LuxTrust Certificate Policy for Normalised Certificates issued to Natural Persons

Version number: v1.7

Publication Date: 12/*04*/*2007*

Document O.I.D: 1.3.171.1.1.2.1.0.*1(version).7(sub-version)*

Document Information

Document title:	LuxTrust Certificate Policy for Normalised Certificates issued to Natural Persons
Project Reference:	LuxTrust
Document Archival Code:	

Table of content

DOCUMENT INFORMATION 2
TABLE OF CONTENT 3
INTELLECTUAL PROPERTY RIGHTS 6
1. INTRODUCTION 7
1.1. OVERVIEW 7
1.1.1. The LuxTrust project 7
1.1.2. The LuxTrust certification services and PKI hierarchy 7
1.1.3. The present document - LuxTrust Certificate Policy for Normalised Certificates issued to Natural Persons 8
1.2. DOCUMENT NAME AND IDENTIFICATION 10
1.3. PKI PARTICIPANTS 11
1.3.1. Certification Authorities 12
1.3.2. Registration Authorities 13
1.3.2.1. Central Registration Authorities 13
1.3.2.2. Local Registration Authorities 14
1.3.3. Subscribers 15
1.3.4. Relying Parties 15
1.3.5. Other participants 15
1.3.5.1. CA Factory Services Provider 15
1.3.5.2. (Secure) Signature Creation Device Provider 15
1.3.5.3. Certificate Validation Services Provider 16
1.3.5.4. Suspension Revocation Authority 16
1.3.5.5. Root Signing Services 16
1.4. CERTIFICATE USAGE 17
1.4.1. Appropriate certificate uses 17
1.4.2. Prohibited certificate uses 18
1.5. POLICY ADMINISTRATION 19
1.5.1. Organisation administering the document 19
1.5.2. Contact person 19
1.5.3. Entity determining CPS suitability for the policy 19
1.5.4. CP Approval Procedure 19
1.6. DEFINITIONS AND ACRONYMS 20
1.7. RELATIONSHIP WITH THE EUROPEAN DIRECTIVE ON ELECTRONIC SIGNATURES 25
2. PUBLICATIONS AND REPOSITORY RESPONSIBILITIES 26
2.1. IDENTIFICATION OF ENTITIES OPERATING REPOSITORIES 26
2.2. PUBLICATION OF CERTIFICATION INFORMATION 26
2.3. TIME OF FREQUENCY OF PUBLICATION 27
2.3.1. Frequency of Publication of Certificates 27
2.3.2. Frequency of Publication of Revocation information 27
2.3.3. Frequency of Publication of Terms & Conditions 27
2.4. ACCESS CONTROL ON REPOSITORIES 27
3. IDENTIFICATION AND AUTHENTICATION 28
3.1. NAMING 28

3.1.1. Types of names 28
3.1.2. Need for names to be meaningful 28
3.1.3. Anonymity or pseudonymity of subscribers 29
3.1.4. Rules for interpreting various name forms 29
3.1.5. Uniqueness of names 29
3.1.6. Recognition, authentication, and role of trademarks 29
3.2. INITIAL IDENTITY VALIDATION 30
3.2.1. Method to prove possession of private key 30
3.2.2. Authentication of organization identity 30
3.2.3. Authentication of individual identity 31
3.2.4. Non-verified subscriber information 31
3.2.5. Validation of authority 31
3.2.6. Criteria for interoperation 32
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY & UPDATE REQUESTS 32
3.3.1. Identification and authentication for routine re-key & update 32
3.3.2. Identification and authentication for re-key after revocation 32
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 32

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 33

4.1. CERTIFICATE APPLICATION 33
4.1.1. Who can submit a certificate application 33
4.1.2. Enrolment process and responsibilities 33
4.1.2.1. Subscriber enrolment process 34
4.1.2.2. Other PKI Participants enrolment process 39
4.1.2.3. PKI Participants responsibilities related to enrolment process 39
4.2. CERTIFICATE APPLICATION PROCESSING 41
4.2.1. Performing identification and authentication functions 41
4.2.2. Approval or rejection of certificate applications 42
4.2.3. Time to process certificate applications 42
4.3. CERTIFICATE ISSUANCE 42
4.3.1. CA actions during certificate issuance 42
4.3.2. Notification to Subscriber by the CA of issuance of Certificate 42
4.4. CERTIFICATE ACCEPTANCE 42
4.4.1. Conduct constituting Certificate acceptance 42
4.4.2. Publication of the Certificate by the CA 43
4.4.3. Notification of Certificate issuance by the CA to other entities 43
4.5. KEY PAIR AND CERTIFICATE USAGE 43
4.5.1. Subscriber private key and certificate usage 43
4.5.2. Relying Party public key and Certificate usage 44
4.6. CERTIFICATE RENEWAL 45
4.7. CERTIFICATE RE-KEY 45
4.8. CERTIFICATE MODIFICATION 45
4.9. CERTIFICATE REVOCATION AND SUSPENSION 46
4.9.1. Circumstances for revocation 46
4.9.2. Who can request revocation 47
4.9.3. Procedure for revocation request 47
4.9.4. Revocation request grace period 50
4.9.5. Time within which CA must process the revocation request 50
4.9.6. Revocation checking requirement for Relying Parties 51
4.9.7. CRL issuance frequency 51
4.9.8. Maximum latency for CRLs 51
4.9.9. On-line revocation/status checking availability 51
4.9.10. On-line revocation checking requirements 52

4.9.11. Other forms of revocation advertisements available 52
4.9.12. Special requirements regarding key compromise 52
4.9.13. Circumstances for suspension 52
4.9.14. Who can request suspension 52
4.9.15. Procedure for suspension request 52
4.9.16. Limits on suspension period 55
4.10. CERTIFICATE STATUS SERVICES 56
4.10.1. Operational characteristics 56
4.10.2. Service availability 56
4.10.3. Optional features 56
4.11. END OF SUBSCRIPTION 56
4.12. KEY ESCROW AND RECOVERY 56

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 57

6. TECHNICAL SECURITY CONTROLS 57

7. CERTIFICATE AND CRL PROFILES 58

7.1. CERTIFICATE PROFILE 58
7.1.1 Version number(s) 58
7.1.1.1 LuxTrust NCP+ Certificates 58
7.1.1.2 LuxTrust NCP Certificates 62
7.1.2 Certificate extensions 64
7.1.3 Algorithm object identifiers 64
7.1.4 Name forms 64
7.1.5 Name constraints 65
7.1.6 Certificate policy object identifier 65
7.1.7 Usage of Policy Constraints extension 65
7.1.8 Policy qualifiers syntax and semantics 65
7.1.9 Processing semantics for the critical Certificate Policies 65
7.2. CRL PROFILE 65
7.2.1. Version number(s) 65
7.2.2. CRL entry extensions 66
7.3. OCSP PROFILE 66
7.3.1. Version number(s) 66
7.3.2. OCSP extensions 66

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 66

9. OTHER BUSINESS AND LEGAL MATTERS 67

9.1. FEES 67
9.2. FINANCIAL RESPONSIBILITY 67
9.2.1. Insurance coverage 67
9.2.2. Other assets 67
9.2.3. Insurance or warranty coverage for end-entities 67
9.3. CONFIDENTIALITY OF BUSINESS INFORMATION 68
9.4. PROTECTION OF PERSONAL INFORMATION 68
9.5. INTELLECTUAL PROPERTY RIGHTS 69

