName | ✓ | | M | D | ***PRO products only****:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.* |
| | localityName | ✓ | | M | D | ***PRO products only****: Company/institution country of HQ (as in articles of association)* |
| | organizationalUnitName 1 | ✓ | | M for PRO prod., condi-tional (O) for PRIV prod.) | D | ***PRO products****:* *Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)* ***PRIVATE products:*** *If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).* |
| | organizationalUnitName 2 | ✓ | | O | D | ***PRO products only****:* *Company/institution department or other information item* |
| subjectPublicKeyInfo | | ✓ | False | | | |
| | Algorithm | ✓ | | | | Public Key: Key length: 1024bit (RSA); 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 SSCD QCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[25] | CE[26] | O/M[27] | CO[28] | Value |
| | AccessMethod | ✓ | | | | Id-ad-2 |
| | accessLocation | ✓ | | | | http://ca.luxtrust.lu/LTQCA.crt |
| | AccessMethod | ✓ | | | | Id-ad-1 |
| | accessLocation | ✓ | | | | http://ocsp.luxtrust.lu |
| cRLDistributionPoint | | ✓ | False | | | |
| | distributionPoint | ✓ | | | S | |
| | fullName | ✓ | | | | "http://crl.luxtrust.lu/LTQCA.crl" |
| Subject Properties | | | | | | |
| subjectAltName | | ✓ | False | | | |
| | Rfc822Name | ✓ | | O | D | *Certificate Holder'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 | False |
| | nonRepudiation | ✓ | | | S | True |
| | keyEncipherment | ✓ | | | S | False |
| | dataEncipherment | ✓ | | | S | False |
| certificatePolicies | | ✓ | False | | | |
| | PolicyIdentifier | ✓ | | | | 1.3.171.1.1.2.4.1 |
| | policyQualifierID | ✓ | | | S | Id-qt-1 (CPS) |
| | qualifier | ✓ | | | S | http://repository.luxtrust.lu |
| | policyQualifierID | ✓ | | | S | Id-qt-2 (User Notice) |
| | noticeNumbers | | | | | |
| | DisplayText | ✓ | | | | LuxTrust Qualified Certificate on SSCD compliant with ETSI TS 101 456 QCP+ certificate policy. Key Generation by CSP. **Sole Authorised Usage**: Support of Qualified Electronic Signature. |
| | PolicyIdentifier | ✓ | | | | 0.4.0.1456.1.1 |
| QualifiedCertificateStat | | | | | | |
| | QcCompliance | ✓ | | M | S | *0.4.0.1862.1.1* |
| | QcLimitValue | ✓ | | O | D | As provided by LuxTrust S.A. in compliance with [5] |
| | QcRetentionPeriod | ✓ | | O | D | As provided by LuxTrust S.A. in compliance with [5] |
| | QcSSCD | ✓ | | M | D | Set |

**+ Nestcape proprietary extension: NetscapeCertificateType: smime**

#### 7.1.1.2 LuxTrust SSCD NCP+ Certificates supporting Authentication & Encryption

LuxTrust SSCD NCP+ Certificates are Normalised Certificates issued on SSCD Hardware token such as LuxTrust Smartcard with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 1024-bit key size and 3 years validity from issuing start date.

These LuxTrust SSCD NCP+ Certificates are compliant with and include the oid reference of the NCP+ certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.2) [3].

The usage purpose of these LuxTrust SSCD NCP+ Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust SSCD NCP+ oid, i.e., **<1.3.171.1.1.2.4.2>**. Further information on Certificate authorised and prohibited usage is provided in section 1.4 of the present CP.

The following table provides the description of the fields for the LuxTrust SSCD NCP+ Certificate type supporting Authentication and Encryption.

| LuxTrust SSCD NCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| **Attribute** | **Field** | **IN[29]** | **CE[30]** | **O/M[31]** | **CO[32]** | **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 |
| | **organizationName** | ✓ | | | S | LuxTrust S.A. |
| **Validity** | | ✓ | False | | | |
| | **NotBefore** | ✓ | | | D | Certificate generation process date/time. |
| | **NotAfter** | ✓ | | | D | Certificate generation process date/time + 36 Months |
| **subject** | | ✓ | False | | | |
| | **serialNumber** | ✓ | | M | D | *Serial Number as constructed by LRAO* |

[29] IN = Included: Attribute / field included within the certificate profile.

