LuxTrust Time Stamping V2 Policy

Version number: 1.14

Publication Date: 26/01/2024

Effective Date: 09/02/2024

Document O.I.D: 1.3.171.1.1.1.10.8

Document Information

Document title:	LuxTrust Time Stamping V2 Policy
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Certificate Policy
Document Distribution List	Relying parties, Other CSP
Document Classification	Public
Document Owner	CSP Board

Version History

Version	Who	Date	Reason of modification
1.0	CSP	20/08/2009	Initial version
1.1	CSP	03/09/2009	Specify Hash function supported
1.2	CSP	28/10/2009	inserted ILNAS logo including accreditation reference and technical standards reference
1.3	CSP	15/12/2010	minor corrections
1.4	CSP	01/07/2011	Adaptation for new certificate validity
1.5	CSP	20/09/2012	Added: LuxTrust Global Timestamping certificate
1.6	YNU	25/03/2014	Typo error on URL
1.7	YNU	18/08/2016	Add reference to EN 319 421 for qualified timestamping Update the provider of this service Update reference to the Timestamping and Qualified Timestamping Certificate Profile Add reference to EU Regulation 910/2014 Update role of ILNAS : supervisory body instead accreditation body
1.8	YNU	17/03/2017	Clarify incident and log recording
1.9	DEL	12/06/2017	Minor corrections
1.10	DEL	15/12/2017	Update hash functions in accordance with normative requirements
1.11	DEL	16/05/2018	Include ETSI EN 319421: requirements in the context of TSA Termination Add decription related to the management of leap seconds, time-stamp drifts or jumps out of synchronization with UTC
1.12	DEL	21/09/2019	Update 5 to 12 years
1.13	YNU/VMI	28/10/2021	Typo update Removal of reference Add: Signature algorithm used in Time Stamp Token
1.14	YNU/VMI	10/11/2023	Update: Best practices Time-Stamp Policy (BTSP) policy identifier Add reference to LT QTS CA : • 1.3.171.1.1.1.16.1.1 • 1.3.171.1.1.1.17.1.1

Table of content

Intellectual Property Rights

Foreword

The present Time Stamping Policy (TSP) is based on and thus compatible with the Standard EN 319 421 "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"

For the interpretation of the present Time Stamping Policy, the following guidelines apply:

1) The international standardisation process influences the titles and subtitles of this Time Stamping Policy. In interpreting this Time Stamping Policy, the text under each title is given precedence over the wordings in the titles.

2) Reference of Time Stamping Policy locations has to be done in the following manner: First the Time Stamping Policy name has to be provided followed by the heading numbering and the section/subsection numbering. For instance: LuxTrust Time Stamping Authority Policy v1.1, section 1.3.2/c3.

3) As a general rule LuxTrust S.A. acting as Time Stamping Service Provider (TSSP), and in accordance with this Time Stamping Policy, shall undertake adequate measures to fulfil all requirements in this Time Stamping Policy. When a section is marked with "Not applicable", it means that this section is not applicable to the present Time Stamping Policy of the LuxTrust Time Stamping Services.

References

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 (eIDAS).

[2] 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.

[3] ETSI TS 101 733 – Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[4] ETSI TS 101 903 – Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR).

[6] IETF RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) – August 2001.

[7] ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles.

[8] LuxTrust Global Qualified Certification Practice Statement and LuxTrust Qualified TS CA Certification Practice Statement latest version in force available on LuxTrust site

[9] LuxTrust Global Root CA - Certificate Profiles and LuxTrust Qualified SelfSigned CA Certificate Profiles latest version in force available on LuxTrust site.

[10] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.

[11] Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique.

[12] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.

[13] Règlement Grand-Ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».

[14] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[15] IETF RFC 5280 – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

[16] EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[17] IETF RFC 5816 – ESSCertIDv2 Update for RFC 3161.

1 Introduction

The LuxTrust Time Stamping Services support assertions of proofs that an electronic record existed before a particular time. These services can be used in support to non-repudiation services, to prove that an electronic signature was generated during the validity period of a public key certificate, to support electronic long term archiving, etc.

The LuxTrust Time Stamping services are provided according to the IETF RFC 5816 [17], RFC 3161 [6], EN 319 421 [16] and EN 319 422 [7] standards, to the LuxTrust Time Stamping Practice Statement[1] and under the authority of LuxTrust S.A. acting as Time Stamping Services Provider. Time Stamp tokens are signed by a LuxTrust S.A. certified key.