ALL TITLE, COPYRIGHTS, TRADEMARKS, SERVICE MARKS, PATENTS, PATENT APPLICATIONS AND ALL OTHER INTELLECTUAL PROPRIETARY RIGHTS NOW KNOWN OR HEREAFTER RECOGNISED IN ANY JURISDICTION (THE IP RIGHTS) IN AND TO LUXTRUST'S TECHNOLOGY, WEB SITES, DOCUMENTATION, PRODUCTS AND SERVICES (THE PROPRIETARY MATERIALS) ARE OWNED AND WILL CONTINUE TO BE EXCLUSIVELY OWNED BY LUXTRUST S.A. AND/OR ITS LICENSORS. LUXTRUST'S CONTRACTORS AND / OR SUBCONTRACTORS AGREE TO MAKE NO CLAIM OF INTEREST IN OR TO ANY SUCH IP RIGHTS. LUXTRUST'S CONTRACTORS AND / OR SUBCONTRACTORS ACKNOWLEDGE THAT NO TITLE TO THE IP RIGHTS IN AND TO THE PROPRIETARY MATERIALS IS TRANSFERRED TO THEM AND THAT THEY DO NOT OBTAIN ANY RIGHTS, EXPRESS OR IMPLIED, IN ANY PROPRIETARY MATERIALS OTHER THAN THE RIGHTS EXPRESSLY GRANTED IN THE CP. 69
9.6. REPRESENTATIONS AND WARRANTIES 69
9.6.1. CA representations and warranties 69
9.6.2. RA representations and warranties 70
9.6.3. Subscriber representations and warranties 70
9.6.4. Relying Party representations and warranties 71
9.6.5. Representations and warranties of other participants 71
9.7. DISCLAIMERS OF WARRANTIES 71
9.8. LIMITATIONS OF LIABILITY 72
9.9. INDEMNITIES 73
9.10. TERM AND TERMINATION 73
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 73
9.12. AMENDMENTS 74
9.12.1. Procedure for amendment 74
9.12.2. Notification mechanism and period 74
9.12.3. Circumstances under which OID must be changed 74
9.13. DISPUTE RESOLUTION PROVISIONS 74
9.14. GOVERNING LAW 74
9.15. COMPLIANCE WITH APPLICABLE LAW 75
9.16. MISCELLANEOUS PROVISIONS 75

Intellectual Property Rights

1. INTRODUCTION

1.1. Overview

1.1.1. *The LuxTrust project*

The LuxTrust project aims to establish a national center of expertise in the form of a Trusted Third Party, with an international reach. The goal of this LuxTrust TTP is to support and secure the existing business needs and promote the development of new “e-business” and “e-government” opportunities, re-using the existing legal and commercial assets, which are unique to Luxembourg.

To this purpose, LuxTrust s.a. has been created to become the provider of the LuxTrust certification services as defined in the Grand-Duchy of Luxembourg modified 14/08/2000 law on electronic commerce [8]. 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.

The LuxTrust PKI (Private Key Infrastructure) is established for the whole of the economic marketplace in Luxembourg, including the private sector as well as public authorities.

1.1.2. *The LuxTrust certification services and PKI hierarchy*

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

- One Internationally recognized root : "GTE Cybertrust Global Root" which 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 and is issuing 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 in the sense of the Grand-Duchy of Luxembourg modified 14/08/2000 law on electronic commerce [8], is using several Certification Authorities (CAs) according to the here described hierarchy to issue the LuxTrust certificates. These CAs include the LuxTrust Root CA, LuxTrust Normalised CA, LuxTrust Qualified CA services (as well as other future CA root-signed by the LuxTrust Root CA). In all CA-certificates of these CAs, LuxTrust s.a. is referred to as the legal entity being the certificate issuing authority and thereby having the final responsibility and liability for all the LuxTrust CAs as well as for all the component services that are used by LuxTrust s.a. to provide LuxTrust certifications services through any one of its CAs, as described in section 1.3. This is true even when LuxTrust s.a. acting as CSP through any one of its CAs is sub-contracting some of these component services 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 component services.

The LuxTrust PKI Hierarchy can be depicted as follows.

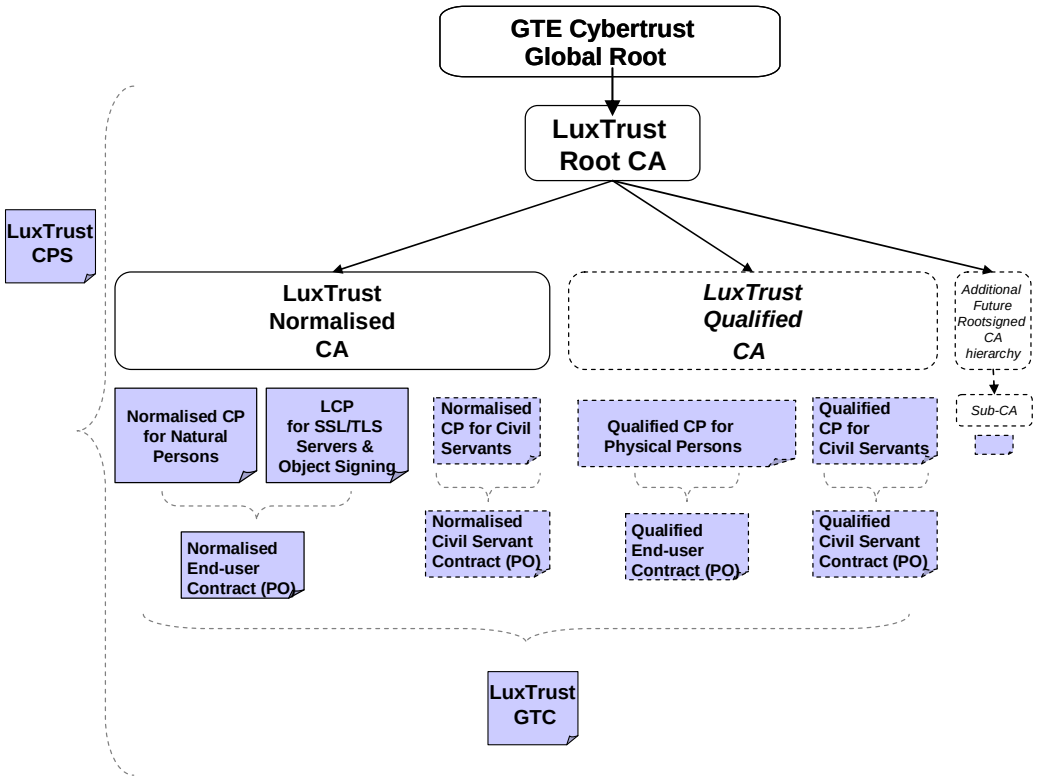


Figure 1 : LuxTrust PKI Hierarchy of CAs and related CPS/CPs and contractual documents

1.1.3. *The present document - LuxTrust Certificate Policy for Normalised Certificates issued to Natural Persons*

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

- the applicability of certificates in the form of *LuxTrust Normalised Certificates issued to Natural Person* (hereinafter referred to as the "Certificates") issued by LuxTrust s.a. as Certification Service Provider (CSP) through its LuxTrust Normalised CA (LTNCA), as well as,

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

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

The present CP is a set of rules, requirements and definitions determining the level of security reached by the LuxTrust Normalised 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 three Normalised Certificate Policies:

- **"LuxTrust NCP+ Signature"**: ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to electronic signature.
- **"LuxTrust NCP+ Authentication & Encryption"**: ETSI TS 102 042 NCP+ compliant Normalised Certificate on SSCD Hardware token (LuxTrust Smart Card), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and with a key usage limited to authentication purpose (to the exclusion of electronic signature)[1] and key & data encryption.
- **"LuxTrust NCP"**: ETSI TS 102 042 NCP compliant Normalised Certificate on a "LuxTrust Server Signing" token (non-SSCD), with creation of the keys by the CSP, 1024-bit key size, three (3) years validity, and a key usage combining digital signature (authentication and electronic signature purposes), key and data encryption.

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

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

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 attributes.

The Certificate provides the highest degree of assurance of proper Certificate Subject authentication since in order to obtain the Certificate and unless the subscriber has already been identified, according to the KYC rules set by the CSSF, the legal entity within which the LRA is set, 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 and, in case the professional quality should be certified, proof of his/her professional quality (e.g.,

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

representation power with regard to the legal person), together with any information required to support the certification process.

Such Certificate can be used for the following security services: encryption and / or authentication and / or Advanced Electronic Signature with the exclusion of Qualified Electronic Signature.

