

LUXTRUST

Enabling a digital world

LuxTrust Enterprise CA Certificate Policy

CPS Reference Document O.I.D: 1.3.171.1.1.1.11

Date issues:

2026-03-11

Publication Date:

2026-03-20

Version 1.2

Copyright © 2026

All rights reserved

LuxTrust S.A.
13-15, Parc d'activités
L-8308 Capellen, Luxembourg

VAT LU 20976985
RCS B112233
Business Number N°00135240/5

+352 26 68 15 – 1
info@luxtrust.lu
www.luxtrust.com

Document Information

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

Version History

Version	Who	Date	Reason of modification
1.0	YNU	17/01/2022	First version
1.1	YNU/VMI	20/07/2022 15/01/2024	Update lifespan of 1.3.171.1.1.1.11.21 Update OID: 1.3.171.1.1.1.11.13
1.2	CSP Board	11/03/2026	Added <ul style="list-style-type: none"> • Signing Server Person LCP <ul style="list-style-type: none"> ○ Added ECC - 1.2.840.10045.2.1 <ul style="list-style-type: none"> ▪ ECDSA_P256 - 1.2.840.10045.3.1.7 ▪ ECDSA_P384 - ansip384r1 - 1.3.132.0.34 • Timestamping LCP Policy - 1.3.171.1.1.1.11.22 • Signing Server eSeal LCP Policy - 1.3.171.1.1.1.11.23

Table of content

Document Information.....	2
Version History.....	2
Table of content	3
Intellectual Property Rights.....	4
References	5
1 Introduction	6
1.1 Overview.....	6
1.2 Document name and identification	6
1.3 PKI Participants.....	6
1.4 Certificate usage.....	6
1.5 Policy administration	6
1.6 Definitions and acronyms.....	6
2 Publications and Repository Responsibilities... 7	
3 IDENTIFICATION AND AUTHENTICATION	8
3.1 Naming	8
3.2 Initial identity validation.....	8
3.3 Identification and authentication for re-key requests	8

3.4 Identification and authentication for revocation request 8

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 9

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 9

6 TECHNICAL SECURITY CONTROLS..... 9

7 CERTIFICATE PROFILES..... 10

7.1 Signing Server Person LCP..... 10

7.2 SSL Client LCP Certificate 13

7.3 Integration certificates..... 16

7.4 Timestamping LCP Certificate Profile 17

7.5 Signing Server eSeal LCP Certificate Profile..... 20

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 23

9 OTHER BUSINESS AND LEGAL MATTERS..... 23

Intellectual Property Rights

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

References

[1] CPS – LuxTrust Enterprise CA Certificate Practice Statement.

[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

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

[4] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data replaced by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR).

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 conjunction 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	<i>Serial Number as constructed by LRAO</i>
	commonName	M	<i>Concatenation of given name(s) and surname(s) separated by a "Space" character</i>
	givenName	M	<i>Given name(s)</i>
	surname	M	<i>Surname(s)</i>

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
	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
	organizationalUnit Name⁴	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).
	organizationalUnit Name⁴	O for PRO	PRO products only: Legal entity department or other value provided by the legal entity
subjectPublicKeyInfo			
	algorithm	M	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$. ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
	subjectPublicKey	M	
Extensions			
Authority Properties			
authorityKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of the LuxTrust Enterprise CA public key
authorityInfoAccess			

LuxTrust Enterprise CA - Signing Server LCP Certificate Profile			
Attribute	Field	O/M ¹	Value
	AccessMethod		Id-ad-2
	accessLocation	M	<a href="http://ca.luxtrust.lu/LTEPCA<sup>2</sup>.crt">http://ca.luxtrust.lu/LTEPCA².crt
	AccessMethod		Id-ad-1
	accessLocation	M	<a href="http://y<sup>3</sup>.epca.ocsp.luxtrust.lu/">http://y³.epca.ocsp.luxtrust.lu/
cRLDistributionPoint			
	distributionPoint		
	fullName	M	<a href="http://epca.crl.luxtrust.lu/LTEPCA<sup>2</sup>-y<sup>3</sup>.crl">http://epca.crl.luxtrust.lu/LTEPCA²-y³.crl
Subject Properties			
subjectAltName			
	Rfc822Name	O	<i>Deprecated - Email address</i>
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
	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