[30] CE = Critical Extension.

[31] O/M: O = Optional, M = Mandatory.

[32] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

| LuxTrust SSCD NCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[29] | CE[30] | O/M[31] | CO[32] | Value |
| | commonName | ✓ | | M | D | ***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*<br>***PSEUDONYM products:***<br>*Concatenation: "PSEUDONYM: " & subject.pseudonym* |
| | givenName | ✓ | | M | D | ***PRO and PRIVATE products**: Given name(s) as on ID card*<br>*(not present in case of pseudonym)* |
| | surname | ✓ | | M | D | ***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*<br>*(not present in case of pseudonym)* |
| | pseudonym | ✓ | | M | D | ***PSEUDONYM products only:***<br>*Pseudonym as provided by the holder* |
| | countryName | ✓ | | M | D | *Nationality of holder (ISO3166)* |
| | emailAddress | ✓ | | O | D | *Subject's email address* |
| | title | ✓ | | M | D | ***PRIVATE products:***<br>*Fixed value: **"Private Person"***<br>***PRO products:***<br>***"Professional Person"** (default) or **"Professional Administrator"***<br>*(Other titles possible for special purpose certificates)*<br>***PSEUDONYM products**:*<br>*Fixed value: **"Private Person"*** |
| | organizationName | ✓ | | M | D | ***PRO products only**:*<br>*Name of company/institution as in articles of association or equivalent documents, including the legal form.* |
| | localityName | ✓ | | M | D | ***PRO products only**: Company/institution country of HQ (as in articles of association)* |

| LuxTrust SSCD NCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| **Attribute** | **Field** | **IN[29]** | **CE[30]** | **O/M[31]** | **CO[32]** | **Value** |
| | **organizationalUnitName 1** | ✓ | | M for PRO prod., condi-tional (O) for PRIV prod.) | D | ***PRO products**:* *Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)* ***PRIVATE products:*** *If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).* |
| | **organizationalUnitName 2** | ✓ | | O | D | ***PRO products only**:* *Company/institution department or other information item* |
| **subjectPublicKeyInfo** | | ✓ | False | | | |
| | **algorithm** | ✓ | | | | Public Key: Key length: 1024 bit (RSA); 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 | | | |
| | **AccessMethod** | ✓ | | | | Id-ad-2 |
| | **accessLocation** | ✓ | | | | http://ca.luxtrust.lu/LTQCA.crt |
| | **AccessMethod** | ✓ | | | | Id-ad-1 |
| | **accessLocation** | ✓ | | | | http://ocsp.luxtrust.lu |
| **cRLDistributionPoint** | | ✓ | False | | | |
| | **distributionPoint** | ✓ | | | S | |
| | **fullName** | ✓ | | | | http://crl.luxtrust.lu/LTQCA.crl |
| **Subject Properties** | | | | | | |
| **subjectAltName** | | ✓ | False | | | |
| | Rfc822Name | ✓ | | O | D | *Certificate Holder'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 |

| LuxTrust SSCD NCP+ Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[29] | CE[30] | O/M[31] | CO[32] | Value |
| | keyEncipherment | ✓ | | | S | True |
| | dataEncipherment | ✓ | | | S | True |
| certificatePolicies | | ✓ | False | | | |
| | PolicyIdentifier | ✓ | | | | 1.3.171.1.1.2.4.2 |
| | policyQualifierID | ✓ | | | S | Id-qt-1 (CPS) |
| | qualifier | ✓ | | | S | http://repository.luxtrust.lu |
| | policyQualifierID | ✓ | | | S | Id-qt-2 (User Notice) |
| | noticeNumbers | | | | | |
| | DisplayText | ✓ | | | | LuxTrust Certificate on SSCD compliant with ETSI TS 102 042 NCP+ certificate policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity Authentication and Data Encryption. |
| | PolicyIdentifier | ✓ | | | | 0.4.0.2042.1.2 |