The present document describes the policy to which the LuxTrust Time Stamping Authority (TSA) adheres, in order to confirm to Subscribers and Relying Parties of the correct operation and management of the respective services, as per international state-of-the-art standards.

The current Time Stamping Policy specifies general rules used by the LuxTrust Time Stamping Authority (TSA) for the issuance of Time Stamp Tokens (TST). It defines the parties involved, their responsibilities, rights and the applicability range. These specific practices described in this present Time Stamping Policy are ruled and operated under the more general practices as described in the LuxTrust Certification Practice Statement (hereafter referred to as the "LuxTrust CPS" [8], respectively [9]).

The present Time Stamping Policy addresses the services provided by the LuxTrust Time Stamping Authority that can be reached via

- OID 1.3.171.1.1.10.3.18.1 : https://tts.luxtrust.lu/qTTS/Timestamp
- OID 1.3.171.1.1.1.16.1.1 & 1.3.171.1.1.1.17.1.1 : https://tts.luxtrust.com/Timestamp.

Time Stamp Tokens issued in accordance with present Time Stamping Policy may be used to provide long-term proof of authenticity for any electronic data, amongst others long-term electronic signatures [3] [4], medical documents, legal records, executable code and electronic transactions.

The Time Stamping Authority does no long-term archiving of any timestamp token and the application using the TSA must save the issued token for a future usage.

The LuxTrust Time Stamping Services are certified against ETSI EN 319 421 and eIDAS regulation [1] and supervised by ILNAS acting as supervision entity.
Additional information and support can be received from infotts@luxtrust.lu.

LuxTrust conforms to the following technical standards:

- ETSI EN 319 411-1
- ETSI EN 319 421
- ETSI EN 319 422

The national registry of Supervised Certification Service Providers is publicly available on the ILNAS website http://www.ilnas.lu.

2 Definitions and Abbreviations

2.1 Definitions

Name	Description
LuxTrust S.A. or LuxTrust	LuxTrust S.A., with registered offices in IVY Building, 13-15, Parc d'activités, L-8308 Capellen
LuxTrust PKI	The LuxTrust Public Key Infrastructure that is deployed by LuxTrust S.A. to provide the LuxTrust Certification Services.

[1] The LuxTrust Time Stamping Practice Statement is made of the combination of the present LuxTrust Time Stamping Policy and of the LuxTrust CPS [8] respectively [9] for the Timestamping, in which practice statements include statements related to the management of the Time Stamping services as part of the LuxTrust PKI.

Name	Description
LuxTrust CSP Board	The Policy Approval Authority within LuxTrust S.A. is called the LuxTrust CSP Board. It is the high level management body with final authority and responsibility for: – Specifying and approving the LuxTrust infrastructure and practices. – Approving the LuxTrust Certification Practice Statement(s) and LuxTrust Certificate and Time Stamping Policies. – Defining the review process for practices and policies including responsibilities for maintaining the Certification / TSA Practice Statements and Certificate / Time Stamping Policies. – Defining the review process that ensures that the LuxTrust CAs and TSAs properly implements the above practices. – Defining the review process that ensures that the Certificate / Time Stamping Policies are supported by the LuxTrust Practice Statement(s). – Publication to the Subscribers and Relying Parties of the Certificates / Time Stamping Policies and Certification / Time Stamping Practice Statements and their revisions. – Specifying cross-certification procedures and handling cross-certification requests.
LuxTrust Services	The LuxTrust Certification Authority and Time Stamping services.
Certification Authority Auditor (CAA)	The LuxTrust Internal CA Auditor that audits the operations of the CA related Entities.
Certification Practice Statement (CPS)	A statement of the practices, which a certification authority applies for the issuing of Certificates, or for the provision of other services related to electronic signatures.
Certification Service Provider	Any natural or legal person issuing Certificates or provides other services related to electronic signatures.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5
Relying Party	Recipient of a Time Stamp Token (TST) who relies on that Time Stamp Token.
Subscriber	Entity requiring the services provided by the LuxTrust Time Stamping Authority and which has explicitly or implicitly agreed to its terms and conditions.
Time Stamping Policy (TSP)	Named set of rules that indicates the applicability of a Time Stamp Token to a particular community and/or class of application with common security requirements.
Time Stamp Token (TST)	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time Stamping Authority (TSA)	Authority which issues Time Stamp Tokens.
Time Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single Time Stamp Token signing key active at a time.
TSA Disclosure Statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and Relying Parties, for example to meet regulatory requirements.
TSA Practice Statement	Statement of the practices that a TSA employs in issuing Time Stamp Tokens. As the LuxTrust TSA is an integral part of the LuxTrust PKI infrastructure and is thus governed by the same rules and procedures, the LuxTrust Certification Practice Statement acts as well as the LuxTrust TSA Practice Statement.
TSA System	Composition of IT products and components organised to support the provision of Time Stamping services.