³ Y corresponds to the last digit for the LuxTrust OID

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	Procédures
LuxTrust	1.3.171.1.1.1.11.1	36 months	Internal procedure / Restricted access
Natixis	1.3.171.1.1.1.11.2	36 months	Internal procedure / Restricted access
EDF	1.3.171.1.1.1.11.3	36 months	Internal procedure / Restricted access
ING	1.3.171.1.1.1.11.4	36 months	Internal procedure / Restricted access
Raiffeisen	1.3.171.1.1.1.11.5	36 months	Internal procedure / Restricted access
3DS	1.3.171.1.1.1.11.6	36 months	Internal procedure / Restricted access
CALIE	1.3.171.1.1.1.11.7	36 months	Internal procedure / Restricted access
DGSANTE	1.3.171.1.1.1.11.8	36 months	Internal procedure / Restricted access
BDL	1.3.171.1.1.1.11.9	36 months	Internal procedure / Restricted access
Thales	1.3.171.1.1.1.11.10	36 months	Internal procedure / Restricted access
BP2S	1.3.171.1.1.1.11.11	36 months	Internal procedure / Restricted access
POST	1.3.171.1.1.1.11.12	36 months	Internal procedure / Restricted access / DPI
SGBT	1.3.171.1.1.1.11.13	36 months	Internal procedure / Restricted access
LuxTrust	1.3.171.1.1.1.11.14	36 months	Internal procedure / Restricted access
BDL	1.3.171.1.1.1.11.15	36 months	Internal procedure / Restricted access
Eagle1	1.3.171.1.1.1.11.16	36 months	Internal procedure / Restricted access
Not Used	1.3.171.1.1.1.11.17	36 months	/
Not Used	1.3.171.1.1.1.11.18	36 months	/
Not Used	1.3.171.1.1.1.11.19	36 months	/
Not Used	1.3.171.1.1.1.11.20	36 months	/

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 performed 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)

LuxTrust SSL Client LCP Certificate Profile			
Attribute	Field	O/M	Value
	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)
	organizationalUnitName⁴	O	As provided by Subscriber
	organizationalUnitName⁴	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:
	subjectPublicKey	M	<ul style="list-style-type: none"> • 3072 bit (RSA) for 12, 24 or 60 months validity • 4096 bit (RSA) for 120 months validity Public exponent: Fermat-4 (=010001).
Extensions			
Authority Properties			
authorityKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of the LuxTrust Enterprise CA public key
authorityInfoAccess			
	AccessMethod		Id-ad-1
	accessLocation	M	<a href="http://y<sup>5</sup>.epca.ocsp.luxtrust.lu/">http://y⁵.epca.ocsp.luxtrust.lu/
	AccessMethod		Id-ad-2
	accessLocation	M	<a href="http://ca.luxtrust.lu/LTEPCA<sup>x2</sup>.crt">http://ca.luxtrust.lu/LTEPCA^{x2}.crt
cRLDistributionPoint			
	distributionPoint		

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
	fullName	M	http://epca.crl.luxtrust.lu/LTEPCA x^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

7.4 Timestamping LCP Certificate Profile

LuxTrust Enterprise CA - Timestamping LCP Certificate Profile			
Attribute	Field	O/M ⁶	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 ⁷
	organizationName	M	LuxTrust S.A.
Validity			
	NotBefore	M	Certificate generation process date/time.
	NotAfter	M	Certificate generation process date/time + 12 years
subject			
	commonName	M	Example: FAIR AND SMART - FAIRANDSMART - TIMESTAMPING
	countryName	M	Nationality of holder (ISO3166)
	organizationName	M	Name of company/institution as in articles of association or equivalent documents, including the legal form.

⁶ O/M: O = Optional, M = Mandatory.

⁷ 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 - Timestamping LCP Certificate Profile			
Attribute	Field	O/M ⁶	Value
	organizationalIdentifier	M	<p>Shall contain information using the following structure in the presented order:</p> <ul style="list-style-type: none"> - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference). <p>The three initial characters shall have one of the following defined values:</p> <ol style="list-style-type: none"> 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. <p>The country code is either the country code where the subject is registered as legal entity when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.</p>
subjectPublicKeyInfo			
	algorithm	M	<p>RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.”</p> <p>ECC - 1.2.840.10045.2.1 ECDSA_P384 - ansip384r1 - 1.3.132.0.34</p>
	subjectPublicKey	M	
Extensions			
Authority Properties			
authorityKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of the LuxTrust Enterprise CA public key
authorityInfoAccess			
	AccessMethod		Id-ad-2