**+ Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime**

#### 7.1.1.3 LuxTrust non SSCD QCP Certificates supporting Advanced Electronic Signatures

LuxTrust non SSCD QCP Certificates are Qualified Certificates **not** issued on SSCD, with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with either a 1024-bit key size or a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust non SSCD QCP Certificates are compliant with and include the oid reference of the QCP certificate policy of the ETSI Technical Specifications 101 456 (i.e., 0.4.0.1456.1.2) [2].

The usage purpose of these Certificates is limited to sole authorised usage of supporting the creation of non-qualified (advanced) electronic signatures supported by a qualified certificate. These Certificates include the corresponding LuxTrust QCP oid, i.e., **< OID 1.3.171.1.1.2.4.3>**.

The following table provides the description of the fields for LuxTrust non SSCD QCP Certificates.

| LuxTrust non SSCD QCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[33] | CE[34] | O/M[35] | CO[36] | Value |
| Base Profile | | | | | | |
| Version | | ✓ | False | | | |
| | | | | | S | Version 3 Value = “2” |
| SerialNumber | | ✓ | False | | | |
| | | | | | FDV | Validated on duplicates. |

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

| LuxTrust non SSCD QCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[33] | CE[34] | O/M[35] | CO[36] | Value |
| 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 |
| | organizationName | ✓ | | | S | LuxTrust S.A. |
| Validity | | ✓ | False | | | |
| | NotBefore | ✓ | | | D | Certificate generation process date/time. |
| | NotAfter | ✓ | | | D | Certificate generation process date/time + **36** Months |
| Subject | | ✓ | False | | | |
| | serialNumber | ✓ | | M | D | *Serial Number as constructed by LRAO* |
| | commonName | ✓ | | M | D | ***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*<br>***PSEUDONYM products:***<br>*Concatenation: "PSEUDONYM: " & subject.pseudonym* |
| | givenName | ✓ | | M | D | ***PRO and PRIVATE products**: Given name(s) as on ID card*<br>*(not used in case of pseudonym)* |
| | surname | ✓ | | M | D | ***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*<br>*(not used in case of pseudonym)* |
| | pseudonym | ✓ | | M | D | ***PSEUDONYM products only:***<br>*Pseudonym as provided by the holder* |
| | countryName | ✓ | | M | D | *Nationality of holder (ISO3166)* |
| | emailAddress | ✓ | | O | D | *Subject's email address* |

| LuxTrust non SSCD QCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[33] | CE[34] | O/M[35] | CO[36] | Value |
| | Title | ✓ | | M | D | ***PRIVATE products:*** *Fixed value:* ***"Private Person"*** ***PRO products:*** ***"Professional Person"*** *(default) or* ***"Professional Administrator"*** *(Other titles possible for special purpose certificates)* ***PSEUDONYM products****:* *Fixed value:* ***"Private Person"*** |
| | organizationName | ✓ | | M | D | ***PRO products only****:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.* |
| | localityName | ✓ | | M | D | ***PRO products only****: Company/institution country of HQ (as in articles of association)* |
| | organizationalUnitName 1 | ✓ | | M for PRO prod., condi-tional (O) for PRIV prod.) | D | ***PRO products****:* *Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)* ***PRIVATE products:*** *If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).* |
| | organizationalUnitName 2 | ✓ | | O | D | ***PRO products only****:* *Company/institution department or other information item* |
| subjectPublicKeyInfo | | ✓ | False | | | |
| | Algorithm | ✓ | | | | Public Key: Key length: 1024 or up to 2048 bit (RSA); 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 | | | |
| | AccessMethod | ✓ | | | | Id-ad-2 |
| | accessLocation | ✓ | | | | http://ca.luxtrust.lu/LTQCA.crt |

