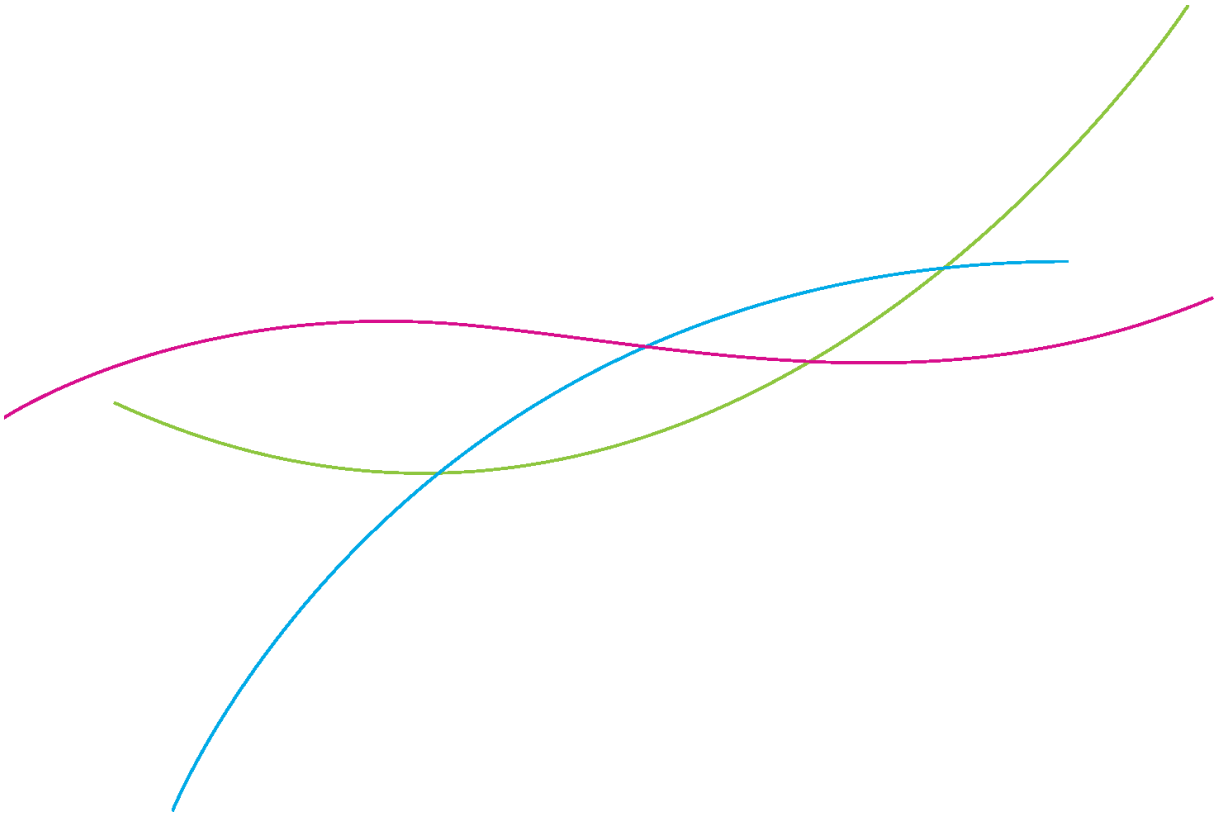

LuxTrust Enterprise CA Certificate Prolicy

Version number: 1.0

CPS Refenrece Document O.I.D: 1.3.171.1.1.1.11

Document Information

Document title:	LuxTrust Enterprise CA Certificate Prolicy
Project Reference:	LuxTrust S.A.
Document Archival Code:	

Version History

Version	Who	Date	Reason of modification
1.0	YNU	17/01/2022	First version

Table of content

Intellectual Property Rights

References

CPS – LuxTrust Enterprise CA Certificate Practice Statement

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

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

1 Introduction

1.1 Overview

This document describes the certificate profile issued by the LuxTrust Enterprise CA. It is also intended to specify, where applicable, the context for the application, issuance, management and use of the type of certificates described in this Certificate Policy (CP). The set of rules, requirements and definitions set out also determines the level of security and assurance provided by the types of certificates that are issued under this CP.