LuxTrust s.a. acting as CSP indicates and guarantees within the present CP that it complies, through the associated LuxTrust Normalised 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:

1.3.171.1.1.2.1.0.1(version).3(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 **LuxTrust Normalised Certificate Policy for Normalised Certificate issued to Natural Person**s. In addition to the specific LuxTrust requirements for Normalised Certificates stated in the present document, these Certificates meet the requirements for "NCP" or "NCP+" certificate policies, as specified by ETSI TS 102 042 and include accordingly the ETSI TS 102 042 certificate policy identifier.

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

- **"LuxTrust NCP+ Signature"**:
  - ETSI 102 042 oid: **0.4.0.2042.1.2**
  - **LuxTrust NCP+ Signature oid**: 1.3.171.1.1.2.1.1

- **"LuxTrust NCP+ Authentication & Encryption"**:
  - ETSI 102 042 oid: **0.4.0.2042.1.2**
  - **LuxTrust NCP+ Authentication & Encryption oid**: 1.3.171.1.1.2.1.2

- **"LuxTrust NCP"**:
  - OID ETSI 102 042: **0.4.0.2042.1.1**
  - **LuxTrust NCP oid**: 1.3.171.1.1.2.1.3

Although the use of the "Signing Server" requires fall-back to the use of the ETSI 102 042 "NCP" Policy (as a down-grade from the NCP+ level), LuxTrust s.a. specifically indicates with this LuxTrust specific policy oid that it only allows LuxTrust-accredited Signing Servers to hold such SCD-Tokens.

1.3. PKI participants

The LuxTrust PKI Participants are the legal entities or set of legal entities filling the role of participant within the LuxTrust PKI, that is either making use of, or providing LuxTrust PKI certification services[2] 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 Normalised 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].

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

1.3.1. *Certification 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 (voir contrat cybertrust Dan).

Within the LuxTrust PKI, the "LuxTrust Normalised CA" is used by LuxTrust s.a. acting as CSP to issue the LuxTrust Normalised Certificates as defined in section 1.1.3.

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

Note 1: In the following text, unless explicitly otherwise indicated, when referring to "the CA", it is expressly meant "the LuxTrust Normalised CA granted to issue LuxTrust Normalised Certificates by the LuxTrust Root CA under the ultimate responsibility of LuxTrust s.a. acting as CSP. The CA is thus legally designating LuxTrust s.a. acting as CSP.

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

The LTNCA, as well as all supporting component services, shall target accreditation against ETSI TS 102 042 [4] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. OLAS shall be the accreditation entity. For further details please refer to section 8 of the present CP.

The LTNCA, that is, LuxTrust s.a. acting as CSP, is established in Grand-Duchy of Luxembourg. LuxTrust s.a. can be contacted, with respect to the LTNCA, using the coordinates as provided in the section 1.5.1 of the present CP. The technical management and operations of the LTNCA (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 and within a secure facility compliant with the LuxTrust CPS and providing a disaster recovery facility in the Grand-Duchy of Luxembourg.

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

1.3.2. *Registration Authorities*

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

- The Central Registration Authority (CRA): It aims to mutualise the RA facilities for several LRAs and provide a central operational communication point between the LRAs and the rest of the LuxTrust PKI (e.g., Certificate factory, LuxTrust token 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[3] of the LuxTrust Certificate Subscribers and to validate the certificate unsuspension and revocation requests from the certified users when the physical presence of the user is requested.

All communications between LRAs, CRA, SRA, the LTNCA, 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.

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 token 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.

[3] 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).

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[4] processing of certificate suspension (validity status of the certificate will be updated accordingly in the entries of the Validation Services / Certificate Suspension/Revocation Status Services) through a 24/7 Hotline. Contact details of this SRA Hotline are available at http://sra.luxtrust.lu.
- By setting-up a LuxTrust Hotline and support website for help desk services, those are available at http://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 Signing Server accounts

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

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

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 unsuspension and revocation requests from the certified Subscribers when their physical presence is requested.

Within the LTNCA 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 LTNCA 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 (unsuspension) 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 a LuxTrust Normalised Certificate.

[4] 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.

The provision of Local Registration Services under the present CP, in compliance with the LuxTrust CPS and under a signed contractual agreement with LuxTrust s.a. acting as CSP, is ensured by:

- *< … insert company identification >*
- *< … insert company identification >*
- *< … insert company identification >*
- *…*

1.3.3. *Subscribers*

The Subscribers of the LuxTrust Normalised Certificates related certification services in the LuxTrust Normalised CA (LTNCA) 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).

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 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 Signature Creation Device (SCD) Services, namely the LuxTrust Signing Server provisioning facilities, under the present CP, in compliance with the LuxTrust CPS and under a signed contractual agreement with LuxTrust s.a. acting as CSP, is ensured:

- by 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 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 Company u-trust consortium is constituted by legal persons (Clearstream Services, Cetrel S.C., Ebrc and Hitec S.A.) that are different and independent from each other.

The provision of Secure Signature Creation Device (SSCD) Services, namely the LuxTrust Smart Card provisioning facilities, under the present CP, in compliance with the 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 (normalised) advanced electronic signature, encryption and authentication.

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.

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 NCP+ Signature" Certificate on LuxTrust Smart Card**: It is an ETSI TS 102 042 NCP+ compliant Normalised Certificate whose key usage limited to electronic signature. The keyUsage is exclusively set to nonRepudiation to the exclusion of any other usage. 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[5].

- **"LuxTrust NCP+ Authentication & Encryption" Certificate on LuxTrust Smart Card**: It is an ETSI TS 102 042 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) 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.

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

> ***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 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 NCP" Certificate (LuxTrust Signing Server Account)**: It is an ETSI TS 102 042 NCP compliant Normalised Certificate with a key usage combining authentication, electronic signature, key encryption and 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, and that Relying Parties **shall accept** such a Certificate to support valid Electronic Signatures. Electronic signatures supported by such a Certificate are Advanced Electronic signatures as long as they can be linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.

Normalised Certificates issued under this CP comply with ETSI TS 102 042, according to the NCP+ or NCP requirements respectively.

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 signature as supported by a LuxTrust NCP+ "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 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.

1.5. Policy administration

1.5.1. *Organisation administering the document*

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

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

Contact Person:	Daniel Neuhengen
Postal Address:	LuxTrust CSP Board, LuxTrust S.A., Boîte Postale 43. L-2010 Luxembourg
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

Definitions:

Advanced Electronic Signature [1]: means an Electronic Signature that meets the following requirements:

- It is uniquely linked to the signatory;
- It is capable of identifying the signatory;
- It is created using means that the signatory can maintain under his sole control; and
- It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Certification Authority (CA) [4]: An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users' keys.

Certificate [1]: An electronic attestation which links signature-verification data to a person and confirms the identity of that person.

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) [3]: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

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 [5]: A 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.

Certification Practice Statement [3]: Statement of the practices which a certification service provider employs in issuing, managing, revoking, and renewing or re-keying certificates.

Commitment Type: a signer-selected indication of the exact intent of an electronic signature.

CRL Distribution Point: A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

Data To Be Signed (DTBS): The complete electronic data to be signed (including both Signer's Document and Signature Attributes)

Digital Signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.

End Entity: A certificate subject that uses its public key for purposes other than signing certificates.

Electronic Signature:

- European Directive [1]: means data in electronic form that are attached to or logically associated with other electronic data.
- 14/08/2000 Luxembourg Law [2]:
  Art. 6. « Signature »
  Après l'article 1322 du Code civil, il est ajouté un article 1322-1 ainsi rédigé :
  "La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.
  Elle peut être manuscrite ou électronique.
  La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article."

Hash Function: A cryptographic function that maps a variable length string of bits to fixed-length strings of bits, satisfying the following two properties:

- It is computationally unfeasible to find for a given output an input which maps to this output
- It is computationally unfeasible to find for a given input a second input which maps to the same output

Key Pair: A Public Key and the corresponding Private Key.