| LuxTrust non SSCD QCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[33] | CE[34] | O/M[35] | CO[36] | Value |
| | AccessMethod | ✓ | | | | Id-ad-1 |
| | accessLocation | ✓ | | | | http://ocsp.luxtrust.lu |
| cRLDistributionPoint | | ✓ | False | | | |
| | distributionPoint | ✓ | | | S | |
| | fullName | ✓ | | | | http://crl.luxtrust.lu/LTQCA.crl |
| Subject Properties | | | | | | |
| subjectAltName | | ✓ | False | | | |
| | Rfc822Name | ✓ | | O | D | *Certificate Holder'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 | False |
| | nonRepudiation | ✓ | | | S | True |
| | keyEncipherment | ✓ | | | S | False |
| | dataEncipherment | ✓ | | | S | False |
| certificatePolicies | | ✓ | False | | | |
| | PolicyIdentifier | ✓ | | | | 1.3.171.1.1.2.4.3 |
| | policyQualifierID | ✓ | | | S | Id-qt-1 (CPS) |
| | qualifier | ✓ | | | S | http://repository.luxtrust.lu |
| | policyQualifierID | ✓ | | | S | Id-qt-2 (User Notice) |
| | noticeNumbers | | | | | |
| | DisplayText | ✓ | | | | LuxTrust Qualified Certificate **not** on SSCD compliant with ETSI TS 101 456 QCP certificate policy. Key Generation by CSP.<br>Sole Authorised Usage: Advanced Electronic Signature supported by a Qualified cert |
| | PolicyIdentifier | ✓ | | | | 0.4.0.1456.1.2 |
| QualifiedCertificateStat | | | | | | |

| LuxTrust non SSCD QCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[33] | CE[34] | O/M[35] | CO[36] | Value |
| | QcCompliance | ✓ | | M | S | *0.4.0.1862.1.1* |
| | QcLimitValue | ✓ | | O | D | As provided by LuxTrust S.A. in compliance with [5] |
| | QcRetentionPeriod | ✓ | | O | D | As provided by LuxTrust S.A. in compliance with [5] |
| | QcSSCD | ✓ | | | | **NOT SET** |

**+ Nestcape proprietary extension: NetscapeCertificateType: smime**

#### 7.1.1.4 LuxTrust non SSCD NCP Certificates supporting Authentication & Encryption

LuxTrust non SSCD NCP Certificates are Normalised Certificates **not** issued on SSCD Hardware token with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with either a 1024-bit key or a 2048-bit key size and 3 years validity from issuing start date.

These LuxTrust non SSCD NCP Certificates are compliant with and include the oid reference of the NCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.1) [3].

The usage purpose of these NCP Certificates is for the combined purpose of authentication and encryption. These Certificates include the corresponding LuxTrust non SSCD NCP oid, i.e., **<1.3.171.1.1.2.4.4>**. Further information on Certificate authorised and prohibited usage is to be provided in section 1.4 of the applicable CP.

The following table provides the description of the fields for the LuxTrust non SSCD NCP Authentication and Encryption Certificate type.

| LuxTrust non SSCD NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[37] | CE[38] | O/M[39] | CO[40] | 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 |

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

| LuxTrust non SSCD NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[37] | CE[38] | O/M[39] | CO[40] | Value |
| | organizationName | ✓ | | | S | LuxTrust S.A. |
| Validity | | ✓ | False | | | |
| | NotBefore | ✓ | | | D | Certificate generation process date/time. |
| | NotAfter | ✓ | | | D | Certificate generation process date/time + 36 Months |
| subject | | ✓ | False | | | |
| | serialNumber | ✓ | | M | D | *Serial Number as constructed by LRAO* |
| | commonName | ✓ | | M | D | ***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*<br>***PSEUDONYM products:***<br>*Concatenation: "PSEUDONYM: " & subject.pseudonym* |
| | givenName | ✓ | | M | D | ***PRO and PRIVATE products**: Given name(s) as on ID card*<br>*(not used in case of pseudonym)* |
| | surname | ✓ | | M | D | ***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*<br>*(not used in case of pseudonym)* |
| | pseudonym | ✓ | | M | D | ***PSEUDONYM products only:***<br>*Pseudonym as provided by the holder* |
| | countryName | ✓ | | M | D | *Nationality of holder (ISO3166)* |
| | emailAddress | ✓ | | O | D | *Subject's email address* |
| | title | ✓ | | M | D | ***PRIVATE products:***<br>*Fixed value: **"Private Person"***<br>***PRO products:***<br>***"Professional Person"** (default) or **"Professional Administrator"***<br>*(Other titles possible for special purpose certificates)*<br>***PSEUDONYM products**:*<br>*Fixed value: **"Private Person"*** |