1.2 Document name and identification

This CP is valid only in conjuction with the LuxTrust Enterprise CA Certificate Practice Statement (CPS) identified through the following OID: 1.3.171.1.1.1.11

1.3 PKI Participants

No requirements other than those specified in the CPS.

1.4 Certificate usage

No requirements other than those specified in the CPS.

1.5 Policy administration

No requirements other than those specified in the CPS.

1.6 Definitions and acronyms

No requirements other than those specified in the CPS.

2 Publications and Repository Responsibilities

No requirements other than those specified in the CPS.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 *Types of names*

See ch. 7 for detailed naming rules and for detailed structure of the Certificates subject attributes.

3.1.2 *Need for names to be meaningful*

No requirements other than those specified in the CPS.

3.1.3 *Anonymity or pseudonymity of Subscribers*

No requirements other than those specified in the CPS.

3.1.4 *Uniqueness of names*

No requirements other than those specified in the CPS.

3.1.5 *Recognition, authentication, and role of trademarks*

No requirements other than those specified in the CPS.

3.2 Initial identity validation

No requirements other than those specified in the CPS.

3.3 Identification and authentication for re-key requests

No requirements other than those specified in the CPS.

3.4 Identification and authentication for revocation request

No requirements other than those specified in the CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

No requirements other than those specified in the CPS.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

No requirements other than those specified in the CPS.

6 TECHNICAL SECURITY CONTROLS

No requirements other than those specified in the CPS.

7 CERTIFICATE PROFILES

7.1 Signing Server Person LCP

The LuxTrust Lightweight Person certificate profile is compliant with the ETSI EN 319 411-1 LCP standard, with key generation by LuxTrust.

7.1.1 *Signing Server Person LCP Certificate Profile*

LuxTrust Enterprise CA - Signing Server LCP Certificate Profile			
Attribute	**Field**	**O/M**[1]	**Value**
Base Profile			
Version			
		M	Version 3 Value = "2"
SerialNumber			
		M	Validated on duplicates.
signatureAlgorithm			
	algorithm	M	OID = "1.2.840.113549.1.1.11" – if SHA256 with RSA Encryption.
signatureValue			
		M	Issuing CA Signature.
Issuer			
	countryName	M	LU
	commonName	M	LuxTrust **Enterprise** CA x[2]
	organizationName	M	LuxTrust S.A.
Validity			
	NotBefore	M	Certificate generation process date/time.
	NotAfter	M	Certificate generation process date/time + **36 || 48 || 60** Months
subject			
	serialNumber	M	*Serial Number as constructed by LRAO*
	commonName	M	*Concatenation of given name(s) and surname(s) separated by a "Space" character*
	givenName	M	*Given name(s)*
	surname	M	*Surname(s)*
	countryName	M	*Nationality of holder (ISO3166)*
	emailAddress	O	*Deprecated - Email address*
	title	M	***PRI products: "Private Person"*** ***PRO products:*** - ***"Professional Person"*** *(default) or* - ***"Professional Administrator"***
	organizationName	M for PRO	***PRO products only****: Name of company/institution*
	localityName	M for PRO	***PRO products only****: Company/institution country*

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

[2] X is a sequential value to distinguish the old CA and the renewed CA. The value 1 is omitted as it is the first CA issued.

