

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

---

**QTSP**

**QUALIFIED TIMESTAMP SERVICE**

**CERTIFICATION PRACTICE STATEMENT E CERTIFICATE  
POLICY**

---

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## INDICE

<b>1</b>	<b>SCOPE</b>	<b>6</b>
1.1	OVERALL	6
1.2	DOCUMENT NAME AND IDENTIFICATION	6
1.2.1	Document identification	6
1.3	PKI PARTICIPANTS	7
1.3.1	Provider	7
1.3.2	Client	7
1.4	USING THE TIMESTAMP	7
1.5	POLICY ADMINISTRATION	8
1.5.1	Administration of the document	8
1.5.2	Responsibility of the suitability	8
1.5.3	Document approval procedures	8
1.6	DEFINITION AND ACRONYMS	8
1.6.1	Definitions	8
1.6.2	Acronyms	11
<b>2</b>	<b>PUBLICATION</b>	<b>12</b>
2.1	REPOSITORY	12
2.2	PUBLICATION OF CERTIFICATION INFORMATION	12
2.2.1	Publication of information on the QTSP	12
2.3	PUBLICATION FREQUENCY	12
2.3.1	Frequency publication of terms and conditions	12
2.3.2	Frequency of publication of certificates	12
2.4	REGISTRATION OF THE TIMESTAMP	13
<b>3</b>	<b>TSU CERTIFICATE AND TIMESTAMP</b>	<b>13</b>
3.1	USER IDENTIFICATION	13
3.2	TSU CERTIFICATE	13
3.3	TIMESTAMP	13
3.3.1	Timestamp request	14
3.3.2	Timestamp (timestamp response)	15
3.4	ACCURACY OF TIMESTAMP	16
3.5	SYNCHRONIZATION	16
3.5.1	Managing leap second	16
3.5.2	Daylight saving time management	16
3.6	TIMESTAMP VALIDATION	16
3.7	TIMESTAMP SERVICES AVAILABILITY	17
3.8	RELEASE OF UNQUALIFIED TIMESTAMPS	17
3.9	MANAGING TSU KEYS	17
3.10	MARKUP PROTOCOL	17
<b>4</b>	<b>CERTIFICATE LIFECYCLE REQUIREMENTS</b>	<b>18</b>
4.1	KEY PAIR AND USE OF THE CERTIFICATE	18
4.1.1	Subscriber private key and certificate usage	18

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

4.1.2	Interested parties – Public key and use of the certificate.....	18
<b>5</b>	<b>FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS.....</b>	<b>19</b>
5.1	PHYSICAL CONTROLS .....	19
5.1.1	Location site and features.....	19
5.1.2	Physical access .....	19
5.1.3	Power supply and air conditioning .....	20
5.1.4	Exposure to water .....	21
5.1.5	Prevention and fire protection.....	21
5.1.6	Media Storage.....	22
5.1.7	Provisions on the disposal of apparatus .....	22
5.1.8	Off-Site Backup .....	22
5.2	PROCEDURAL CONTROLS.....	22
5.2.1	Roles .....	22
5.2.2	Number of people required for task .....	23
5.2.3	Identification and authentication of roles .....	23
5.2.4	Roles required segregation .....	23
5.3	PERSONNEL CONTROL .....	23
5.3.1	Qualifications, experience and clarity of requirements .....	24
5.3.2	Background verification procedures.....	24
5.3.3	Training requirements .....	24
5.3.4	Refresh rate .....	25
5.3.5	Sanctions on unauthorized actions .....	25
5.3.6	Requirements on consultants.....	25
5.3.7	Documentation provided to staff .....	25
5.4	AUDIT PROCEDURES .....	26
5.4.1	Types of events stored .....	26
5.4.2	Frequency of audit processes.....	26
5.4.3	Audit log retention period .....	27
5.4.4	Audit log protection .....	27
5.4.5	Audit log backup procedures.....	27
5.4.6	Audit event collection system.....	27
5.4.7	Verbosity error notification.....	27
5.4.8	Vulnerability Assessment .....	27
5.5	STORING RECORDS .....	28
5.6	TSA KEY CHANGEVER.....	28
5.7	COMPROMISE AND DISASTER RECOVERY.....	28
5.7.1	Incident and compromise management procedures .....	29
5.7.2	Computing Resources, Software, and/or corrupted data .....	29
5.7.3	Private key compromise procedures .....	29
5.7.4	Capacity of business continuity in case of disaster .....	29
5.8	CESSATION OF ACTIVITY .....	30
<b>6</b>	<b>TECHNICAL SECURITY CHECKS .....</b>	<b>31</b>
6.1	GENERATING AND INSTALLING KEY PAIR .....	31
6.1.1	Generating key pair .....	31
6.1.2	Key size.....	31
6.1.3	Key generation parameters and quality control.....	32
6.1.4	Key usage purpose (see key usage field X.509 v3) .....	32
6.2	PRIVATE KEY PROTECTION AND CONTROLS ON CRYPTOGRAPHIC COMPONENT .....	32
6.2.1	Standard and cryptographic controls .....	32