| LuxTrust non SSCD NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| **Attribute** | **Field** | **IN[37]** | **CE[38]** | **O/M[39]** | **CO[40]** | **Value** |
| | **organizationName** | ✓ | | M | D | ***PRO products only**:* *Name of company/institution as in articles of association or equivalent documents, including the legal form.* |
| | **localityName** | ✓ | | M | D | ***PRO products only**:* *Company/institution country of HQ (as in articles of association)* |
| | **organizationalUnitName 1** | ✓ | | M for PRO prod., conditional (O) for PRIV prod.) | D | ***PRO products**:* *Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)* ***PRIVATE products:*** *If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).* |
| | **organizationalUnitName 2** | ✓ | | O | D | ***PRO products only**:* *Company/institution department or other information item* |
| **subjectPublicKeyInfo** | | ✓ | False | | | |
| | **algorithm** | ✓ | | | | Public Key: Key length: 1024 or up to2048 bit (RSA); 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 | | | |
| | **AccessMethod** | ✓ | | | | Id-ad-2 |
| | **accessLocation** | ✓ | | | | http://ca.luxtrust.lu/LTQCA.crt |
| | **AccessMethod** | ✓ | | | | Id-ad-1 |
| | **accessLocation** | ✓ | | | | http://ocsp.luxtrust.lu |
| **cRLDistributionPoint** | | ✓ | False | | | |
| | **distributionPoint** | ✓ | | | S | |
| | **fullName** | ✓ | | | | http://crl.luxtrust.lu/LTQCA.crl |
| **Subject Properties** | | | | | | |
| **subjectAltName** | | ✓ | False | | | |
| | Rfc822Name | ✓ | | O | D | *Certificate Holder's email address* |
| **subjectKeyIdentifier** | | ✓ | False | | | |

| LuxTrust non SSCD NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[37] | CE[38] | O/M[39] | CO[40] | Value |
| | 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 | ✓ | | | | 1.3.171.1.1.2.4.4 |
| | policyQualifierID | ✓ | | | S | Id-qt-1 (CPS) |
| | qualifier | ✓ | | | S | http://repository.luxtrust.lu |
| | policyQualifierID | ✓ | | | S | Id-qt-2 (User Notice) |
| | noticeNumbers | | | | | |
| | DisplayText | ✓ | | | | LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Data or Entity Authentication and Data Encryption. |
| | PolicyIdentifier | ✓ | | | | 0.4.0.2042.1.1 |

**+ Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime**

#### 7.1.1.5 LuxTrust Signing Server Account NCP Certificates supporting Signature, Authentication & Encryption

LuxTrust Signing Server Account NCP Certificates are Normalised Certificates **not** issued on SSCD Hardware token with creation of the keys by LuxTrust CSP according to the enrolment and issuing process and procedures described in the applicable CP, with a 1024-bit key size and 3 years validity from issuing start date.

These LuxTrust Signing Server Account NCP Certificates are compliant with and include the oid reference of the NCP certificate policy of the ETSI Technical Specifications 102 042 (i.e., 0.4.0.2042.1.1) [3].

The usage purpose of these Certificates is for the combined purpose of electronic signature, authentication and encryption. These Certificates include the corresponding LuxTrust Signing Server Account NCP oid, i.e., **<1.3.171.1.1.2.4.5>**. Further information on Certificate authorised and prohibited usage is to be provided in section 1.4 of the applicable CP.

When the credentials are sent by SMS the corresponding certificate is issued valid and the end-user has not to activate his certificate, otherwise it is issued in suspended mode.