2.2 Abbreviations

Acronym	Definition	Acronym	Definition
AES	Advanced Electronic Signature	PKI	Public Key Infrastructure
ARL	Authority Revocation List	PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
B2B	Business to Business	PKCS	Public Key Certificates Standard

Acronym	Definition	Acronym	Definition
CA	Certification Authority	PSF	Professionnel du Secteur Financier (FSP – Financial Sector Professional)
CAA	Certification Authority Auditor	QES	Qualified Electronic Signature
CME	Cryptographic Module Engineering	QCP	Qualified Certificate Policy
CP	Certificate Policy	RA	Registration Authority
CPS	Certification Practice Statement	RAO	Registration Authority Officer
CRL	Certificate Revocation List	RFC	Request for Comments
CSP	Certification Service Provider	RSA	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
EC	Family of public-key cryptosystems, which is based on the algebraic structures of the elliptic curves over finite fields.	SCD	Signature Creation Device
HSM	Hardware Security Module	SRA	Suspension and Revocation Authority
IETF	Internet Engineering Task Force	SRAO	Suspension and Revocation Authority Officer
ISO	International Organisation for Standardisation	SSCD	Secure Signature Creation Device
ITU	International Telecommunications Union	TSA	Time Stamping Authority
LCP	Lightweight Certificate Policy	TSP	Time Stamping Policy
LDAP	Lightweight Directory Access Protocol	TSS	Time Stamping Service
NCP	Normalised Certificate Policy	TST	Time Stamp Token
NCP+	Normalised Certificate Policy +	TSSP	Time Stamping Service Provider
OID	Object Identifier	TSU	Time Stamping Unit
OCSP	Online Certificate Status Protocol	URL	Uniform Resource Locator
PIN	Personal Identification Number	UTC	Coordinated Universal Time

3 General Concepts

3.1 Time Stamping Services

The Time Stamping Services (TSS) consists of the management of the infrastructure for, and the provisioning of Time Stamp Tokens. These services are provided by the LuxTrust Time Stamping Services Provider (TSSP) to the Subscribers and are an integral part of the LuxTrust PKI and in the context of the broad definition of CSP as given by European Regulation 910/2014.

The TSS assures use of a reliable time source and proper management of all system components.

3.2 Time Stamping Authority

The LuxTrust Time Stamping Authority (TSA) is responsible for provisioning of TSS as described in the previous paragraph. It has the responsibility for the operation of the relevant TSU's that are created and signed on behalf of the TSA. The legal entity responsible for the TSA is LuxTrust S.A., acting as TSSP.

It is this authority that is trusted by the users of the LuxTrust Time Stamping services (i.e. Subscribers as well as Relying Parties) to issue Time Stamp Tokens.

3.3 Subscriber

The Subscriber may be an organisation comprising several end-users or an individual end-user.

When the Subscriber is an organisation, some of the obligations that apply to that organisation will have to apply as well to the end-users. In any case the organisation will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organisation shall duly notify its end-users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

The procedure to become acknowledged as a Subscriber and the pricelist describing the related charging fees can be obtained upon request from infotts@luxtrust.lu.

3.4 Time Stamping Policy and TSA Practice Statement

3.4.1 Purpose

The present Time Stamping Policy is to be used in conjunction with the LuxTrust CPS [8] that forms together with the present policy the LuxTrust TSA Practice Statement.

In general, the present Time Stamping Policy states "what is to be adhered to", while the LuxTrust TSA Practice Statement states "how it is adhered to".

The present document specifies a Time Stamping Policy to meet general requirements for trusted Time Stamping services. The LuxTrust CPS [8] specifies in practice statements how these requirements are met (including personnel management, personnel selection, physical security, etc.) for the operation of the LuxTrust Time Stamping Services.

The present Time Stamping Policy is publicly available. Distribution of this document is restricted as described in the “Intellectual Property Rights” section.

3.4.2 Level of specificity

The present Time Stamping Policy describes only general rules of issuing and managing TST’s. Detailed description of the infrastructure and related operational procedures are described in additional documents that are not made publicly available. These additional documents are only available to authorised LuxTrust personnel and, on a need-to-know basis, to auditors of the TSS.