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

6.2.2	Private key segregation control (MofN) .....	33
6.2.3	Key Escrow private key.....	33
6.2.4	Backup private key .....	33
6.2.5	Key storage .....	33
6.2.6	Transfer of the private key to/from the cryptographic module .....	33
6.2.7	Storing the private key on the cryptographic module .....	33
6.2.8	Private key activation method .....	34
6.2.9	Method of deactivating private key .....	34
6.2.10	Method of destruction of the private key .....	34
6.2.11	Cryptographic module evaluation .....	34
6.3	OTHER ASPECTS OF KEY MANAGEMENT.....	35
6.3.1	Public key storage .....	35
6.3.2	Validity of the certificate and keys .....	35
6.4	ACTIVATION DATA.....	35
6.4.1	Activation data generation and installation .....	35
6.4.2	Activation data protection.....	35
6.5	COMPUTER SECURITY CONTROLS.....	35
6.5.1	Specific technical security requirements on IT system .....	35
6.5.2	Assessment of IT system security.....	36
6.6	LIFE CYCLE OF ROADWORTHINESS TEST .....	36
6.6.1	Control of development system.....	36
6.6.2	Security management controls .....	36
6.6.3	Life cycle of security controls .....	37
6.7	NETWORK SECURITY CHECKS .....	37
6.8	TIME-STAMPING .....	38
7	CERTIFICATES, CRL, AND OCSP PROFILES .....	39
7.1	CERTIFICATE PROFILE.....	39
7.1.1	Specification X509.....	39
7.1.2	Certificate extensions .....	39
7.1.2.1	Continuity management of Lottomatica S.p.A. certificates .....	41
7.1.2.2	Continuity management of Lottomatica Holding certificates following VAT change .....	42
7.1.3	Object Identifier Algorithms .....	42
7.1.4	Composition of the name.....	42
7.1.5	Constraints on name .....	42
7.1.6	Certificate Object Identifier policy .....	42
7.1.7	Usage of policy constraints extension.....	43
7.1.8	Syntax and semantics of policy qualifiers .....	43
7.1.9	Semantics management for critical policy extensions.....	43
7.2	CRL PROFILE .....	43
7.2.1	Version .....	43
7.2.2	Specification of CRL Extensions .....	43
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	45
8.1	FREQUENCIES OR ASSESSMENT REQUIREMENTS.....	45
8.2	IDENTITY/QUALIFICATION OF ASSESSOR.....	45
8.3	INDEPENDENCE OF THE ASSESSOR .....	45
8.4	TOPICS COVERED BY THE ASSESSMENT .....	46
8.5	ACTIONS TAKEN IN THE EVENT OF NON-COMPLIANCE.....	46
8.6	COMMUNICATING THE RESULT .....	46

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

<b>9</b>	<b>LEGAL ECONOMIS ASPECTS</b>	<b>47</b>
9.1	RATES	47
9.2	FINANCIAL LIABILITIES	47
9.2.1	Insurance coverage	47
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	47
	THE CONFIDENTIALITY OF BUSINESS-RELATED INFORMATION IS MANAGED IN ACCORDANCE WITH CURRENT LEGISLATION.	47
9.4	PROTECTION OF PERSONAL DATA	47
9.4.1	Methods of protection of personal data	48
9.5	INTELLECTUAL PROPERTY RIGHTS	51
9.6	DECLARATIONS AND WARRANTIES	52
9.6.1	Statements and warranties of the TSA	52
9.7	WARRANTY STATEMENTS	52
9.8	LIABILITY LIMIT	52
9.9	ALLOWANCES	53
9.10	SERVICE LIFE AND TERMINATION	53
9.10.1	Duration	53
9.10.2	Resolution	53
9.10.3	Effects of cessation	53
9.11	NOTIFICATIONS AND COMMUNICATIONS WITH USERS	54
9.12	CHANGES TO THE CPS	54
9.12.1	Procedures for the dissemination of CPS	54
9.12.2	Notification and timing mechanism	54
9.12.3	Circumstances under wich it is necessary to change OID	54
9.13	DISPUTE RESOLUTION	54
9.14	GOVERNAMENT LAWS	54
9.15	COMPLIANCE WITH LAWS IN FORCE	54
<b>10</b>	<b>REFERENCES</b>	<b>55</b>