Normalised Certificate Policy (NCP) [4]: A Certificate Policy which offers the same quality as that offer by the Qualified Certificate Policy (QCP) as defined in the technical standard ETSI TS 101 456 but without the legal constraints implied by the Electronic Signature Directive [1] without requiring the use of a Secure User Device (signing or decrypting).

Normalised Certificate Policy + (NCP+) [4]: Normalised Certificate Policy requiring a Secure User Device.

Object Identifier (OID): a sequence of numbers that uniquely and permanently references an object.

Online Certificate Status Provider Protocol (OCSP): an on line trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the server (which contains the certificate status) and the client application (which is informed of that status).

Public Key: That key of an entity's asymmetric key pair that can be made public

Private Key: That key of an entity's asymmetric key pair that should only be used by that entity.

Qualified Certificate [1]: a 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].

Qualified Electronic Signature [1]: an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Note: Definition of Art. 5.1 signature taken from [1]).

Secure Signature Creation Device [1]: means a Signature Creation Device that meets the requirements laid down in [1], Annex III.

Secure User Device [4]: Device which holds the user's private key, 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]: means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature Creation Device [1]: means configured software or hardware used to implement the signature creation data.

Signature Policy: a 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: An organization that creates, maintains and publishes a signature policy.

Signature Policy Issuer Name: A name of a Signature Policy Issuer.

Signature Verification: a 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, which are 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: the registered name of the signer (i.e. as registered by the CSP supplying the signer's certificate).

Signer's Document: The 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): An authority trusted (and widely recognised, possibly accredited) by one or more users to provide Trusted Services such as Timestamping, Certification …

Time Stamp: A 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: An authority trusted by one or more users to provide a Time Stamping Service.

Time Stamping Service: A service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

Validation Data: additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.

Verifier: an 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): a 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): a 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.

Acronyms:

AES	Advanced Electronic Signature
ARL	Authority Revocation List
B2B	Business to Business
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NCP	Normalised Certificate Policy
NCP+	Normalised Certificate Policy +
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKCS	Public Key Certificates Standard
PSF	Prestataire de Services Financiers
QES	Qualified Electronic Signature
QCP	Qualified Certificate Policy
RA	Registration Authority
RAO	Registration Authority Officer
RFC	Request for Comments
RSA	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SCD	Signature Creation Device
SRA	Suspension and Revocation Authority
SRAO	Suspension and Revocation Authority Officer
SSCD	Secure Signature Creation Device
TSA	Time Stamping Authority
TSP	Time Stamping Policy
TSSP	Time Stamping Service Provider
TSU	Time Stamping Unit

URL	Uniform Resource Locator
UTC	Coordinated Universal Time

1.7. Relationship with the European Directive on Electronic Signatures

The LTNCA, as well as all supporting component services, shall target accreditation against ETSI TS 102 042 [4] in application of Article 30 of the Grand-Duchy of Luxembourg law of 14 August 2000 on electronic commerce. OLAS shall be the accreditation entity. For further details please refer to section 8 of the present CP.

Electronic signatures supported by the "LuxTrust NCP+ Signature Certificate" or by the "LuxTrust NCP 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. See the section 1.4 for further details on authorized and prohibited usages of these certificates.

2. Publications and Repository Responsibilities

2.1. Identification of entities operating repositories

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

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

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

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

2.2. Publication of Certification Information

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

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

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

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

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

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 LTNCA, 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 http://status.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

2.3. Time of Frequency of Publication

2.3.1. *Frequency of Publication of Certificates*

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

2.3.2. *Frequency of Publication of Revocation information*

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

2.3.3. *Frequency of Publication of Terms & Conditions*

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

2.4. Access Control on Repositories

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

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

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

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 equivalent identity proofs.

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 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:

- *"Employee"*
- *"Administrator"*

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 Normalised CA Certificates (issued by the LuxTrust Root CA):

Country (C)	LU
Organization (O)	LuxTrust s.a.
Common Name (CN)	LuxTrust Normalised 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*

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 NCP" 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 102 042 technical standard. 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 (S)SCD 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 (S)SCD and/or the Activation Data to the Subscriber using two separated channels. Face-to-face based procedure is optional but not mandatory. 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.

Subscriber's key escrow is never allowed.

3.2.2. *Authentication of organization 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, passport or any equivalent proof of identity) of one of the physical persons who are 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 PSF rules set by the CSSF, 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 any equivalent recognised official document;
- 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 card 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 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[6], 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 http://repository.luxtrust.lu and on http://sra.luxtrust.lu.

[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.

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 LTNCA domain, including the Relying Parties, there is a continuous obligation to inform in a timely manner LuxTrust s.a. with regards to the LTNCA:

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

4.1. Certificate Application

4.1.1. *Who can submit a certificate application*

Any physical person can submit a Certificate application.

E.g. applications of physical persons with a terrorist or criminal background shall be refused if detected.

The LTNCA 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 fulfill the tasks related to the LTNCA 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.

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 Smart Card (LuxTrust NCP+ Certificates) or the LuxTrust Server Signing Account (LuxTrust NCP Certificate) 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 LTNCA). 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.

In case of LuxTrust Smart Card Subscribers, the Certificates are generated in a suspended mode by the LuxTrust LTNCA (Factory). This suspension notification is immediately available in the related CRL and via the LuxTrust Validation Services. In order to collect his/her LuxTrust Smart Card and to unsuspend his/her LuxTrust NCP+ Certificates the Subscriber may present himself (herself) to the LRA where his/her identity will be checked prior Smart Card delivery and re-activation of Certificates.

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

4.1.2.1. Subscriber enrolment process

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

Registration preparation

The Subscriber 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: http://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 CPS [6].

Online Registration Preparation

In order to facilitate the Subscriber registration preparation, to reduce the amount of errors, it shall be foreseen an end-user web-based registration preparation interface. 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: type of identity (physical private person or physical person with professional attributes), type of Signature Creation Device (server signing account, or smart card). 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) may present himself, in person, to one of the LRAs authorized under the present CP. If physical presence is required, the Subscriber may arrange a meeting with an LRA Officer (LRAO) and go there in person, bringing with him/her the 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, passport or equivalent official document. This copy must be signed by the Subscriber;
- A (two-sided) copy of a valid ID card, passport or any equivalent official document 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, passport or equivalent official document. 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, passport or equivalent official document. 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.

The next steps in the Subscriber enrolment process will depend on the choice of the Subscriber to apply either for a LuxTrust Smart Card (i.e., for two LuxTrust NCP+ Certificates respectively for signature purposes and for Authentication & Encryption purposes), or for a LuxTrust Signing Server Account (i.e., for a multipurpose LuxTrust NCP Certificate). These two cases are further detailed here after.

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.
1. Unless identified as stated in section 1.1.3 of the current CP 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.
2. The LRAO will be able to register the personal details and perform a face-to-face identification and authentication.
3. If the subscriber is and 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.

4. 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. 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 subscribers shipping address via postal mail.
5. 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).
6. The Central RA will initiate the creation of the Subscriber's profile by the LuxTrust Signing Server Authority on the LuxTrust Signing Server.
7. The LuxTrust Signing Server responds to the CRA with the User-ID & Public Key which was generated for this Subscriber.
8. The Central RA will request the Certificate from the Certificate Factory (CA).
9. The CA generates the Certificate, and, in case the Subscriber has agreed so, publishes it on the LuxTrust Directory Server
10. The CA responds with the Certificate to the Central RA
11. The Central RA will send the Certificate back to the Signing Server
12. The Signing Server generates the Static Password, and sends the User-ID & Static Password ("Signing Server Account PIN-Letter") securely to the Central RA
13. The Central RA sends the "Signing Server Account PIN-Letter" securely to the Subscriber's shipping data under secure envelope.
14. The CRA sends the UID / OTP-Credential Serial Number information to the LuxTrust Signing Server Authentication Service Provider.
15. 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 per postal mail the Subscriber's PIN-Letter. 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.

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].

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.