3.4.3 Approach

The present Time Stamping Policy is defined independently of the specific details of the specific operating environment of the LuxTrust TSA, whereas the LuxTrust CPS [8] is tailored to the organisational structure, operating procedures, facilities, and computing environment of the LuxTrust TSA.

4 Time Stamping Policies

4.1 Overview

The present Time Stamping Policy is a set of rules used during the issuing of TST's and is regulating the security level for the LuxTrust TSA.

TST's are issued with an accuracy of one (1) second.

The profiles of the public key certificates used by the LuxTrust TSA comply with the RFC 5816 [17]. The full set of rules used by LuxTrust S.A. for the issuing and management of these certificates that are issued by a LuxTrust CA, as well as their extensions, are described in the LuxTrust Internal Certificate Policy for PKI Participants other than Subscribers and Relying Parties.

The LuxTrust TSA issues TST's according to ETSI Standard EN 319 422.

The profile of the TSA certificates issued by LuxTrust Global Qualified CA x is defined in "LuxTrust Global Root CA - Certificate Profiles" [9] and 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.

The Signature algorithm used in Time Stamp Token is RSA (PKCS) #1 version 1 with a key size of: 3072 bits.

4.2 Identification

The present Time Stamping Policy covers the following documents OIDs:

Under the LuxTrust Global Qualified CA X[2] : 1.3.171.1.1.10.3.18.1

Identifier	Description
1.3.171.1.1.10.3.18.1	Qualified Production TSTs under the LuxTrust Global Qualified CAx with validity as described in 6.1.2 and an accuracy as defined in 4.1.

Under the LuxTrust QTS CA X[2] :

- RSA 1.3.171.1.1.1.16.
- EC 1.3.171.1.1.1.17.

Identifier	Description
1.3.171.1.1.1.16.1.1 1.3.171.1.1.1.17.1.1	Qualified Production TSTs under the LuxTrust Qualified TS CAx with validity as described in 6.1.2 and an accuracy as defined in 4.1.

4.3 User Community and applicability

The present Time Stamping Policy does not define any limitations on users' eligibility or applicability of the services delivered. The LuxTrust TSA can provide Time Stamping services for Time Stamping of any electronic data to any user, including closed communities.

[2] X is a sequential value to distinguish the old CA from the renewed CA and greater than or equal to 3 for this OID.

4.4 Conformance

The LuxTrust TSA uses the identifier of the present Time Stamping Policy in TST's as given in section "Identification".

The LuxTrust TSA ensures compliance of provided services with regulations specified in section 5.1 "TSA obligations" and ensures reliability of control mechanisms described in section 6 "Requirements on TSA practices".

5 Obligations and liability

5.1 TSA obligations

5.1.1 General

This chapter includes, directly or by reference, all the obligations, liabilities, guarantees and responsibilities of the LuxTrust TSA, its Subscribers and TST users (Subscribers and Relying Parties). These obligations and responsibilities are regulated by mutual agreements signed between the parties.

LuxTrust agreements with Subscribers and Relying Parties describe mutual obligations and responsibilities, including financial responsibilities.

The present Time Stamping Policy and the LuxTrust CPS [8] are integral parts of the agreements signed between LuxTrust S.A. and the Subscribers and Relying Parties.

LuxTrust S.A. guarantees that all the requirements of the LuxTrust TSA, including procedures and practices related to the issuance of TST's, review of system and security audit are in accordance with regulations described in section 6 "Requirements on TSA practices" of the present TSP.

The LuxTrust TSA acts in accordance with the above procedures. No exclusions of these regulations are allowed. Additional obligations of the TSA, Subscribers and Relying Parties are described in the LuxTrust CPS [8].

5.1.2 TSA obligations towards Subscribers

LuxTrust S.A. guarantees an availability of 99.6 % of the LuxTrust TSA services in a 24/7 mode excluding scheduled technical breaks, concerning equipment and system conservation.