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 1 SCOPE

This document contains the policy specifications for the issuance of qualified timestamp (certificate policy – hereinafter referred to as CP) and describe process, methodology and operating process (Certification Practice Statement –hereinafter referred to as CPS) for the Qualified trust service provider Lottomatica Holding S.r.l., and concerning the Timestamp Service.

This methodology is described in this document (hereinafter, document).

This document is compatible with the requirements expressed in the European regulation 910/2014 [28] and, and the activity described is compatible with the provision of services provided by qualified Trust service providers (hereinafter QTSP).

The QTSP (Lottomatica Holding S.r.l.) reserves the right to make changes to this document for technical requirements or for changes to the procedures that have occurred either due to law or regulations, or for the optimization of the working cycle.

Each new version of the manual cancels and replaces the previous versions, which remain however applicable to certificates issued during their validity and until the first expiration of the same.

### 1.1 OVERALL

The Timestamp system document contains a "set of rules that specify the usability of a time stamping service for a community and/or a class of applications with common security requirements."

This document consists of 9 chapters containing the security requirements, processes and practices defined by the QTSP to be followed during the delivery of the service

This document defines basic requirements for Timestamp and, in particular, the TSA and the TSU. The manner in which these requirements are respected, the detailed description of the methods mentioned are included in the practice statement of the qualified Timestamp Service (CPS) issued by Lottomatica Holding S.r.l..

### 1.2 DOCUMENT NAME AND IDENTIFICATION

#### 1.2.1 Document identification

This document is called "*QTSP Qualified Timestamp Service – Certification Practice Statement and Certificate Policy*" and is characterized by the document code: LTIS-05-00007/18. The version and the release level can be identified on the heading of each page.

All time stamps issued by the QTSP refer to specific Policies for which they are issued. The following OID is a unique identifier issued to Lottomatica Holding S.r.l..

1-3-76-49

The timestamp issued in accordance with this document complies with the following standard:

- ETSI EN 319 421 [25]  
BTSP: a best practices policy for time-stamp  
OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1)  
best-practices-ts-policy (1);

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- DPCM 22 febbraio 2013.

The mentioned OID is included in the Timestamps released by the QTSP. The organization-specific OID and used in the certificate profile are detailed in this paragraph.

This document is reviewed at least annually as well as the relevant applicability criteria. This document includes specific requirements relating to services provided for Italian customers, operating under Italian law in Italian language.

Below is the unique identifier of this document

OID	Description
(1)	International Organization for Standardization (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2
(76)	UNINFO
(49)	Lottomatica Holding S.r.l.
(2)	Lottomatica Holding S.r.l. Time Stamp Authority
(1)	Documents
(1)	Public Documents
(51)	Lottomatica Holding S.r.l. Certification Authority qualified Timestamp Service - Certification Practice Statement and Certificate Policy

## 1.3 PKI PARTICIPANTS

### 1.3.1 Provider

The qualified Timestamp service provider is a qualified Trust Service (hereinafter QTSP), which issues the date and time within the scope of a qualified trust.

The QTSP delivers the service through a component of CA (TSA) that emits certificates for the TSU components, and the TSU components that physically deliver the Timestamps.

The contact details of Lottomatica Holding S.r.l. are detailed in 1.5.1.

### 1.3.2 Client

The term client refers to the set of applications that use the Timestamp service provided by the QTSP.

