LUXTRUST
Enabling a digital world

LuxTrust Qualified SelfSigned CA Certificate Profiles

Version number: 1.00
Publication Date: 26.01.2024
Effective Date: 09.02.2024

ILNAS

PRESTATAIRE DE SERVICES DE CONFIANCE QUALIFIÉ

SUPERVISION N°2018/8/001

Règlement européen n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance

Copyright © 2024 – 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 title:	LuxTrust Qualified Timestamping CAs Certificate Specifications
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Technical Specification
Document Distribution List	Any
Document Classification	Public
Document Owner	CSP Board

Version	Who	Date	Reason of modification
1.0	YNU	27/11/2023	Initial Version

Contents

Introduction

1. The LuxTrust project

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

Established in November 2005 through a partnership between the Luxembourg government and the major private financial actors in Luxembourg, LUXTRUST S.A. was created to become a Trust Service Provider (“TSP”) as defined in the Luxembourg Law of 17/07/2020 on electronic commerce as amended itself derived from the European Regulation N°910/2014. Before mentioned law and regulation set out the legal framework for electronic signatures in the Grand Duchy of Luxembourg as well as for LuxTrust activities as TSP.

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

LuxTrust services are in line with the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS).

2. Goal of the LuxTrust PKI

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

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

LuxTrust will also promote these services towards application service providers in order to facilitate the emergence of e-applications.

3. LuxTrust PKI Hierarchy

LuxTrust S.A., acting as “TSP” as described in the Luxembourg Law of 17/07/2020 on electronic commerce as amended is using several Certification Authorities (CAs).

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

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

LuxTrust Certification Authorities

As described in section 1.3, LuxTrust S.A. acting as TSP is using several Certification Authorities (CAs) to issue LuxTrust Certificates.

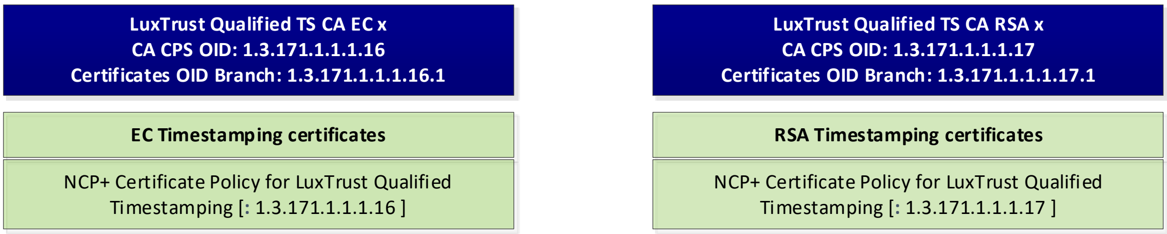
These Certificates are covered by the ILNAS accreditation as registered under the reference N° 2018/8/001 by the national registry of Accredited Certification Service Providers.

1. CA hierarchy

The legal person (organisation) responsible for these CAs is LuxTrust S.A. acting as TSP.

The Qualified LuxTrust PKI consists in a one-level CA hierarchy which is described in this document

- LuxTrust Qualified TimeStamping CA



LuxTrust Qualified TS CA EC x
CA CPS OID: 1.3.171.1.1.1.16
Certificates OID Branch: 1.3.171.1.1.1.16.1

EC Timestamping certificates

NCP+ Certificate Policy for LuxTrust Qualified Timestamping [: 1.3.171.1.1.1.16]

LuxTrust Qualified TS CA RSA x
CA CPS OID: 1.3.171.1.1.1.17
Certificates OID Branch: 1.3.171.1.1.1.17.1

RSA Timestamping certificates

NCP+ Certificate Policy for LuxTrust Qualified Timestamping [: 1.3.171.1.1.1.17]

Figure 1 - LuxTrust Qualified TS CA SelfSigned Hierarchy

or a two-level CA hierarchy which is covered by the document “LuxTrust Global Root CA - Certificate Profiles”

Note 1: Unless explicitly otherwise indicated, “the CA”, refers to the LuxTrust CAs granted to issue Certificates under responsibility of LuxTrust S.A. acting as TSP. “The CA” is thus legally designating LuxTrust S.A. acting as TSP.

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

CERTIFICATE AND CRL PROFILES

1. Certificate types

The following table indicates and shortly describes the various types of certificates that are to be issued by LuxTrust under the two LuxTrust Qualified Timestamping CAs:

CP identification	CP OID	CPS OID	Short Description
LuxTrust Qualified TimeStamping Certification Authority			
Timestamping Certificate Profile **EC**	1.3.171.1.1.1.16.1	1.3.171.1.1.1.16	ETSI EN 319 421 compliant Certificate on HSM with creation of the keys by the TSP, **EC**: ecdsa-with-SHA512 , twelve (12) years validity with two (2) years Private Key Usage.
Timestamping Certificate Profile **RSA**	1.3.171.1.1.1.17.1	1.3.171.1.1.1.17	ETSI EN 319 421 compliant Certificate on HSM with creation of the keys by the TSP, **RSA**: rsassaPss SHA512, twelve (12) years validity with two (2) years Private Key Usage.