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

Enrolment of a new LuxTrust Smart-Card 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.
1. Unless identified as stated in section 1.1.3 of the current CP 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.
2. The LRAO will be able to register the personal details and perform a face-to-face identification and authentication, and request the Subscriber Smart Card.
3. If the subscriber is an identified person as stated in section 1.1.3 of the current CP the subscriber can forward above the mentioned documents via postal mail to the LRA.
4. 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 "Smart Card PIN/PUK-Letter" to the Subscriber (so called Shipping Data).
5. The Central RA will initiate the creation of a LuxTrust Smart Card for the Subscriber's profile to the LuxTrust Smart Card Issuing Authority.
6. The SSCD Issuing Authority will generate the Subscriber key-pairs on a Non-personalised card, and extract the public keys.
7. The SSCD Issuing Authority responds to the CRA with the Public Keys to be certified.
8. The Central RA will request the Certificates from the Certificate Factory (CA).
9. The CA generates the Certificate (in a suspended mode), and, in case the Subscriber has agreed so, publishes them on the LuxTrust Directory Server.
10. The CA responds with the Certificate to the Central RA.
11. The Central RA will send the Certificates back to the SSCD Issuing Authority
12. The SSCD Issuing Authority will add the Certificates to the card, create and send the Smart Card securely to the LRAO or if applicable to the Shipping Data coordinates (this might be done through the CRA).
13. If applicable the LRAO acknowledges reception of the Smart Card (this may be done through the CRA).

14. The SSCD Issuing Authority sends the corresponding "Smart Card PIN/PUK-Letter" to the Central RA.
15. The Central RA sends the PIN/PUK-Letter to the Subscriber's Shipping Data coordinates, via secure channels, inviting the Subscriber to go to the LRA(O).
16. The LRAO hands over the Smart Card to the Subscriber who can request the unsuspension of the suspended Certificates.
17. 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 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 Shipping Data, mentioned here above, are (detailed) coordinates of the Subscriber needed to send per postal mail the Subscriber's Smart Card PIN/PUK-Letter.

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.

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

The detailed procedures and guidelines for 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. Other PKI Participants enrolment process

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

4.1.2.3. 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 the

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

- The Subscriber must agree to the retention - for a period of 10 years from the date of expiry of the last Subscriber Certificate - by the CSP and LRA of all information used for the purposes of registration, for the provision of a (S)SCD or for the suspension or revocation of the Certificate, and, in the event that the CSP ceases its activities, the Subscriber must permit this information to be transmitted to third parties under the same terms and conditions as those laid down in this CP.

- The Subscriber hereby acknowledges the rights, obligations and responsibilities of the CSP, and other PKI participants. These are set out in the LuxTrust CPS [6] currently in effect, in the Order Form and in the General Terms and Conditions relating thereto, and in the present CP.

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 authorized.
- 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 must indicate the full name (last name and first names), date and place of birth of its 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.
- As a post-registration step, the LRAO prepares to the attention of LuxTrust s.a. a paper copy of the full paper-based registration file of the subscriber. Once a month (or at another frequency indicated by LuxTrust s.a.), all these copies of subscribers' paper files are securely sent to LuxTrust s.a. according to the law against money bleaching.
- The 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;
  - 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 and within related LuxTrust internal CRA procedures as part of the CPS.

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 himself 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].
< … insert here any specific action (e.g., check on certificate content format, etc.) that can be performed in the context of this particular CP, reference may be done to the Certificate profile section … >

4.3.2. *Notification to Subscriber by the CA of issuance of Certificate*

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

4.4. Certificate acceptance

4.4.1. *Conduct constituting Certificate acceptance*

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

Objections to accepting an issued Certificate are notified via the 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 4.10 of the present CPS.

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

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

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

4.5. Key pair and certificate usage

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

4.5.1. *Subscriber private key and certificate usage*

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

- In using the Key Pair, the Subscriber must comply with any limitations indicated in the Certificate, in the present CP or in applicable contractual agreements.
- In accordance with the LuxTrust CPS [6] and with the present CP, the Subscriber must protect the Private Key and its Activation Data at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. Once the Private and Public key pair has been delivered to the Subscriber, the Subscriber is personally responsible for ensuring the confidentiality and integrity of the Key Pair. The Subscriber is deemed the sole user of the Private Key. The Private Key Activation Data (e.g., 5 digit Activation Code, PIN-code or password(s)) used to prevent unauthorized use of the Private Key must never be held in the same place as the Private Key itself, nor alongside its storage medium. Nor must it be stored without adequate protection. The Subscriber must never leave the Private Key or the Private Key Activation Data unsupervised when it is not locked (e.g., leave it unsupervised in a work station when the PIN code or password has been entered).

- The Subscriber has sole liability for the use of the Private Key. LuxTrust s.a. acting as CSP is not liable for the use made of the Key Pair belonging to the Subscriber or for any damage resulting from misuse of the Key Pair.
- The Subscriber shall refrain from tampering with a Certificate.
- The Subscriber shall only use Private Key and Certificate for legal and authorised purposes in accordance with the present CP, the Subscriber Agreement and the LuxTrust CPS [6], and as it may be reasonable under the circumstances.
- The Subscriber must ask the CSP to revoke the Certificate as required pursuant to the LuxTrust CPS [6], and in particular if:
    - The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
    - The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data (e.g. PIN code) has been compromised or for any other reason[7]; 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 LuxTrust Smart Card Subscriber shall ensure the destruction of the SSCD or shall give his Smart Card back to a LuxTrust LRA for destruction once all Certificates on the Smart Card are either revoked or expired.
- The LuxTrust Signing Server Account Subscriber accepts that his certified private key shall be destroyed once expired or revoked.

4.5.2. *Relying Party public key and Certificate usage*

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

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

[7] 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).

4.6. Certificate renewal

Not applicable as not allowed.

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 LuxTrust Smart Card and of the secure delivery of the new LuxTrust Smart Card and associated Activation Data (via two separated channels),
- or on a new LuxTrust Signing Server Account (SCD) and of the secure delivery of the SCD (Token) and the associated LuxTrust Signing Server Account Activation Data and the SCD

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.

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

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

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 LTNCA 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 dully 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 unsuspended to become valid again. The revocation process is irreversible. Once revoked, the Certificate cannot be unrevoked. Once the LuxTrust NCP Certificate is revoked (or expired), the corresponding private key is destroyed in accordance with the LuxTrust CPS [6]. shall be destroyed by the Certificate Subscriber himself or brought back by the Subscriber to a LuxTrust LRA for destroying in accordance with the present CPS. [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 CPS); or,

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

The LRA and SRA request promptly to the LTNCA the suspension of a Certificate (or a pair of Certificates in case of LuxTrust Smart Card 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 one month (two months for initial suspension of LuxTrust Smart Card Certificates).

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.

Under specific circumstances, LuxTrust s.a. acting as CSP may request revocation to the SRA of any Certificate in accordance with the LuxTrust CPS. E.g. specific circumstances may be that a LuxTrust Certificate Subscriber appears in a Blacklist.

The suspension, un-suspension and revocation processes are managed by the Suspension and Revocation Authority (SRA), through the CRA towards the LTNCA who technically suspends or revokes a Certificate. The LTNCA 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: http://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

Step 1: The revocation requestor has two means to initiate the procedure:

a) **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 identity through his Suspension/Revocation Password (Challenge).

- If the Challenge is correct, the SRA Hotline will suspend the Certificate for a period of one (1) month maximum, and inform the LuxTrust CRA of the event. This latter will continue the procedure (Step 2).
- If the Challenge is not correct, 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 revocation requestor proceeds via web-site:

- The revocation requestor electronically signs his revocation request (e.g., web-based form) and the signature can be correctly validated, then the revocation request is promptly sent to the CA for prompt processing and revocation of the certificate. The process stops here. CRA can keep trace of the event.
- The revocation requestor does not electronically sign his request, but provides a correct Challenge, then the SRA proceeds to a prompt suspension for a period of one (1) month maximum and inform the LuxTrust CRA of the event. This latter will continue the procedure (Step 2).
- If the Challenge or the electronic signature is not correct or cannot be verified, the SRA performs no change on the validity status of the Certificate but raises an "alarm" towards the CRA.