## 1.4 USING THE TIMESTAMP

Through the affixing of a Timestamp, it is possible to associate a date and time legally certain and opposable to third parties in accordance with current European and national legislation.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

The service described in this document is used by Lottomatica Holding S.r.l. exclusively for the integration of a qualified time stamp within the qualified electronic signature issued by Lottomatica Holding S.r.l. and/or in any case within the activities attributable or conveyed by Lottomatica Holding S.r.l. and / or LIS - Lottomatica Italia Servizi S.p.A. o companies subject to the common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A.

## 1.5 POLICY ADMINISTRATION

### 1.5.1 Administration of the document

The staff data that administers this document are as follows:

Contact	Carmine Tufano
Organization name	Lottomatica Holding S.r.l.
Address	Viale del Campo Boario 56/d, 00154 Roma
Phone	(+39) 06 518991
Email	<b><u>firmaqualificata@pec.lottomatica.it</u></b> → from <b>01 March 2021</b> the reference address will be <b>caigt@pec.it</b>

### 1.5.2 Responsibility of the suitability

The QTSP is responsible for providing the services in accordance with the regulations and standards mentioned in this CPS.

The certification services and related procedures in this CPS are supervised by the AgID (Digital Italian Agency).

The trust list of certification certificates of Qualified Trust Service Providers is made available on the AgID website.

### 1.5.3 Document approval procedures

Where provided for or subject to changes to the regulations, the QTSP applies criteria for review and approval of this CPS in accordance with the internal procedures for reviewing and approving the document, and in accordance with the 9.12.

In particular, this document is subject to a review process, at least annually, by the Managers of the Organizational Structure of the Digital Signature Service and the changes made are subject to final approval of the CTO.

## 1.6 DEFINITION AND ACRONYMS

### 1.6.1 Definitions

From the European Regulation 910-2014 eIDAS, Art 3 [28]:

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- (1) 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- (2) 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- (3) 'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- (4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
- (5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- (6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;
- (7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- (8) 'body governed by public law' means a body defined in point (4) of Article 2 paragraph (1) of Directive 2014/24/EU of the European Parliament and of the Council;
- (9) 'signatory' means a natural person who creates an electronic signature;
- (10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- (11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
- (12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
- (13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;
- (14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
- (15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
- (16) 'trust service' means an electronic service normally provided for remuneration which consists of:
  - (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
  - (b) the creation, verification and validation of certificates for website authentication; or
  - (c) the preservation of electronic signatures, seals or certificates related to those services;
- (17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;
- (18) 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
- (19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- (20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
- (21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
- (22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
- (23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;
- (24) 'creator of a seal' means a legal person who creates an electronic seal;
- (25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- (26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;
- (27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
- (28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;
- (29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
- (30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;
- (31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;
- (32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;
- (33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- (34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;
- (35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
- (36) 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- (37) 'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;
- (38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- (39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
- (40) 'validation data' means data that is used to validate an electronic signature or an electronic seal;
- (41) 'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 1.6.2 Acronyms

QTSP	Qualified Trust Service Provider
CA	Certification Authority
HSM	Hardware Security Module
HA	High Availability
CRL	Certificate Revocation List
OCSP	Online Certificate Protocol Status
TSA	Time Stamp Authority
TSU	Time Stamp Unit
QSCD	Qualified Signature Creation Device
RAO	Registration Authority Officer
RAA	Registration Authority Administrator
RA	Registration Authority
PKI	PKI Public Key Infrastructure - This term means a series of agreements that allow trusted third parties to verify and / or guarantee the identity of a user, as well as associate a public key with a user, usually by means of distributed software co-ordinated on Different systems. Public keys typically take the form of digital certificates.
PIN	Personal Identification Number
PUK	Personal Unlock Key
SN	Serial Number
SSL	Secure Socket Layer – Standard protocol for managing secure Internet transactions based on the use of public key cryptographic algorithms.
WS	Web Service
ICT	Information and Communication Technology
VPN	Virtual Private Network
PdV	Stores
CAB	Conformity Assessment Body
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
HTTP	HyperText Transfer Protocol
OID	Object Identifier
OTP	One Time Password

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 2 PUBLICATION

### 2.1 REPOSITORY

The QTSP publishes this document and other documents containing terms and conditions on which it is based on their service.

### 2.2 PUBLICATION OF CERTIFICATION INFORMATION

TSA certificates are available on the **QTSP portal**.

#### *TSA Certificates*

The QTSP publishes information about its certificates through:

- CPS documents;
- On the **QTSP Portal**

#### *TSU Certificates*

The QTSP publishes information about the status of the TSU certificate through the Certificate Revocation list (CRL).