Moreover LuxTrust S.A. guarantees that:

- Its commercial activity is provided on the basis of reliable equipment and software.
- The activities and services provided are legally compliant; in particular they do not violate intellectual property, license and other related rights.
- Services delivered are conformant to generally accepted norms.
- Issued TST's do not contain any false data or mistakes.
- It will deliver, upon Subscriber's request, all elements that permit attestation of the reliability of date and time contained in the TST's.
- That it will maintain a competent and experienced team that can ensure the continuity of the TSS.
- It will ensure on a permanent basis the physical and logical security, as well as the integrity of materials, software and databases required for the correct functioning of the TSS, as described in the LuxTrust CPS [8].
- It will monitor and control the TSS (e.g. Intrusion Detection) and the whole TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the TSS resulting from deliberate attacks, as described in the present Time Stamping Policy and the LuxTrust CPS [8].
- It will take all measures required according to generally accepted norms to secure its services, in order to prevent outages of the TSS.
- It will make available a back-up infrastructure that can be used in case of service interruption of the main infrastructure.

5.2 Subscriber obligations

Subscribers retrieving TST's, should verify the electronic signatures posed by the LuxTrust TSA on the TST's.

Such verification comprises:

- Verification whether the signature on the TST is valid.

- Verification of the TSA certificate:
  - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself),
  - Verification whether the certificate is not expired at the moment of signature,
  - Verification whether the certificate was not revoked or suspended at the moment of signature. This verification will preferentially be done by OCSP request via the link referenced in the AIA of the timestamp certificate or alternatively by CRL lookup with appropriate software accessing the LuxTrust Certificate Public Registry or any other validation method proposed by LuxTrust.

Additional Subscriber obligations are described in the LuxTrust CPS [8].

5.3 Relying Party obligations

Parties relying on TST's should verify the electronic signatures created by the LuxTrust TSA on the TST's.

Such verification comprises:

- Verification whether the signature on the TST is valid.
- Verification of the TSA certificate:
  - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself),
  - Verification whether the certificate is not expired at the moment of signature,
  - Verification whether the certificate was not revoked or suspended at the moment of signature. This verification will preferentially be done by OCSP request via the link referenced in the AIA of the timestamp certificate or alternatively by CRL lookup with appropriate software accessing the LuxTrust Certificate Public Registry or any other validation method proposed by LuxTrust.

The Relying Party should only rely on a TST where the TSA certificate has expired, when a non-repudiable proof exists (e.g. another TST, or notary record) that guarantees that the TST did exist before expiry of the certificate and has not been changed since. This is specifically of importance when the cryptographic functions or TSA certificate key length of the TST are not considered secure anymore at the time the party intends to rely on the TST.

The present Time Stamping Policy does not specify any limits or limitation related to the usage of TST's.

Additional Relying Party obligations are described in the LuxTrust CPS [8].

5.4 Liability

The liability of LuxTrust S.A. acting as TSSP and Relying Parties connected with the services is specified in mutual agreement or is as foreseen in the applicable legislation.

Without prejudice to the above limitations, LuxTrust S.A. acting as TSSP is held liable for direct damages resulting from:

- Non-respect of requirements specified in the present Time Stamping Policy,
- Any breach of confidentiality obligation with regards of personal data sent by Subscribers,
- Damages to Subscribers or Relying Parties in case of non-execution of contractual terms,
- Damages caused by its personnel in the context of the provisioning of services as described in the contract,
- Damages to partners / Subscribers as a result of dysfunction of devices used by LuxTrust TSA,
- Lack of precision and/or integrity of data that it delivers or manages.

The other liabilities and regulation of the provision of TSA services are described in LuxTrust CPS [8].

LuxTrust TSA declines any responsibility with regard to the usage that is made with the TSTs it delivers and signs.

6 Requirements on TSA practices

LuxTrust TSA shall implement controls that meet ETSI EN 319 421 and ETSI EN 319 422 requirements.

6.1 Practice and Disclosure Statements

6.1.1 TSA Practice Statement

- Risk Assessment: The provision of LuxTrust TSA services is placed in the more general context of the provision of Trust (Certification) Services as ruled by the LuxTrust CPS [8]. A risk assessment is regularly carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures that have been taken.
- Procedures, control mechanisms and technical infrastructure described in section 6 of the present document are the basis of the LuxTrust TSA functioning. Other controls are described in the LuxTrust CPS [8]. LuxTrust ensures that TSA event logs are retained for at least 10 (ten) years after these events have occurred.
- The LuxTrust TSA Practice Statement is currently the collection of the Time Stamping Policies and the LuxTrust CPS [8]. These documents are available to the public and published on the LuxTrust website https://repository.luxtrust.com. Together with associated internal confidential documents, they rule the LuxTrust TSA services operation.
- The terms and conditions regarding the use of the LuxTrust TSA services are disclosed and made available to all Subscribers and Relying Parties as specified in section 6.1.2 of the present document.
- Final authority and management of the LuxTrust TSA services and its practices are ensured by LuxTrust S.A. acting as TSSP, through the LuxTrust CSP Board. The CSP Board of LuxTrust S.A. shall ensure that the practices are properly implemented under the final responsibility of the LuxTrust senior management. The CSP Board is in charge of defining the review process for the practices, including the responsibilities for maintaining the TSA practices statement.
- The LuxTrust TSA will give due notice of changes it intends to make in the LuxTrust TSA Practice Statement. Any such changes will be subject to revision and approval by the CSP Board. The LuxTrust TSA shall make the revised version immediately available as described in the LuxTrust CPS [8].