Step 2: Following immediate suspension performed in Step 1, LuxTrust CRA will ask the revocation requestor to go to an LRA and to proceed to the confirmation of his/her revocation requests within the month.

- When no authorized requestor authenticates to an LRA within the month, the Certificate is automatically revoked.
- When an authorized requestor presents himself at an LRA before the end of the one month period:
  (a) If the authorized requestor confirms at LRA the revocation request, then the LRA, once the authorized requestor and his/her request are authenticated and validated, sends the revocation confirmation to the CRA (using LRA software).
  (b) If the authorised requestor confirms at LRA that (s)he wants to un-suspend the certificate, once the authorized requestor and his/her request are authenticated and validated, sends the un-suspension confirmation to the CRA (using LRA software). This action can also be produced via the SRA Website.
  (c) If the 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.

(Note that unsuspension and suspension case 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 CPS:

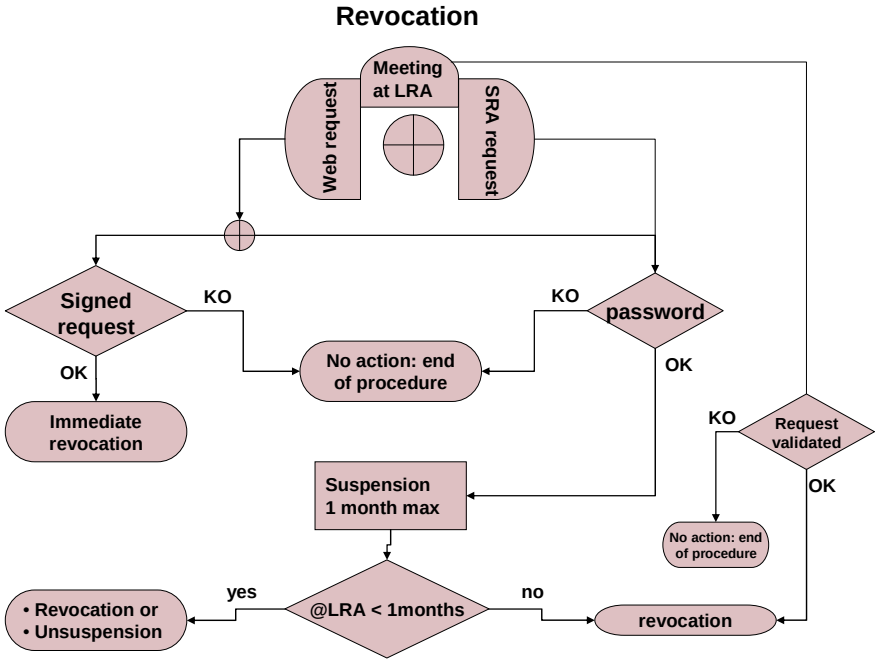
- The LuxTrust Smart Card Subscriber shall ensure the destruction of his Smartcard or alternatively give his Smartcard back to a LuxTrust LRA for destruction once all Certificates on the Smart Card are either revoked or expired.
- The LuxTrust Signing Server Account Subscriber accepts that his certified 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 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, 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 at 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 do not allow affiliated LRAs to access to a digitalised version of the end-user registration file, the revocation requestor shall be required to perform a full validation of his request using a process that is similar to the initial enrolment (registration) process to provide all the required proofs.



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 (updated 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 LTNCA updates OCSP, CRLs and the Web based interface Certificate status validation service accordingly. Relying Parties are made aware of the maximum delay between the receipt of a suspension (or revocation) request or report and the change of certificate validity status information being available to all Relying Parties is indicated in section 4.9.5. Relying Parties shall take this information into account when checking validity status of a Certificate.

4.9.7. *CRL issuance frequency*

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

LuxTrust s.a. makes available Certificate status checking services including CRLs, OCSP and appropriate web interfaces. CRLs are available from http://crl.luxtrust.lu. OCSP services are available from http://ocsp.luxtrust.lu. Web interface for Certificate status checking services is available from http://status.luxtrust.lu and allows a user to obtain status information on a Certificate covering the full history of this Certificate.

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

LuxTrust s.a. makes available all CRLs issued by the LTNCA in the previous [*12*] months available on its repository. Every CRL is stored, archived and available for retrieval for 10 years. Recovery of CRLs older than [*12*] months may be subject to retrieval and administration fees as stated in section 9.1 of the present CP.

4.9.8. *Maximum latency for CRLs*

Not applicable.

4.9.9. *On-line revocation/status checking availability*

LuxTrust s.a. makes available Certificate status checking services related to Certificates issued by the LTNCA 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 LTNCA 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*

In case of Smart Card Subscribers, i.e., LuxTrust NCP+ Certificates, the Certificates are generated in a suspended mode by the LuxTrust LTNCA (Factory). This suspension notification is immediately available in the related CRL and via the LuxTrust Validation Services. Unless the Smartcard was sent directly to the Subscribers Shipping Data the Subscriber may be requested to present himself (herself) to the LRA to collect his/her Smartcard and where his/her identity will be checked prior Smart Card delivery and re-activation of Certificates. If the SSCD is sent to the Certificate Subscriber by postal mail, the activation and testing of the card can be performed online through http://cat.luxtrust.lu. Initial suspension has a maximum duration of two (2) months. 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: http://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 Smart-Card Certificates, (certificates are kept suspended until hand-over of the card to the card owner).
- Requested suspension by an authorized party (see also section 4.9.14).

Initial Suspension of LuxTrust NCP+ Certificates (on LuxTrust Smart Card)

The initial suspension (related to LuxTrust Smart Card Certificates issuance) leads to a two (**2) months** suspension period at a maximum. Two cases are then possible:

a. The Smart Card Subscriber presents himself for the hand-over of his Smart Card at LRA before the end of the 2 months period, and then the Certificates are un-suspended. This action can also be performed via the SRA Website.
b. If the Subscriber does not present himself before the end of the 2 months period, the Certificates are automatically revoked.

Suspension of an existing LuxTrust Subscriber: process overview

A requested suspension leads to a **one (1) month 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 http://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.
- If the Challenge, the SRA Hotline will suspend the Certificate for a maximum period of one (1) month, 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.

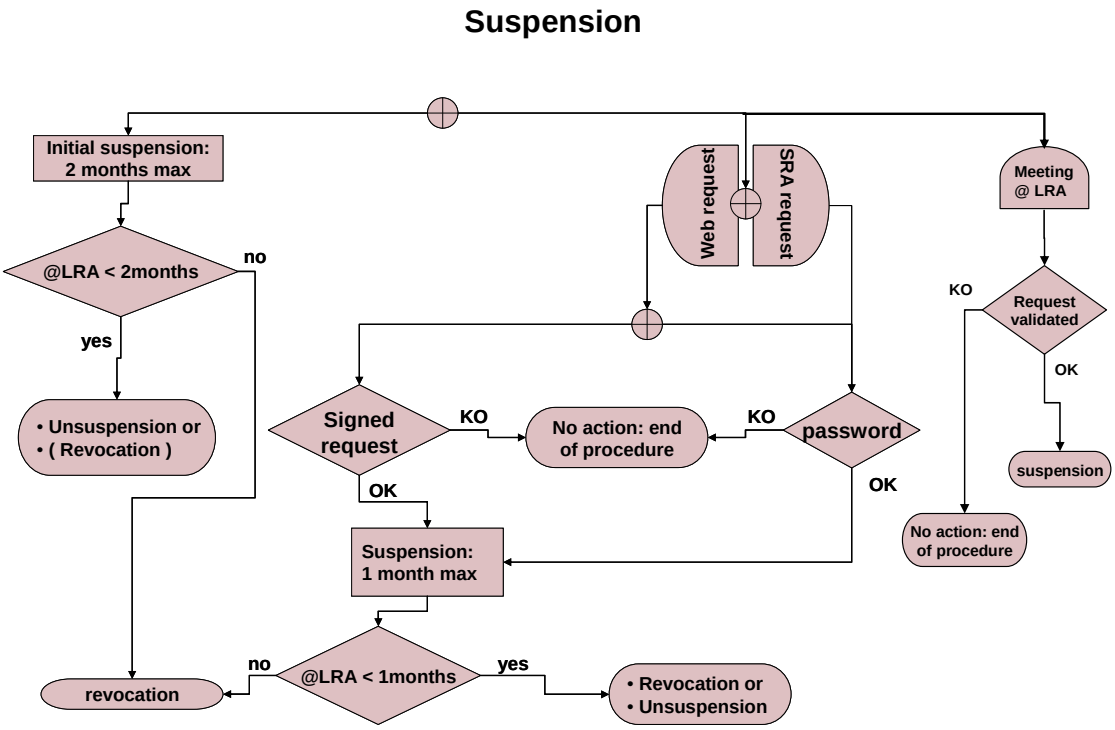
b) **SRA Website based procedure**: The suspension requestor proceeds via web-site:
- The suspension requestor electronically signs a suspension form-based request. If the signature is validated, then the suspension request is promptly sent to the CA for prompt processing and suspension of the certificate for a period of one (1) month and the SRA will inform the LuxTrust CRA of the event..
- The suspension requestor does not electronically sign his request, but provides a correct Challenge, then the certificate is promptly suspended by the SRA for a period of one (1) month 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 one month suspension period the Certificate can either be un-suspended or revoked before automatic revocation at expiration of the one month 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 unsuspension is performed at an LRA within the one month suspension period, the Certificate is automatically revoked.