#### 2.2.1 Publication of information on the QTSP

The QTSP publishes contractual terms and conditions electronically on the **QTSP portal**.  
New documents relating to the service are disclosed on the site 14 days of entry into force.  
The documents in force are available on the site, in addition to all previous versions of all documents.

### 2.3 PUBLICATION FREQUENCY

#### 2.3.1 Frequency publication of terms and conditions

The publication of new versions of this document complies with the modalities described in paragraph 9.12.

#### 2.3.2 Frequency of publication of certificates

The QTSP publishes certificate to root TSA before it starts operating.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 2.4 REGISTRATION OF THE TIMESTAMP

In accordance with the provisions of Title IV of the DPCM of 22 February 2013, art. 53, "All time stamps issued by a validation system are stored in a special digital archive that can not be modified for a period of at least 20 years or, at the request of the party concerned, for a longer period of time under the conditions provided by the QTSP"

## 3 TSU CERTIFICATE AND TIMESTAMP

### 3.1 USER IDENTIFICATION

The qualified Timestamp service provided by QTSP is used according to the limitations described in par. 1.4.

To do this, there is no end-user identification, but a service delivery against authentication mechanisms managed by IT systems.

### 3.2 TSU CERTIFICATE

In order to ensure the integrity and authenticity of the public key:

- TSU's public key is published as a certificate; The certificate for the key pair used for temporal validation must be able to identify the temporal validation system;
- The TSU certificate and issued by the TSA of QTSP in accordance with the standard ETSI en 319 411-1 [3];
- The TSU certificate issuing the qualified Timestamp in accordance with regulation 910/2014/EU [28], must be issued by a CA (TSA) providing service in accordance with the standard ETSI en 319 411-2 [4];
- The TSU can only release the Timestamps when it has a certificate for Timestamp verification, the signature of which is verified through the recognition of the certificate chain that points to the TSA;
- In order to limit the number of Timestamps, the TSU certificate is renewed within a maximum limit of 3 months (DPCM 22 February 2013 Art 49 paragraph 2);
- For the subscription of Certificates for Timestamp keys, specially generated certification keys are used.

### 3.3 TIMESTAMP

The timestamp operation:

- It must conform to the IETF RFC 3161 [13] Standard and ETSI en 319 422 [26];
- It is released in a safe environment and must contain a correct time reference;
- The internal clock of the TSU used for the release of the timestamp must be connected to an accurate source;
- The time reference provided in the timestamp must conform to the time value provided by UTC, and the difference must not exceed the accuracy indicated in the policy and the timestamp itself;
- The TSU must not deliver the timestamp when the accuracy measured at the time of the Timestamp is processed does not exceed the declared value;
- The private keys used to certify the timestamp must not be used for any other purpose;
- TSU must refuse any Timestamp request if the duration of the subscription keys is exceeded.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 3.3.1 Timestamp request

The timestamp client supports the Timestamp request in accordance with the IETF RFC 3161 [13] section 2.4.1 Standard.

In particular, it is recommended to use the following fields:

- Reqpolicy;
- Nonce;
- CertReq.

The QTSP supports the use of any extension.

The QTSP accepts the hashing algorithms in the timestamp request that conform to the standard ETSI TS 119 312 [10]. In detail:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
--------	--

#### *Timestamp request structure*

The Timestamp request requires the following fields:

- Version; the version is the V1 specified in IETF RFC 3161, and containing the value 1;
- MessageImprint: The given object of Timestamp, and containing
  - hashing algorithm, the OID of the hash algorithm in the hash;
  - hash, the value of the hash applied to the original document;
- Certificate Request: set to false;

Optional values:

- ReqPolicy, reference to the policy for which the Timestamp is required;
- Nonce, a value of type 64-bit integer, which is used to prove the uniqueness of the timestamp. When used, the response contained in the timestamp must contain the same value;
- Extensions, field to specify extension information.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 3.3.2 Timestamp (timestamp response)

The QTSP supports the timestamp response in accordance with the IETF RFC 3161 [13] Chapter 2.4.2 Standard, with the following additional requirements:

- "accuracy";
- "nonce".

In the case of using the "nonce" field in the timestamp request, the response mark must contain the same value that is contained in the request.