6.1.2 TSA Disclosure Statement

LuxTrust TSA disclose to all Subscribers and potential Relying Parties the terms and conditions regarding the use of its Time Stamping services. TSA disclosure statement from LuxTrust TSA is compliant with requirements from ETSI EN 319 421 [16], based on the ETSI BTSP best practices policy for Time-Stamp referenced with OID 0.4.0.2023.1.1, and is included in Subscriber / Relying Party contractual agreement.

LuxTrust TSA contact information is

LuxTrust contact information	
Contact Person:	CSP Board Contact
Postal Address:	LuxTrust S.A. Time Stamping Authority c/o CSP Board Member IVY Building 13-15, Parc d'activités L-8308 Capellen
Telephone number:	+352 26 68 15 - 1
Fax number:	+352 26 68 15 - 789
E-mail address:	*cspboard@luxtrust.lu*
Website:	https://www.luxtrust.com

Every TST issued by LuxTrust TSA includes the policy identifier, defined in section 4.2 of the present document.
Cryptographic hash functions, used in the timestamping process are in accordance with normative requirements, SHA-256 and SHA-512. The customer specifies the chosen hash function in the timestamp request (TSQ).

Expected validity period of TST and of the signature used to sign the TST is twelve (12) years. Accuracy of the time, which is provided in a TST, is regulated in section 4.1 of the present document. Applicability limitations related with TSA system have been defined in section 4.3 of this policy. Subscriber obligations are described in section 5.2 of the present policy. TST verification should be performed with the usage of appropriate software.

Liabilities are defined in section 5.4 of the present document.

Complaints, suggestions and remarks on LuxTrust TSA services should be addressed to the LuxTrust helpdesk using the e-mail: infotts@luxtrust.lu.

Provision of LuxTrust TSA services are ruled by the Grand-Duchy of Luxembourg Laws.

6.2 Key management life cycle

6.2.1 TSA key generation

LuxTrust TSA ensures that any TSA cryptographic keys are generated under controlled circumstances and in accordance with general key pair generation and installation practices related to PKI Participants other than Subscribers and Relying Parties as described in the LuxTrust CPS [8].

LuxTrust TSA keys are generated within a Hardware Security Module (HSM) complying with LuxTrust HSM rules as stated in the LuxTrust CPS [8] in a physically secured environment, by personnel in trusted role in accordance with the LuxTrust CPS [8]. TSA key generation algorithm is described in section 4.1 of the present document.

6.2.2 TSU private key protection

LuxTrust TSA ensures that TSU private keys are and remain confidential and maintain their integrity. LuxTrust TSA keys are generated, held and used within Hardware Security Module (HSM) complying with LuxTrust HSM rules as stated in the LuxTrust CPS [8], in a physically secured environment, by personnel in trusted role in accordance with the LuxTrust CPS [8].

The procedures and circumstances for TSA key back-up and key recovery in case of a disaster, failure of the system or system conservation are in accordance with the LuxTrust CPS [8].

6.2.3 TSU public key Distribution

LuxTrust TSA ensures that the integrity and the authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution towards Relying Parties. LuxTrust TSA certificates are published in the LuxTrust Certificate Public Registry and are available on the LuxTrust website https://www.luxtrust.com in the Public Certificate Registry section.

LuxTrust TSU certificates are issued by LuxTrust Global Qualified CAx in accordance with the LuxTrust CPS [8] (and Internal CP for certificates issued to PKI Participants other than Subscribers or Relying Parties).

6.2.4 Rekeying TSU Keys

The lifetime of the LuxTrust TSU certificates is no longer than the period of time that the chosen algorithm and key length are recognised as being fit for the purpose.