LuxTrust Enterprise CA - Timestamping LCP Certificate Profile			
Attribute	Field	O/M ⁶	Value
	accessLocation	M	http://ca.luxtrust.lu/LTEPCA ² .crt
	AccessMethod		Id-ad-1
	accessLocation	M	http://y ⁸ .epca.ocsp.luxtrust.lu/
cRLDistributionPoint			
	distributionPoint		
	fullName	M	http://epca.crl.luxtrust.lu/LTEPCA ² -y ³ .crl
Subject Properties			
subjectKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of Subject public key – Use of 160 bits
Policy Properties			
keyUsage			
	digitalSignature	M	True
	contentCommitment/nonRepudiation	M	False
certificatePolicies			
	PolicyIdentifier	M	1.3.171.1.1.1.11. 22
	policyQualifierID		Id-qt-1 (CPS)
	qualifier	M	https://repository.luxtrust.com
	policyQualifierID		Id-qt-2 (User Notice)
	PolicyIdentifier	M	0.4.0.2042.1.3
extendedKeyUsage			
	TimeStamping	M	True
BasicConstraints			
	CA	M	False
	pathLenConstraint	M	None

⁸ Y corresponds to the last digit for the LuxTrust OID

7.5 Signing Server eSeal LCP Certificate Profile

LuxTrust Enterprise CA - Signing Server eSeal LCP Certificate Profile			
Attribute	Field	O/M ⁹	Value
Base Profile			
Version			
		M	Version 3 Value = "2"
SerialNumber			
		M	Validated on duplicates - Random CSN
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 ¹⁰
	organizationName	M	LuxTrust S.A.
Validity			
	NotBefore	M	Certificate generation process date/time.
	NotAfter	M	Certificate generation process date/time + 5 years
subject			
	serialNumber	M	<i>Serial Number as constructed by LRAO</i>
	commonName	M	<i>Shall contain the full registered name of the subject (legal person).</i>
	countryName	M	<i>the country in which the subject (legal person) is established (ISO3166)</i>
	organizationName	M	<i>Shall contain the full registered name of the subject (legal person).</i>

⁹ O/M: O = Optional, M = Mandatory.

¹⁰ 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 eSeal LCP Certificate Profile			
Attribute	Field	O/M ⁹	Value
	organizationIdentifier	M	<p>Shall contain information using the following structure in the presented order:</p> <ul style="list-style-type: none"> - 3 character legal person identity type reference; - 2 character ISO 3166 country code; - hyphen-minus "-" and - identifier (according to country and identity type reference). <p>The three initial characters shall have one of the following defined values:</p> <ol style="list-style-type: none"> 1) "VAT" for identification based on a national value added tax identification number. 2) "NTR" for identification based on an identifier from a national trade register. 3) "LT." for identification based on the value provided by the legal entity or by LuxTrust. The country code is either the country code where the subject is registered as legal entity when the identifier is provided by the legal entity or LU when the identifier is provided by LuxTrust.
	organizationalUnitName⁴	O	OPTIONAL - Company/institution department or other information item
	organizationalUnitName⁴	O	OPTIONAL - Company/institution department or other information item
subjectPublicKeyInfo			
	algorithm	M	RSA - 1.2.840.113549.1.1.1 3072 bit up to 4096 bit Based on ETSI TS 119 312, the public exponent e shall be an odd positive integer such that $2^{16} < e < 2^{256}$.
	subjectPublicKey	M	ECC - 1.2.840.10045.2.1 ECDSA_P256 - 1.2.840.10045.3.1.7 ECDSA_P384 - ansip384r1 - 1.3.132.0.34
Extensions			
Authority Properties			
authorityKeyIdentifier			

LuxTrust Enterprise CA - Signing Server eSeal LCP Certificate Profile			
Attribute	Field	O/M ⁹	Value
	keyIdentifier	M	SHA-1 Hash of the issuing CA public key – Use of 160 bits
authorityInfoAccess			
	AccessMethod		Id-ad-2
	accessLocation	M	http://ca.luxtrust.lu/LTEPCAx ² .crt
	AccessMethod		Id-ad-1
	accessLocation	M	http://y ¹¹ .epca.ocsp.luxtrust.lu/
cRLDistributionPoint			
	distributionPoint		
	fullName	M	http://epca.crl.luxtrust.lu/LTEPCAx ² -y ³ .crl
Subject Properties			
subjectKeyIdentifier			
	keyIdentifier	M	SHA-1 Hash of Subject public key – Use of 160 bits
Policy Properties			
keyUsage		M	
	digitalSignature		False
	contentCommitment/nonRepudiation		True
certificatePolicies			
	PolicyIdentifier	M	1.3.171.1.1.1.11.23
	policyQualifierID		Id-qt-1 (CPS)
	qualifier	M	https://repository.luxtrust.com
	policyQualifierID		Id-qt-2 (User Notice)
	PolicyIdentifier	M	0.4.0.2042.1.3
BasicConstraints			
	CA		False
	pathLenConstraint		None

¹¹ Y corresponds to the last digit for the LuxTrust OID

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.