The QTSP uses policies related to the use of cryptographic algorithms and length of timestamp signature keys that conform to the standard ETSI TS 119 312 [10].

In detail, the supported hashing algorithms are:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
--------	--

#### Timestamp structure

The timestamp structure includes the following fields:

- Status, state information concerning the release, in accordance with the public IETF RFC 3161, chap. 2.4.2.

Optional values:

- Timestamp token, valued in the Status field is worth 0 or 1, otherwise it is not included in the response.

#### Token timestamp structure

The structure of the token timestamp includes the signature of the TSU and is in accordance with what is specified in the public IETF RFC 3161, chap. 2.4.2.

Are included in TST:

- Version is the V1 specified in IETF RFC 3161, and contains the value 1;
- Policy, specifies the policy to which the Timestamp is compliance. The value contained must be that corresponding to the reqPolicy of the corresponding request;
- MessageImprint, the Timestamp data containing the same value as the request;
- SerialNumber, a unique serial of Timestamp, released by TSU (maximum 160 bits in length);
- GenTime: Timestamp issuance time in UTC format; The time reference must be in accordance with the precision value declared in 3.4;
- Accuracy, accuracy of the Timestamp, in accordance with the precision value declared in 3.4.

Optional values:

- Nonce, a value of type 64-bit integer, which is used to prove the uniqueness of the timestamp. When used, the response contained in the timestamp must contain the same value;
- Ordering, default value: false;
- TSA, the value della subject contained in the TSU certificate which issued the Timestamp;
- Extensions, the QTSP uses this extension to indicate the qualified status of the timestamp in accordance with the and regulation, as follows:

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

Qualified certificate statements – non-critical

OID: 1.3.6.1.5.5.7.1.3

The extension contains one statement: "Esi4-qtstStatement-1"

### 3.4 ACCURACY OF TIMESTAMP

The accuracy contained in the Timestamp must be up to 1 second.

The TSU clock must be protected against threats that could impair its accuracy;

The QTSP time-stamping control the declared accuracy; If the value exceeds the reported accuracy value, the QTSP suspends service delivery. The accuracy of the QTSP watch is examined annually.

### 3.5 SYNCHRONIZATION

The TSU component is synchronized with NTP sources, as defined in the Security Plan of QTSP.

Synchronization has the main task of keeping the accuracy value specified in chapter 3.4.

#### 3.5.1 Managing leap second

The QTSP must synchronize the clock according to the notification of the competent body with respect to the occurrence of the leap second. The application of the timetable must be changed at the last minute of the day established according to the specifications contained in the ETSI standard 319 421 [25] Annex C, and as defined in the ITU-R TF recommendation. 460-6 [17].

#### 3.5.2 Daylight saving time management

The time that is provided in UTC within the timestamp can be interpreted by client applications in different format, often in local time format.

Potential problems associated with (the erroneous) interpretation of the temporal reference must be brought to the attention of the parties involved in this document.

### 3.6 TIMESTAMP VALIDATION

When verifying the validity of the electronic signature in the timestamp, the parties involved must comply with the standard ETSI en 319 102-1 [8].

When checking the timestamp:

- It must be verified that the timestamp contained in the document is attributable to the certificate issued by the TSA;
- The signature must be verified on the timestamp;
- It must be verified that the timestamp complies with the specific requirements related to the accuracy of the time reference, and the reliability of the certificate issued QTSP.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 3.7 TIMESTAMP SERVICES AVAILABILITY

The QTSP guarantees that the availability of its systems at least 99.7% on an annual basis, while the downtime of the services may not exceed 8 hours in each case.

### 3.8 RELEASE OF UNQUALIFIED TIMESTAMPS

The QTSP does not deliver unqualified timestamp.

### 3.9 MANAGING TSU KEYS

The TSU subscription keys are managed in accordance with the Italian DPCM of 22 February 2013, Title IV, art. 49.

### 3.10 MARKUP PROTOCOL

The service is only exposed through the HTTPS protocol. The secure channel is established on the basis of the certificate installed on the TSU. Access to the service requires username and password.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 4 CERTIFICATE LIFECYCLE REQUIREMENTS

### 4.1 KEY PAIR AND USE OF THE CERTIFICATE

#### 4.1.1 Subscriber private key and certificate usage

The TSU private key must only be used for the certification of the timestamp issued by the service, and it is forbidden to use the same for other purposes. Lottomatica Holding S.r.l. warrants that the document is timed, does not contain macros, executable codes or other elements such as to activate features that may modify acts, facts or data in the same representations, in compliance with Article 4, paragraph 3 of the DPCM February 22, 2013 [24].