Subscriber’s Agreement (Purchase Orders and General Terms and Conditions) is made available to customers by LuxTrust S.A. acting as TSP.

In addition to these “external” certificate types, “Internal Certificate Policies” are exclusively reserved by LuxTrust S.A. acting as TSP for issuance of security credentials (and certificates) within the management and operation domains of the LuxTrust PKI. This encompasses but is not limited to PKI component services provider’s entities (e.g., RA, SRA, TSAs, devices, components, etc.), specific officers considered as security officers, etc.

Within the present document, Certificates issued by LuxTrust S.A. acting as TSP are collectively called the “Certificates” regardless of their type, unless they are more clearly and specifically identified.

In addition to the above described certifications services, the LuxTrust TSP activities include the LuxTrust Time Stamping Services (TSS). These services consist of the management of the infrastructure, and the provisioning of Time Stamp Tokens according to the LuxTrust Time Stamping Policy.

These services are provided by LuxTrust S.A. acting as LuxTrust Trusted Time Stamping Services Provider (TTSSP) to the Subscribers and are an integral part of the LuxTrust PKI. Hereafter the term TSP includes the activities and provision of trusted time stamping services as expressed in the (eIDAS) regulation). LuxTrust Trusted Time Stamping services are covered within the LuxTrust Trusted Time Stamping V2 policy.

The LuxTrust CSP Board acts as Policy Approval Authority for LuxTrust S.A. In particular the CSP board manages the LuxTrust Certification Practice Statement (CPS) and all related CPs, covering the statements of the practices followed by LuxTrust S.A. acting as TSP in issuing CA and end-entities certificates as well as in issuing TSTs through its TSAs.

By means of the CPS and related CPs, LuxTrust S.A. acting as TSP indicates and guarantees that it complies with regulatory and standard texts applicable, and whether or not this guarantee is supported by an accreditation as well as the name and coordinates of the accreditation body

2. Certification Authorities – Certificates profiles

LuxTrust certificates are X.509 v3, compliant with RFC 5280.

LuxTrust CAs certificate profiles description is available as follows:

2.1 LuxTrust Qualified TimeStamping CA-RSA

Field	**Field OID**	-	**LuxTrust Qualified Timestamping CA RSA**
		Version	
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA RSA
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976988
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	20Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA RSA
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976988
		PublicKey	RSA - 1.2.840.113549.1.1.1 4096 bits public exponent: Fermat-4 (=010001).
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.17
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

2.2 LuxTrust Qualified TimeStamping CA-EC

Field	**Field OID**	-	**LuxTrust Qualified Timestamping CA EC**
		Version	
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	ecdsa-with-SHA512
		SignatureValue	
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA EC
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976987
Validity			
	n/a	NotBefore	Certificate Generation Process Date/Time
	n/a	NotAfter = NotBefore + x	25Y
Subject			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA EC
	2.5.4.10	organizationName	LuxTrust S.A
	2.5.4.97	organizationIdentifier	VATLU-20976987
		PublicKey	ECC - 1.2.840.10045.2.1 ECDSA_P521 - 1.3.132.0.35
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	keyCertSign	TRUE
	n/a	crlSign	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	1.3.171.1.1.1.16
	1.3.6.1.5.5.7.2.1	Qualifier-1	https://repository.luxtrust.com
BasicConstraints	2.5.29.19		
	n/a	CA	TRUE
	n/a	pathLenConstraint	0

Text in Red : Critical extension

3. End Entity – Certificates profiles

3.1 NCP+ Certificate Policy for LT Qualified Timestamping

LuxTrust Timestamping Certificates are issues by the LuxTrust Qualified Timestamping CA with keys located on HSM devices, with generation by LuxTrust TSP according to the processes and procedures described in the applicable CP.

The profiles of the public key certificates used by the LuxTrust QTS CA comply with the RFC 3161 and RFC5816.

This profile aims at issuing qualified electronic time-stamps as per Regulation (EU) No 910/2014. It is compliant with ETSI EN 319 421-Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and ETSI EN 319 422-Time-stamping protocol and time-stamp token profiles. This profile complies with the requirements of the standard ETSI EN 319 411-1 describing the Requirements for trust service providers issuing Extended Normalized Certificate Policy.