LuxTrust Enterprise CA - Signing Server LCP Certificate Profile			
Attribute	**Field**	**O/M[1]**	**Value**
	organizationalUnitName[4]	M for PRO O for PRI	***PRO products**:* *Company/Institution VAT number (or if no VAT number available, either another unique national identifier of the legal entity or a value provided by the legal entity or by LuxTrust.)* ***PRI products:*** *If the holder is underage: "Mineur jusqu'à : " & (Date of birth + 18 years).*
	organizationalUnitName[4]	O for PRO	***PRO products only**: Legal entity department or other value provided by the legal entity*
subjectPublicKeyInfo			
	algorithm	M	Public Key: Key length: From 3072 bits up to 4096 bit (RSA); public exponent: Fermat-4 (=010001).
	subjectPublicKey	M	
Extensions			
Authority Properties			
authorityKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of the LuxTrust Enterprise CA public key
authorityInfoAccess			
	AccessMethod		Id-ad-2
	accessLocation	M	http://ca.luxtrust.lu/LTEPCAx[2].crt
	AccessMethod		Id-ad-1
	accessLocation	M	http://y[3].epca.ocsp.luxtrust.lu/
cRLDistributionPoint			
	distributionPoint		
	fullName	M	http://epca.crl.luxtrust.lu/LTEPCAx[2]- y[3].crl
Subject Properties			
subjectAltName			
	Rfc822Name	O	*Deprecated - Email address*
subjectKeyIdentifier			
	keyIdentifier	M	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			
	digitalSignature	M	True
	nonRepudiation	M	True
	keyEncipherment	M	True
	dataEncipherment		False
certificatePolicies			
	PolicyIdentifier	M	1.3.171.1.1.1.11.**z** please refer to the list below 7.1.2 for the value of **z**

[3] Y corresponds to the last digit for the LuxTrust OID

LuxTrust Enterprise CA - Signing Server LCP Certificate Profile			
Attribute	**Field**	**O/M[1]**	**Value**
	policyQualifierID		Id-qt-1 (CPS)
	qualifier	M	https://epca.repository.luxtrust.lu
	policyQualifierID		Id-qt-2 (User Notice)
	PolicyIdentifier	M	0.4.0.2042.1.3

7.1.2 *Signing Server Person LCP Certificate OID*

This list specifies the name of the ra to which the OID is assigned.

The certificate profile used is the one described above in 7.1.1

The certificate can only be used in the context of the services offered by the RA to which the OID is assigned.

RA Name	OID	Duration	Key length	Procédures
LuxTrust	1.3.171.1.1.1.11.1	36 months	3072	Internal procedure / Restricted access
Natixis	1.3.171.1.1.1.11.2	36 months	3072	Internal procedure / Restricted access
EDF	1.3.171.1.1.1.11.3	36 months	3072	Internal procedure / Restricted access
ING	1.3.171.1.1.1.11.4	36 months	3072	Internal procedure / Restricted access
Raiffeisen	1.3.171.1.1.1.11.5	36 months	3072	Internal procedure / Restricted access
3DS	1.3.171.1.1.1.11.6	36 months	3072	Internal procedure / Restricted access
CALIE	1.3.171.1.1.1.11.7	36 months	3072	Internal procedure / Restricted access
DGSANTE	1.3.171.1.1.1.11.8	36 months	3072	Internal procedure / Restricted access
BDL	1.3.171.1.1.1.11.9	36 months	3072	Internal procedure / Restricted access
Thales	1.3.171.1.1.1.11.10	36 months	3072	Internal procedure / Restricted access
BP2S	1.3.171.1.1.1.11.11	36 months	3072	Internal procedure / Restricted access
POST	1.3.171.1.1.1.11.12	36 months	3072	Internal procedure / Restricted access / DPI
Not Used	1.3.171.1.1.1.11.13	36 months	3072	/
Not Used	1.3.171.1.1.1.11.14	36 months	3072	/
Not Used	1.3.171.1.1.1.11.15	36 months	3072	/
Not Used	1.3.171.1.1.1.11.16	36 months	3072	/
Not Used	1.3.171.1.1.1.11.17	36 months	3072	/
Not Used	1.3.171.1.1.1.11.18	36 months	3072	/
Not Used	1.3.171.1.1.1.11.19	36 months	3072	/
Not Used	1.3.171.1.1.1.11.20	36 months	3072	/

7.2 SSL Client LCP Certificate

LuxTrust SSL Client LCP Certificate is compliant with ETSI EN 319 411-1 LCP standard. The creation of the keys is perfomed by the Subscriber, with

- 3072-bit key size five (5) validity from issuing start date.
- 4096-bit key size ten (10) validity from issuing start date.

This LuxTrust SSL Client Certificate is compliant with and include the OID reference of the LCP certificate policy of the ETSI Standard EN 319 411-1 (i.e., 0.4.0.2042.1.3).