LuxTrust TST's are signed with LuxTrust TSA/TSU certificates of twelve (12) years (10 years + 2 years) validity; the expected validity period of such TST's is ten (10) years (actual validity period will be between 10 and 12 years). LuxTrust TSA/TSU certificates of twelve (12) years (10 years + 2 years) validity are only used to sign TST's during a usage period of two (2) years.

LuxTrust TSA/TSU rekey procedure is executed upon expiry of the usage period (2 years) of the TSA/TSU certificate in accordance with the LuxTrust CPS [8]. Public keys are archived for a period of at least ten (10) years from the expiration date of the certificate. Private Key protection is in accordance with the LuxTrust CPS [8].

6.2.5 End of TSU key life cycle

LuxTrust TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when a TSU's key usage period expires, and that TSU private keys or any part, including any copies are destroyed such that the private key cannot be retrieved as in accordance with the LuxTrust CPS [8]. TST generation system shall reject any attempt to issue a TST if the signing private key is expired or if the signing private key usage period is expired.

6.2.6 Life cycle management of cryptographic module used to sign time-stamps

LuxTrust TSA ensures the security of the HSM throughout its lifecycle. Procedure and controls are in place in accordance with the LuxTrust CPS [8] to ensure:

- that TST signing cryptographic hardware (HSM) is not tampered with during shipment, while stored or deployed,
- that installation, activation and duplication of TSU's signing keys in HSM's is done only by personnel in trusted roles, in a physically secure environment,
- that TST HSM's are functioning correctly, and
- that TSU private signing keys stored on TSU HSM's are erased upon device retirement.

6.3 Time Stamping

6.3.1 Time Stamp Token

LuxTrust TSA ensures that TST are issued securely and include the correct time.

Every TST issued by LuxTrust TSA includes a unique identifier of the policy as described in section 5.2 of the present document. TST's issued by LuxTrust TSA include date and time value traceable to the real UTC time value. Accuracy of the time is defined in section 4.1 of the present document. Signature algorithm used in Time Stamp Token is defined in section 4.1 of the present document.

Each TST has a unique identifier and is signed using a key generated exclusively for this purpose. The time stamp token format is described in "LuxTrust Global Root CA - Certificate Profiles" [9].

6.3.2 Clock Synchronisation with UTC

The LuxTrust TSA ensures that its clock is synchronised with UTC within the declared accuracy. For this purpose, LuxTrust uses two distinct time sources.

LuxTrust TSA incorporates the time in the TST with the accuracy described in section 4.1 of this policy.

LuxTrust TSA ensures that if the time that would be indicated in a TST drifts or jumps out of synchronisation with UTC, this will be detected.

When the TSU clock drifts outside 500 ms, LuxTrust TSA stops issuing time-stamps until the correct time is restored.

LuxTrust implements security controls preventing unauthorised operation, aimed at calibration of the clock out of order, any manipulation or physical damage to the clock.

6.3.3 Leap Second handling procedure

A leap second is a one-second adjustment that is occasionally applied to Coordinated Universal Time (UTC) in order to keep its time of day close to the mean solar time.

Since leap seconds are scheduled for either June 30 or December 31, a bi-annual monitoring is performed to check if a leap second will occur in June or December:

Leap seconds checks are tracked via checking International Earth Rotation and Reference Systems Service (IERS). The checks are traced in LuxTrust ticketing system.

LuxTrust has set up a process to ensure the management of leap seconds once detected.

6.4 TSA management and operation

6.4.1 Security management

LuxTrust TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognised best practices.

All requirements and subjects related to security management are implemented as described in the LuxTrust CPS [8].

6.4.2 Asset classification and management

LuxTrust TSA ensures that its information and other assets receive an appropriate level of protection.

The description of methods and measures undertaken for affirmation of continuity and stability of LuxTrust TSA system operation is described in the LuxTrust CPS [8].

LuxTrust TSA maintains an inventory of all assets that are assigned a classification for the protection requirements in a consistent way with the risk analysis.

6.4.3 Personnel security

LuxTrust TSA ensures that the personnel and hiring practices enhance and support the trustworthiness of the TSA's operations. Description of the personnel security rules as well as the trusted roles used in LuxTrust TSA services environment is provided in the LuxTrust CPS [8].

Managerial and operational personnel possess the appropriate skills and knowledge of Time Stamping, digital signatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.

6.4.4 Physical and environmental security

LuxTrust TSA ensures that physical access to critical services is controlled and physical risks to its assets minimised.

The implementation of the physical and environmental security is provided in accordance with the rules described in the LuxTrust CPS [8].