- When an authorized requestor presents himself at an LRA before the end of the one month suspension period:
  (a) If the authorized requestor requests at LRA the revocation of the Certificate, then the LRA, once the authorized requestor and his/her request are authenticated and validated, sends the revocation request to the CRA (using LRA software).
  (b) If the authorized requestor requests at LRA that (s)he wants to un-suspend the certificate, once the authorized 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 authorized 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 he can electronically sign an appropriate web-based form), the suspension requestor must present himself to an LRA to proceed to the authentication of his request.



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

4.9.16. *Limits on suspension period*

In case of Smart Card Subscribers, i.e., LuxTrust NCP+ Certificates, the Certificates are generated in a suspended mode by the LuxTrust CA (Factory). This initial suspension is set for a maximum period of two (2) months; afterwards if not correctly unsuspended the Certificates are revoked. Unless the Smartcard was sent directly to the Subscribers Shipping Data the Subscriber is requested to present himself (herself) to the LRA to collect his/her Smartcard and where his/her identity will be checked prior Smart Card delivery and re-activation of Certificates. Un-suspension procedure can occur during face-to-face delivery of Subscriber's LuxTrust Smart Card during initial enrolment process or in a more general way as it is described hereafter.

When otherwise suspended, the Certificate is suspended for a maximum period of one (1) month. After this period, unless the Certificate has been validly requested to be un-suspended, the Certificate is automatically revoked.

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

1. The un-suspension requestor may present him(her)-self to an LRA to proceed to confirmation of his/her un-suspension request (i.e., within one month from a suspension or a revocation request, or within two months from NCP+ 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 trough 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.

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 Normalised 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 LTNCA 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 LTNCA 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

7.1.1 Version number(s)

X.509 v3 is supported and used.

7.1.1.1 LuxTrust NCP+ Certificates

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

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

The usage purpose of these LuxTrust NCP+ Certificates is either for electronic signature purpose or for the combined purpose of authentication and encryption. The LuxTrust NCP+ Certificates include the corresponding LuxTrust NCP+ oid, i.e., respectively for Signature Certificate *<1.3.171.1.1.2.1.1>***,** and for the Authentication & Encryption Certificate ***<1.3.171.1.1.2.1.2>*.** See section 1.4 for further information on Certificate authorized and prohibited usage.

The following tables provide the description of the fields for LuxTrust NCP+ Certificates.

LuxTrust NCP+ Signature Certificate Profile

Attribute	Field	IN[8]	CE[9]	O/M[10]	CO[11]	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 Normalised 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			
	countryName	✓		M	D	*Nationality (ISO3166)*
	localityName	✓		M	D	***Professional or Legal Person**: Legal person locality of HQ (as in articles of association) – Mandatory*
	organizationName	✓		M	D	***Professional Person only**: Name as in articles of association, including the legal form. Mandatory when Subscriber is a legal representative of the Organisation*
	organizationalUnitName 1	✓		M	D	*Mandating company RCSL number (or VAT number if no RCSL available)*
	organizationalUnitName 2	✓		O	D	*Company department involved*
	commonName	✓		M	D	***Legal Person**: Concatenation of surname and first given name as on ID card*
	surName	✓		M	D	*Surname*
	givenName	✓		M	D	*Given name(s) as on ID card*
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	emailAddress	✓		M	D	*Subject's email address*
	title	✓		M	D	***Professional Person or Administrator**: <Physical Professional Person*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 1024 (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Normalised CA public key

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

Attribute	Field	IN[8]	CE[9]	O/M[10]	CO[11]	Value
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTNCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				"http://crl.luxtrust.lu/LTNCA.crl"
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		M	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	✓			S	1.3.171.1.2.1.1
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	http://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	LuxTrust Normalised Certificate on SSCD. Usage: Electronic Signature (OID 1.3.171.1.2.1.1) Authentication and Encryption (OID 1.3.171.1.2.1.2). Key Generation by CSP
	PolicyIdentifier	✓			S	0.4.0.2042.1.2

LuxTrust NCP+ Authentication & Encryption Certificate Profile

Attribute	Field	IN[12]	CE[13]	O/M[14]	CO[15]	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 Normalised 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			
	countryName	✓		M	D	*Nationality (ISO3166)*
	localityName	✓		M	D	***Professional or Legal Person**: Legal person locality of HQ (as in articles of association) – Mandatory*
	organizationName	✓		M	D	***Professional Person only**: Name as in articles of association, including the legal form. Mandatory when Subscriber is a legal representative of the Organisation*
	organizationalUnitName 1	✓		M	D	*Mandating company RCSL number (or VAT number if no RCSL available)*
	organizationalUnitName 2	✓		O	D	*Company department involved*
	commonName	✓		M	D	***Legal Person**: Concatenation of surname and first given name as on ID card*
	surName	✓		M	D	*Surname*
	givenName	✓		M	D	*Given name(s) as on ID card*
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	emailAddress	✓		M	D	*Subject's email address*
	title	✓		M (M for Prof. Pers.)	D	***Professional Person or Administrator**: <Physical Professional Person* ***Legal person**: legal form*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 1024 (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Normalised CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2

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

Attribute	Field	IN[12]	CE[13]	O / M[14]	CO[15]	Value
	accessLocation	✓				http://ca.luxtrust.lu/LTNCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				"http://crl.luxtrust.lu/LTNCA.crl"
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		M	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
	keyEncipherment	✓			S	True
	dataEncipherment	✓			S	True
certificatePolicies		✓	False			
	PolicyIdentifier	✓			S	1.3.171.1.2.1.2
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	http://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	LuxTrust Normalised Certificate on SSCD. Usage: Electronic Signature (OID 1.3.171.1.2.1.1) Authentication and Encryption (OID 1.3.171.1.2.1.2). Key Generation by CSP
	PolicyIdentifier	✓			S	0.4.0.2042.1.2

7.1.1.2 LuxTrust NCP Certificates

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

These LuxTrust NCP Certificates are compliant with and include the oid reference of the NCP certificate policy of the ETSI Technical Standard 102 042 (i.e., 0.4.0.2042.1.1).

The usage purpose of these LuxTrust NCP Certificates is the combined purpose of electronic signature, authentication and encryption. The LuxTrust NCP Certificates include the corresponding LuxTrust NCP oid, i.e., < OID 1.3.171.1.2.1.x>.