The purpose of using this LuxTrust SSL Client LCP certificate is to authenticate a client to a remote server during an online request. The key usage is specified by the combination of the digital signature, the key and the data encryption. The LuxTrust LCP Server Certificates include the corresponding **LuxTrust OID SSL client LCP certificate**, i.e., 1.3.171.1.1.1.11.21

The identity validation procedure is documented in the internal LuxTrust SSL Client procedure.

The following table provides the description of the fields for this LuxTrust SSL Client Certificate:

LuxTrust SSL Client LCP Certificate Profile			
Attribute	**Field**	**O/M**	**Value**
Base Profile			
Version			
		M	Version 3 Value = "2"
SerialNumber			
		M	Validated on duplicates.
signatureAlgorithm			
	Algorithm	M	OID = "1.2.840.113549.1.1.11" - SHA256 with RSA Encryption.
signatureValue			
		M	Issuing CA Signature.
Issuer			
	countryName	M	LU
	commonName	M	LuxTrust Enterprise CA x[2]
	organizationName	M	LuxTrust S.A.
Validity			
	NotBefore	M	Certificate generation process date/time.
	NotAfter	M	Certificate generation process date/time + **60 || 120** Months
Subject			
	countryName	M	Country in which the company's or institution's registered office is established (as specified in the memorandum and articles of association). (ISO3166)
	stateOrProvinceName	O	State or Province in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	localityName	M	Location in which the company's registered office is established (as specified in the memorandum and articles of association or an equivalent document)
	organizationName	M	Names as in articles of association, including the legal form (as specified in the memorandum and articles of association or an equivalent document)
	organizationalUnitName[4]	O	As provided by Subscriber
	organizationalUnitName[4]	O	As provided by Subscriber
	commonName	M	As provided by Subscriber
	serialNumber	O	Serial Number as provided by subscriber
	emailAddress	O	Subject's email address
subjectPublicKeyInfo			
	Algorithm		Public Key: Key length: • 3072 bit (RSA) for 60 months validity • 4096 bit (RSA) for 120 months validity Public exponent: Fermat-4 (=010001).
	subjectPublicKey	M	
Extensions			
Authority Properties			
authorityKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of the LuxTrust **Enterprise** CA public key
authorityInfoAccess			
	AccessMethod		Id-ad-1
	accessLocation	M	http://y[5].epca.ocsp.luxtrust.lu/

[4] it is an option to set two different values for this field

[5] Y corresponds to the last digit for the LuxTrust OID

LuxTrust SSL Client LCP Certificate Profile			
Attribute	**Field**	**O/M**	**Value**
	AccessMethod		Id-ad-2
	accessLocation	M	http://ca.luxtrust.lu/LTEPCAx[2] .crt
cRLDistributionPoint			
	distributionPoint		
	fullName	M	http://epca.crl.luxtrust.lu/LTEPCAx[2]- y[3].crl
Subject Properties			
subjectAltName			
	Rfc822Name	O	Certificate Holder's email address
subjectKeyIdentifier			
	keyIdentifier	M	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). Fixed value
Policy Properties			
keyUsage			
	digitalSignature	M	True
	nonRepudiation		False
	keyEncipherment	M	True
	dataEncipherment	M	True
certificatePolicies			
	PolicyIdentifier	M	1.3.171.1.1.1.11.21
	policyQualifierID		Id-qt-1 (CPS)
	Qualifier	M	https://epca.repository.luxtrust.lu
	PolicyIdentifier		0.4.0.2042.1.3
Extended Key Usage			
	serverAuth		False
	clientAuth (1.3.6.1.5.5.7.3.2)	M	True
	emailProtection	M	True

7.3 Integration certificates

Integration certificates delivered in the context of test activities are identified by same O.I.D as real certificates and prefixed with 2.999 {joint-iso-itu-t(2) example(999)}, e.g. 2.999. 1.3.171.1.1.1.11.1

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No requirements other than those specified in the CPS.

9 OTHER BUSINESS AND LEGAL MATTERS

No requirements other than those specified in the CPS.