The following table provides the description of the fields for the LuxTrust Signing Server Account NCP Signature, Authentication and Encryption Certificate type.

| LuxTrust Signing Server NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| **Attribute** | **Field** | **IN**[41] | **CE**[42] | **O/M**[43] | **CO**[44] | **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 |
| | **organizationName** | ✓ | | | S | LuxTrust S.A. |
| **Validity** | | ✓ | False | | | |
| | **NotBefore** | ✓ | | | D | Certificate generation process date/time. |
| | **NotAfter** | ✓ | | | D | Certificate generation process date/time + **36** Months |
| **subject** | | ✓ | False | | | |
| | **serialNumber** | ✓ | | M | D | *Serial Number as constructed by LRAO* |
| | **commonName** | ✓ | | M | D | ***PRO and PRIVATE products**: Concatenation of given name(s) and surname(s) as on ID card separated by a "Space" character*<br>***PSEUDONYM products:***<br>*Concatenation: "PSEUDONYM: " & subject.pseudonym* |
| | **givenName** | ✓ | | M | D | ***PRO and PRIVATE products**: Given name(s) as on ID card*<br>*(not used in case of pseudonym)* |

41 IN = Included: Attribute / field included within the certificate profile.

42 CE = Critical Extension.

43 O/M: O = Optional, M = Mandatory.

44 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

| LuxTrust Signing Server NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[41] | CE[42] | O/M[43] | CO[44] | Value |
| | surname | ✓ | | M | D | ***PRO and PRIVATE products**: Surname(s) as on ID card without indication "épouse", "ép." or similar and the subsequent name(s)*<br>*(not used in case of pseudonym)* |
| | pseudonym | ✓ | | M | D | ***PSEUDONYM products only:***<br>*Pseudonym as provided by the holder* |
| | countryName | ✓ | | M | D | *Nationality of holder (ISO3166)* |
| | emailAddress | ✓ | | O | D | *Subject's email address* |
| | title | ✓ | | M | D | ***PRIVATE products:***<br>*Fixed value: **"Private Person"***<br>***PRO products:***<br>***"Professional Person"** (default) or **"Professional Administrator"***<br>*(Other titles possible for special purpose certificates)*<br>***PSEUDONYM products**:*<br>*Fixed value: **"Private Person"*** |
| | organizationName | ✓ | | M | D | ***PRO products only**:*<br>*Name of company/institution as in articles of association or equivalent documents, including the legal form.* |
| | localityName | ✓ | | M | D | ***PRO products only**:*<br>*Company/institution country of HQ (as in articles of association)* |
| | organizationalUnitName 1 | ✓ | | M for PRO prod., condi-tional (O) for PRIV prod.) | D | ***PRO products**:*<br>*Company/Institution VAT number (or if no VAT number available, other unique national company/institution identifier)*<br>***PRIVATE products:***<br>*If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).* |
| | organizationalUnitName 2 | ✓ | | O | D | ***PRO products only**:*<br>*Company/institution department or other information item* |
| subjectPublicKeyInfo | | ✓ | False | | | |
| | algorithm | ✓ | | | | Public Key: Key length: 1024 bit (RSA); public exponent: Fermat-4 (=010001). |
| | subjectPublicKey | ✓ | | M | | |
| Extensions | | | | | | |