#### 4.1.2 Interested parties – Public key and use of the certificate

The parties interested to a qualified timestamp verification, must proceed in accordance with the contained in the document with particular regard to the following:

- Interested parties should check the validity and revocation status of the certificate marking;
- Interested parties must validate the certificate by appropriately verifying the whole chain of certificates;
- Interested parties must take into account any usage limitations specified in certificate and specified in this document.

The QTSP makes available services to allow the verification of certificates issued.

QTSP also publishes a portal (online verifier) for validating a signed digital signature and time stamp, publicly available at the following URL:

**<https://ver.ca.firmadigitale.lottomaticaitalia.it>**

The user needs to check the validity of the qualified electronic signature of a document, and the relative temporal marking, accessing the service indicated above and carries out loading (or upload) the file. The service returns the results of the validation test. The online verifier is a web based component implemented in Java, based on DSS project recommended by the European Commission for the full recognition of computer documents signed in the different Member States.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

### 5.1 PHYSICAL CONTROLS

QTSP adopts a set of technical and organizational measures that allow site access control and the safeguarding of corporate assets from thefts / disappearances and / or voluntary and involuntary damages. The definition of physical security policies is part of a wider process aimed at protecting information media and assuming a risk assessment activity that identifies the risks associated with the censored assets.

#### 5.1.1 Location site and features

The CED systems related to the production environments, are running on a HW infrastructure located on two separate sites:

- Site A is located in Rome, Viale del Campo Boario, 56d; the systems are located inside a dedicated cage;
- Site B is located in Rome, via dello Scalo Prenestino, 15 within the Data Center of AlmaViva, within which Lottomatica Holding S.r.l. has a machine room for exclusive use; the systems are located inside a dedicated cage.

Data centers are interconnected by a private backbone network and both connected to Internet access networks with bandwidth that provide qualified services with the same performance. The interconnection of individual DCs to both the public and private networks is implemented through redundant connections. This infrastructure ensures that the indicators described in section 4.10.2 are respected.

The CED area of the site A is made with adequate construction criteria. The rooms that host the apparatus are equipped with counter-floors and counter-ceilings (Site B), in compliance with standards and standards of reference. The infrastructures are all built using non-combustible, sound-absorbent and shatterproof materials.

In the processing room there is a lighting system that complies with the regulations and is equipped with an adequate emergency system.

#### 5.1.2 Physical access

##### *Site A*

The building and safe areas of Lottomatica Holding S.r.l. are protected by an access control system in order to guarantee the entry to the only authorized personnel.

Lottomatica Holding S.r.l. Defines internal security policy procedures that regulate physical access to the venue and reserved areas for both employees and occasional or habitual visitors.

In particular, a number of behavioural rules are envisaged:

##### Is required:

- Access the workplace using its access credentials (eg magnetic badges) from the prepared passes and the ways established by the company;
- Observe the rules from time to time given in writing or verbally by persons responsible for access to restricted areas;
- Respect corporate procedures for requesting access to external staff (consultants, regular and casual visitors);

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Communicate promptly any breaches of the rules to your Responsible Authority, to supervise your home or directly to the Security Area.

#### It is forbidden to:

- Give third party access credentials, even temporarily, and in case the credentials are lost, it must be timely communicated to the Security Area;
- Access restricted areas unless you have a specific authorization.

With regard to physical access control, Lottomatica Holding S.r.l. has implemented the following controls:

- Access is only allowed to holders of unexpired badges issued by the security area;
- The badge is assigned to employees and visitors, only after being previously identified and authorized by an internal Lottomatica Holding S.r.l. referent;
- The issuance of the badge must be consistent with the employee's company profile and must allow access only to areas of close competence;
- At any time the supervisors can carry out checks on the validity of the badge and therefore, if required, must be promptly exhibited.
- Access events (entry and exit) are recorded.

#### Site B

The building and safe areas of the Site B are protected by an access control system in order to guarantee entry to only authorized personnel.