			LuxTrust Qualified Timestamping CA **EC: 1.3.171.1.1.1.16 & RSA: 1.3.171.1.1.1.17**
Field	Field OID		Timestamping
		Version	Version 3 Value = “2”
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 || RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha529
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20977002
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	12Y
Subject			
	2.5.4.3	commonName	LuxTrust Qualified Timestamping
	2.5.4.6	countryName	LU
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
		PublicKey	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.”
	2.5.29.16	privateKeyUsagePeriod	24M
Authority			
	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
AIA	1.3.6.1.5.5.7.1.1		
	1.3.6.1.5.5.7.48.1	aia-ocsp-url	http://qtsca.ocsp.luxtrust.lu
	1.3.6.1.5.5.7.48.2	aia-ca-issuer	http://qtsca.luxtrust.lu/LTQTSCA-XX.crt

cRLDistributionPoints	2.5.29.31		
		cdp-url	http://qtsca.crl.luxtrust.lu/LTQTSCA-XX-1.crl
subjectAltName	2.5.29.17		
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.8	TimeStamping	TRUE
certificatePolicies	2.5.29.32		
	n/a	PolicyIdentifier-1	EC : 1.3.171.1.1.1.16.1 RSA : 1.3.171.1.1.1.17.1
	1.3.6.1.5.5.7.2.1	CPS Pointer Qualifier-1	https://repository.luxtrust.com
	n/a	PolicyIdentifier-2	0.4.0.2042.1.2
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE
	n/a	pathLenConstraint	n/a

Text in Red : Critical extension

4. LuxTrust CRL / OCSP – Certificates profiles

4.1 CRL profile

In conformance with the IETF PKIX RFC 2459, the LuxTrust CAs support CRLs compliant with:

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

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

			LuxTrust Qualified Timestamping CA **EC: 1.3.171.1.1.1.16 & RSA: 1.3.171.1.1.1.17**	
Field	OID		Non Public	Public - By OID
	n/a	Version	Version 2 Value = "1"	
	n/a	SignatureAlgorithm	EC: ecdsa-with-SHA512 || RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512	
	n/a	SignatureValue	Issuing CA Signature	
Issuer				
	2.5.4.6	countryName	LU	
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX	
	2.5.4.10	organizationName	LuxTrust S.A.	
	2.5.4.97	organizationIdentifier	VATLU-20976985	
Validity				
	n/a	Last Update - UTC Time	Certificate generation process date/time. - UTC Time	
	n/a	NextUpdate = LastUpdate + x - UTC Time	24 hours = 6 hours (Update Interval) + 18 hours (Margin)	4 hours 30 minutes = 1 hour (Update Interval) + 3 hours 30 minutes (Margin)

CRL Extensions				
	2.5.29.28	Issuing Distribution Point	n/a	http://crl.luxtrust.lu/LTGTSCA-XX-Y.crl
	2.5.29.20	CRL Number	Non-critical CRL unique sequence number	
	2.5.29.60	expiredCertsOnCRL	Non-critical <CA issuance date>	n/a
	2.5.29.35	Authority Key Identifier	Non-critical <subject key identifier of the CA >	
revokedCertificates				
	n/a	Serial Number	<certificate serial number>	
	n/a	Revocation Date - UTC Time	<revocation date and time>	
	2.5.29.21	CRL Entry Extension - CRL Reason Code	<revocation reason>	

Legend

XX	RSA or EC
Y	Last digit of EE CP OID
n/a	Not Applicable
<Field>	Critical Extension

4.2 OCSP profile

The OCSP profile follows IETF PKIX RFC 6960 OCSP v1 and v2. The LuxTrust CAs support signed status requests, and multiple Certificates status requests in one OCSP request as long as they are signed by the same CA.

The following table provides the description of the fields for LuxTrust OCSP profile.

			LuxTrust Qualified Timestamping CA **EC: 1.3.171.1.1.1.16 & RSA: 1.3.171.1.1.1.17**
Field	Field OID		
		Version	Version 3 Value = “2”
		CertificateSerialNumber	Random CSN - Validated on duplicates - Entropy
		SignatureAlgorithm	EC: ecdsa-with-SHA512 || RSA: rsassaPss with Hash Algorithm: sha512 and mask Algorithm: mgf1 with sha512
		SignatureValue	Issuing CA Signature
Issuer			
	2.5.4.6	countryName	LU
	2.5.4.3	commonName	LuxTrust Qualified Timestamping CA XX
	2.5.4.10	organizationName	LuxTrust S.A.
	2.5.4.97	organizationIdentifier	VATLU-20976985
Validity			
	n/a	NotBefore	Certificate generation process date/time.
	n/a	NotAfter = NotBefore + x	3M
Subject			
	2.5.4.3	commonName	LuxTrust S.A. OCSP Server
	2.5.4.6	countryName	LU
	2.5.4.10	organizationName	LuxTrust S.A.
		PublicKey	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.”
Authority			

	2.5.29.35	AuthorityKeyIdentifier	SHA-1 Hash of the issuing CA public key
subjectAltName	2.5.29.17		
	2.5.29.14	subjectKeyIdentifier	SHA-1 Hash of Subject public key – Use of 160 bits
keyUsage	2.5.29.15		
	n/a	digitalSignature	TRUE
	n/a	contentCommitment FKA nonRepudiation	FALSE
extendedKeyUsage	1.3.6.1.5.5.7.3		
	1.3.6.1.5.5.7.3.9	OCSPSigning	TRUE
BasicConstraints	2.5.29.19		
	n/a	CA	FALSE