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

LuxTrust NCP Certificate Profile						
Attribute	**Field**	**IN**[16]	**CE**[17]	**O/M**[18]	**CO**[19]	**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 Normalised 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			
	countryName	✓		M	D	*Nationality (ISO3166)*
	stateOrProvinceName	✓		n/a	D	
	localityName	✓		M	D	***Professional or Legal Person**: Legal person locality of HQ (as in articles of association) – Mandatory*
	organizationName	✓		M	D	***Professional Person only**: Name as in articles of association, including the legal form. Mandatory when Subscriber is a legal representative of the Organisation*
	organizationalUnitName (x2)	✓		M	D	Mandating company RCSL number (or VAT number if no RCSL available)
	commonName	✓		M	D	***Legal Person:** Concatenation of surname and first given name as on ID card*
	surName	✓		M	D	*Surname*
	givenName	✓		M	D	*Given name(s) as on ID card*
	pseudonym	✓		n/a	D	*(only present in case of pseudonym)*
	serialNumber	✓		M	D	*Serial Number as constructed by LRAO*
	postalAddress	✓		M	D	*HQ*
	homePostalAddress	✓		n/a	D	
	emailAddress	✓		M	D	*Subject's email address*
	title	✓		M	D	***Professional Person**: <Physical Professional Person - >*
subjectPublicKeyInfo		✓	False			
	algorithm	✓				Public Key: Key length: 1024 (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	✓		M		
Extensions						
Authority Properties						
authorityKeyIdentifier		✓	False			

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

LuxTrust NCP Certificate Profile						
Attribute	**Field**	**IN**[16]	**CE**[17]	**O/M**[18]	**CO**[19]	**Value**
	keyIdentifier	✓				SHA-1 Hash of the LuxTrust Normalised CA public key
authorityInfoAccess		✓	False			
	AccessMethod	✓				Id-ad-2
	accessLocation	✓				http://ca.luxtrust.lu/LTNCA.crt
	AccessMethod	✓				Id-ad-1
	accessLocation	✓				http://ocsp.luxtrust.lu
cRLDistributionPoint		✓	False			
	distributionPoint	✓			S	
	fullName	✓				"http://crl.luxtrust.lu/LTNCA.crl"
Subject Properties						
subjectAltName		✓	False			
	Rfc822Name	✓		M	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	✓			S	LuxTrust NCP OID
	policyQualifierID	✓			S	Id-qt-1 (CPS)
	qualifier	✓			S	http://repository.luxtrust.lu
	policyQualifierID	✓			S	Id-qt-2 (User Notice)
	noticeNumbers					
	DisplayText	✓			S	LuxTrust CP for Normalised Certificates. *Usage: Encryption, Authentication and Electronic Signature.* Not supported by SSCD, Key Generation by CSP. GTC, CP and CPS on http://repository.luxtrust.lu
	PolicyIdentifier	✓			S	0.4.0.2042.1.1
Netscape Proprietary						
NetscapeCertificateType		✓	False			
	SSL Client	✓			S	Set
	S/MIME	✓			S	Set

7.1.2 Certificate extensions

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

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

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

7.1.5 Name constraints

Name constraints are supported as per RFC 3280.

7.1.6 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739.

7.1.7 Usage of Policy Constraints extension

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

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies

Not applicable.

7.2. CRL profile

In conformance with the IETF PKIX RFC 2459, LuxTrust s.a., through its LTNCA 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:

Field	**Comments**
Version	v2
Signature	Sha1RSA
Issuer	<subjectCA>
thisUpdate	<creation time>
nextUpdate	<creation time + 14 days>
revokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
reasonCode	*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 LTNCA 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 service for Certificates issued by its LTNCA.

7.2.2. *CRL entry extensions*

See section 7.2.

7.3. OCSP profile

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

7.3.1. *Version number(s)*

See section 7.3.

7.3.2. *OCSP extensions*

See section 7.3.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

With regard to the provision of LuxTrust Normalised Certificates (NCP & NCP+), LuxTrust s.a. through its LuxTrust Normalised 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 to the ETSI technical standard TS 102 042 “Policy requirements for certification authorities issuing public key certificates” (Normalised level),
- According to the present CP and the LuxTrust CPS.

As described and ruled in the LuxTrust CPS, LuxTrust s.a. acting as CSP accepts for its LTNCA and all its supporting certification services compliance audit to ensure they meet, within 18 months following services set-up, the OLAS 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 OLAS website, www.olas.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.

Please refer to the LuxTrust CPS 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 Signing Server 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 CPS, such as:
  - Repositories access fees: None for the time being, but this might be subject to changes in the future depending on several factors.
  - Time Stamping Services fees: None for the time being, but this might be subject to changes in the future depending on several factors
- 9.1.5 Refund policy: not applicable

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 thirty (30) 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.

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 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 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, express or implied, in any Proprietary Materials other than the rights expressly granted in the CP.

9.6. Representations and warranties

9.6.1. *CA representations and warranties*

LuxTrust s.a., through its LTNCA issues X509 v3-compatible Certificates (ISO 9594-8).

LuxTrust s.a., through its LTNCA issues Certificates compliant with ETSI TS 102 042 Normalised Certificates requirements. To this end, LuxTrust s.a. publishes the elements supporting this statement of compliance.

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

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

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

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

LuxTrust s.a. acting as CSP through its LTNCA 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 CPS, LuxTrust s.a. acting as CSP may revoke or suspend the Certificate, provided it informs the Subscriber (and any other concerned authorised party, if applicable) of the Certificate in advance by appropriate means.

LuxTrust s.a. 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 standard ETSI TS 102 042.

LuxTrust s.a. guarantees that it will provide a SCD (NCP) or SSCD (NCP+) in a secured way and in accordance with the requirements set out in the technical standard ETSI TS 102 042. 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 LTNCA shall undertake liability for all RA services provided on behalf of the LTNCA. RA liabilities are therefore primarily handled between LuxTrust s.a. and the RA. LuxTrust s.a. shall synchronize its contract with the RA to the present CP.

See LuxTrust CPS for all additional rights, responsibilities and obligations of LuxTrust s.a. acting as CSP through its LTNCA.

9.6.2. *RA representations and warranties*

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

9.6.3. *Subscriber representations and warranties*

The Subscriber accepts the Certification Practice Statement (CPS) currently in effect, as provided by LuxTrust CSP and setting out the procedures used for providing the Certificates.
The Subscriber agrees to the present CP and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the present CP (e.g., but not limited to, 1.3.3, 1.4, 4, 4.1.2.3, 4.5.1, 9).

In particular, the Subscriber is liable towards Relying Parties for any use that is made of his/her LuxTrust Smart Card or LuxTrust 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 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, 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, 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 his agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that LuxTrust s.a. and its agents and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:

- Falsehood or misrepresentation of fact by the Subscriber;
- Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive LuxTrust or any person receiving or relying on the Certificate;
- Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key.

9.8. Limitations of liability

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

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

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

9.9. Indemnities

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

9.10. Term and termination

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

9.11. Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the present 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:

Contact Person: Daniel Neuhengen

Postal Address:
LuxTrust CSP Board,
LuxTrust S.A.,
Boîte Postale 43.
L-2010 Luxembourg
Telephone number: +352 26 68 15 - 1
Fax number: +352 26 68 15 - 789
E-mail address: *cspboard@luxtrust.lu*
Website: *www.luxtrust.lu*

9.12. Amendments

9.12.1. *Procedure for amendment*

LuxTrust s.a. via its CSP Board is responsible for approval and changes of the present CP.

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

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

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

9.12.2. *Notification mechanism and period*

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

9.12.3. *Circumstances under which OID must be changed*

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

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

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

9.13. Dispute resolution provisions

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

9.14. Governing law

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

9.15. Compliance with applicable law

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

9.16. Miscellaneous provisions

LuxTrust s.a. acting as CSP incorporates by reference, through its LuxTrust Normalised CA, the following information in all Certificates it issues:

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

To incorporate information by reference LuxTrust s.a. through its LTNCA uses computer-based and text based pointers that include URLs, OIDs, etc.