6.4.5 Operations management

LuxTrust TSA ensures that the TSA system components are secure and correctly operated, with minimal risk of failure.

LuxTrust TSA possesses the procedures, processes and infrastructure to comply with the operational management, procedural security requirements, system access management, trustworthy systems deployment and maintenance, business continuity management and incident handling as defined in ETSI EN 319 421. This information is mainly internal company documentation, disclosed to the TSA auditors on a need-to-know basis in conformance with the LuxTrust CPS [8].

LuxTrust TSA ensures that TSA system access is limited to properly authorised individuals in accordance with the LuxTrust CPS [8].

6.4.6 Trustworthy Systems Deployment and Maintenance

LuxTrust TSA ensures that it uses trustworthy systems and products that are protected against modifications in accordance with the LuxTrust CPS [8]. Analysis of security requirements is carried out at the design and requirement specifications stage of any systems development project undertaken by the TSA or on behalf of the TSA to ensure that security is built into IT systems. Change control procedures are applied for releases, modifications and emergency software fixes of any operational software.

6.4.7 Compromise of TSA Services

LuxTrust TSA ensures that in the case of events which affect the security of TSA services, including compromise of TSU private signing keys or detected loss of calibration, that relevant information is made available to Subscribers and Relying Parties in accordance with the LuxTrust CPS [8] and in accordance with ETSI EN 319 421 [16].

6.4.8 TSA termination

LuxTrust TSA ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation of the TSA Time Stamping services, and in particular ensures that continued maintenance of information required for verification of the correctness of Time Stamp Tokens. LuxTrust

TSA revokes the Time Stamping Units (TSU's) certificates when it terminates its services. TSA termination is also ruled in accordance of the LuxTrust CPS [8].

6.4.9 Compliance with Legal Requirements

LuxTrust TSA ensures compliance with appropriate legal requirements and is acting under the Grand-Duchy of Luxembourg law regulations, and in particular data protection and privacy regulations.

With regard to the provision of LuxTrust Qualified Certificates, LuxTrust S.A. acting as CSP through its LuxTrust Global Qualified CA x operates:

- Following the terms of the Luxembourg Law of 17/07/2020 on electronic commerce as amended [11]. This law is based on European REGULATION (EU) No 910/2014 and lays out the legal framework of electronic signatures in the Grand Duchy of Luxembourg,
- According to the ETSI standard EN 319 411-1 and 2, EN 319 421 & EN 319 422,
- According to the present LuxTrust CPS and the applicable CP.

LuxTrust S.A. acting as CSP accepts annual compliance audit for its LuxTrust CAs and all its supporting certification services to ensure they meet the ILNAS requirements for the voluntary "Supervision of Certification Service Providers issuing certificates or providing other services related to electronic signatures" as described and available on the official ILNAS website, www.ilnas.lu. LuxTrust S.A. is listed as "under supervision" by ILNAS, the Luxembourg public standardisation service, as a certification service provider (CSP).
LuxTrust is certified by LSTI acting as certification entity.

6.4.10 Recording of information concerning operation of Time Stamping service

LuxTrust TSA ensures that all relevant information concerning the operations of the LuxTrust Time Stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings, in accordance with the LuxTrust CPS [8].

In addition, records concerning all events relating to synchronization of a TSU's clock to UTC are logged, including but not limited to: :

- synchronization of clocks used in time-stamping
- detection of loss of synchronization

6.5 Organisational

LuxTrust TSA ensures that its organisation is reliable as required in ETSI EN 319 421 [16]. LuxTrust S.A. has the financial stability and resources required to operate in conformity with LuxTrust Global Qualified Certification Practice Statement [8]. Official address of LuxTrust S.A. is as follows:

LuxTrust contact information	
Contact Person:	CSP Board Contact
Postal Address:	LuxTrust S.A. Time Stamping Authority c/o CSP Board Member IVY Building 13-15, Parc d'activités L-8308 Capellen
Telephone number:	+352 26 68 15 - 1
Fax number:	+352 26 68 15 - 789
E-mail address:	*cspboard@luxtrust.lu*
Website:	https://www.luxtrust.com

LuxTrust is supervised by ILNAS acting as supervision entity.

The supervised CP 1.3.171.1.1.10.3.18 is under the LuxTrust Global Qualified CA x.

The national registry of supervised Certification Service Providers is publicly available on the ILNAS website http://www.ilnas.lu/.

6.6 Dispute Resolution Provisions

Procedures for dispute resolution are applicable as laid out by the LuxTrust CPS [8].