| LuxTrust Signing Server NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[41] | CE[42] | O/M[43] | CO[44] | Value |
| Authority Properties | | | | | | |
| authorityKeyIdentifier | | ✓ | False | | | |
| | keyIdentifier | ✓ | | | | SHA-1 Hash of the LuxTrust **Qualified** CA public key |
| authorityInfoAccess | | ✓ | False | | | |
| | AccessMethod | ✓ | | | | Id-ad-2 |
| | accessLocation | ✓ | | | | http://ca.luxtrust.lu/LTQCA.crt |
| | AccessMethod | ✓ | | | | Id-ad-1 |
| | accessLocation | ✓ | | | | http://ocsp.luxtrust.lu |
| cRLDistributionPoint | | ✓ | False | | | |
| | distributionPoint | ✓ | | | S | |
| | fullName | ✓ | | | | http://crl.luxtrust.lu/LTQCA.crl |
| Subject Properties | | | | | | |
| subjectAltName | | ✓ | False | | | |
| | Rfc822Name | ✓ | | O | D | *Certificate Holder'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 | True |
| | keyEncipherment | ✓ | | | S | True |
| | dataEncipherment | ✓ | | | S | True |
| certificatePolicies | | ✓ | False | | | |
| | PolicyIdentifier | ✓ | | | | 1.3.171.1.1.2.4.5 |
| | policyQualifierID | ✓ | | | S | Id-qt-1 (CPS) |
| | qualifier | ✓ | | | S | http://repository.luxtrust.lu |
| | policyQualifierID | ✓ | | | S | Id-qt-2 (User Notice) |
| | noticeNumbers | | | | | |

| LuxTrust Signing Server NCP Certificate Profile | | | | | | |
|---|---|---|---|---|---|---|
| Attribute | Field | IN[41] | CE[42] | O/M[43] | CO[44] | Value |
| | DisplayText | ✓ | | | | LuxTrust Certificate not on SSCD compliant with ETSI TS 102 042 NCP certificate policy. Key Generation by CSP. Sole Authorised Usage: Signature, Data or Entity Authentication and Data Encryption. |
| | PolicyIdentifier | ✓ | | | | 0.4.0.2042.1.1 |

**+ Nestcape proprietary extension: NetscapeCertificateType: sslClient, smime**

### *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 [10] and RFC 3280 [11].

### *7.1.4 Name forms*

Name forms are in the X.500 distinguished name form as implemented in RFC 3739 [12].

### *7.1.5 Name constraints*

Name constraints are supported as per RFC 3280 [11].

### *7.1.6 Certificate policy object identifier*

Certificate policy object identifiers are used as per RFC 3739 [12].

### *7.1.7 Usage of Policy Constraints extension*

Usage of Policy Constraints extension is supported as per RFC 3280 [11].

### *7.1.8 Policy qualifiers syntax and semantics*

The use of policy qualifiers defined in RFC 3280 [11] 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 3280 [11], 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><br><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 [13]. 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 [6].

### *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 and Normalised Certificates, QCP(+) & NCP(+), 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,
- According respectively to the ETSI technical specifications TS 101 456 [2] and to the ETSI technical specifications TS 102 042 [4],
- 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 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, affiliated LRAs and LRAOs, shall accept for being selected for audit or controls, shall provide all required assistance and work to successfully comply and pass audit or controls.

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

- ETSI TS 101 456 on Policy requirements for certification authorities issuing qualified certificates [2] ;
- ETSI TS 102 042 on Policy requirements for certification authorities issuing public key certificates [4], and
- ETSI TS 102 023 on Policy requirements for time-stamping authorities.

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

Please refer to the LuxTrust CPS [6] for further details on compliance audit and other assessments requirements.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

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

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

LuxTrust S.A. acting as CSP, and via its LuxTrust CSP Board acting as Policy Approval Authority, may modify such fees, in view of operational or other costs of functioning of LuxTrust, at any time on its sole discretion. Such fee modifications shall be published on updated versions of the present CP and take effect 30 (thirty) days as from the day they are published.

## 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.

### *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 LRA(O)s. The received data from end-users can be used solely for the provision of certification services.

The LRA 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.

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

## 9.5 Intellectual property rights

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

## 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 101 456 [2] and ETSI TS 102 042 [4] 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 [6] 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 [6] 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.

LuxTrust S.A. acting as CSP through its LTQCA is liable for damage caused to any entity or legal or natural person who reasonably relies on that Certificate:

- As regards the accuracy at the time of issuance of all information contained in the Certificate and as regards to the fact that the Certificate contains all the details prescribed in section 7.1 of the present CP;
- For assurance that at the time of issuance of the Certificate, the signatory identified in the Certificate held the Private Key corresponding to the Public Key given or identified in the Certificate;
- For assurance that the Private Key and the Public Key can be used in a complementary manner.

LuxTrust S.A. is liable for damages caused to any entity or legal or natural person who reasonably relies on that Certificate for failure to register revocation of the Certificate unless LuxTrust S.A. can prove that it has not acted negligently.

In certain cases described in the LuxTrust CPS [6], LuxTrust S.A. acting as CSP may revoke or suspend the Certificate, provided it informs the Subscriber (and any other concerned authorised party, if applicable) of the Certificate in advance by appropriate means.

LuxTrust S.A. guarantees that each Key Pair created by LuxTrust S.A. acting as CSP for a Subscriber is generated in a secure way and that the private character of the Private Key of the Subscriber is guaranteed in accordance with the requirements set out in the technical specifications ETSI TS 101 456 [2].

LuxTrust S.A. guarantees that it will provide the SSCD in a secured way and in accordance with the requirements set out in the technical standard ETSI TS 101 456 [2]. The Key pair will be created via this device.

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). LuxTrust S.A. acting as CSP through its LTQCA shall undertake liability for all RA services provided on behalf of the LTQCA. RA liabilities are therefore primarily handled between LuxTrust S.A. and the RA. LuxTrust S.A. shall synchronise its contract with the RA to the present CP.

See LuxTrust CPS [6] for all additional rights, responsibilities and obligations of LuxTrust S.A. acting as CSP through its LTQCA.

### *9.6.2 RA representations and warranties*

The LRA is under a contractual obligation to comply scrupulously with the LuxTrust CPS [6], with the relevant section of the present CP (e.g., but not limited to sections 4.1.2), and with the LRA relevant LuxTrust internal procedures.

### *9.6.3 Subscriber representations and warranties*

The Subscriber accepts the Certification Practice Statement (CPS) currently in effect [6], 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 delivered LuxTrust SSCD, or non-SSCD or Signing Server Account, including the keys or Certificate(s), unless (s)he can prove that (s)he has taken all the necessary measures for a timely revocation of his/her Certificate(s) when required.

### 9.6.4 Relying Party representations and warranties

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

- Receive notice and adhere to the conditions of the present CP and of the LuxTrust CPS [6] 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*
  - ***suspended or revoked*** – by following the link to the Certificate Revocation List (CRL) and making sure that the certificate is not listed there, using the OCSP validation services or the web based interface allowing to check the status of a Certificate.
- ***Never rely on expired or revoked certificates.***
- See also relevant section 4.5.2 and 4.9.6 of the present CP.
- Without prejudice to the warranties provided in the present CP or in the LuxTrust CPS [6], the Relying Party is wholly accountable for verification of a Certificate before trusting it. LuxTrust S.A. acting as CSP accepts liability up to an aggregate limit for each Certificate of [*€ 25.000 Euros*] for direct losses, due to non-compliance with the LuxTrust CPS [6], towards a Relying Party reasonably relying on a Certificate.
- If a Relying Party relies on a Certificate without following the above rules, the LuxTrust CSP Board will not accept liability for any consequences.
- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt.
- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify LuxTrust S.A. acting as CSP.

### 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. 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. The limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages, incurred by any person, including without limitation a Subscriber, an applicant, a recipient, or a Relying Party, that are caused by reliance on or use of a Certificate LuxTrust S.A. issues, manages, uses, suspends or revokes, or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim.

d. By accepting a Certificate, the Subscriber agrees to indemnify and hold LuxTrust and its 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 agent(s) and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:
   - Falsehood or misrepresentation of fact by the Subscriber;
   - Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive LuxTrust or any person receiving or relying on the Certificate;
   - Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key.

## 9.8 Limitations of liability

The liability of LuxTrust S.A. acting as 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 communicated 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<br>LuxTrust S.A.<br>IVY Building<br>13-15, Parc d'Activités<br>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 [6]. 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 (fourteen) 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 (fourteen) 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

Prior to litigation, the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services associated with the present CP is ruled by the "LuxTrust Dispute Resolution Procedure" as publicly available from https://repository.luxtrust.lu, otherwise complaints 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 [6];
- 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 customised elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a Certificate.

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