The entire external perimeter of the DC, completely fenced, is illuminated in night time and constantly monitored by a CCTV system consisting of fixed cameras and DOM, all brought to a system of screens installed in the room directed by the vigilance and supervised H24x7. Images are recorded on a digital device for ex post checks and verifications.

### 5.1.3 Power supply and air conditioning

#### Site A

All the environments of the CED are adequately air conditioned through dedicated systems. As already mentioned, the conditioning system of the CED area is a direct expansion. Each unit is made up of two separate circuits. The modularity, together with the total power reserve, allows to cope with the stops for programmed maintenance and temporary failures.

Internal procedures ensure proper system maintenance.

The power supply is provided by the medium voltage distribution network by means of double ring connection. The medium voltage delivery cabin is physically separated from the cabin housing the two transformers, redundant configuration. The Site A also has uninterruptible power supplies to meet temporary power supply needs. All alarms from the systems that are relevant to the service continuity of the CED (including power supply, air conditioning, fire prevention, anti-flooding) are managed by a supervisory system.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

#### *Site B*

All DC processing rooms are air-conditioned by the use of chilled water cooled conditioners. Refrigerant power is produced by two active-standby refrigeration units located in distant areas. All alarms from the systems that are relevant to the service continuity of the CED (including power supply, air conditioning, fire prevention, anti-flooding) are managed by a supervisory system.

### 5.1.4 Exposure to water

#### *Site A*

The CED is maintained at temperature and humidity levels that prevent condensation. Cage cooling system is present over the condensation system and the water supply to the humidifiers of the air-conditioning system.

These three systems are equipped with special precautions in order to avoid water leakage. For any eventuality, an alarm system is installed that signals and locates any unlikely spillages of water below the raised floor, allowing the control staff to verify the causes and eliminate them.

#### *Site B*

The processing room near the ends of of the coolant distribution that serves the air conditioners is equipped with water detection sensors that bring to the system of monitoring of the plants, manned 24x7x365.

### 5.1.5 Prevention and fire protection

#### *Site A*

The site where the CED is located is equipped with fire protection systems under the law. The CED fire alarm system consists of a smoke detection system and a FM200 gas extinguishing fire. The system can operate both in automatic and manual mode. The sensors of the detection system are inserted both at ceiling and below the technical floor with repeating gems of the operating state of the single sensor.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### **Site B**

The CED is equipped with a centralized smoke detection system, which is headed to the supervised control room.

The processing rooms and the premises of the technological plants have the centralized smoke detection system also extended to the space under the floating floor and are equipped with automatic gas extinguishing systems in the ceiling, in the environment and under the floating floor, enslaved to the detection system and partitioned so as to confine the areas of activation.

The activation of the extinguishing system is automatic, and controlled by control units to the detection system.

#### **5.1.6 Media Storage**

Media storage activities are defined within internal security procedures.

#### **5.1.7 Provisions on the disposal of apparatus**

As a result of internal assessments or reports relating to failures, obsolescence or maintenance of hardware and/or media, the technical staff identifies the assets to be verified.

If the hardware or media support is working and reusable, you can delete the information in it, also availing itself of appropriate products that make the shredding of the data or formats at low level and the reuse of hardware or medium support as needed.

If it is impossible to restore the correct operation of the hardware, the safe deletion of the data contained in it by physical destruction (CD, DVDs made illegible with deep incisions, dat tape cutting) or profound alteration of the hardware and the subsequent request for the disposal of the property at internal structures in accordance with internal procedures on the disposal of company assets.

#### **5.1.8 Off-Site Backup**

Backup activities are defined within internal security procedures.

### **5.2 PROCEDURAL CONTROLS**

The QTSP applies internal processes aimed at ensuring that its systems are managed in a secure manner. Procedural precautions have the objective of integrating the effectiveness of physical security measures, together with those which apply to staff, by appointing and identifying trusted (unambiguous) roles, and to the computer application of the associated identification and authentication mechanisms.

The QTSP guarantees that its operation complies with the laws in force and its internal regulations.

#### **5.2.1 Roles**

In the exercise of its functions, the QTSP creates recognized roles, to which authorization mechanisms are applied commensurate with the related responsibilities.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

In accordance with the February 22, 2013 [24] DPCM, art. 38, QTSP has defined the organizational structure is present in the main roles defined to manage the services of qualified digital signature and timestamp that predicts the existence of the following figures:

- Responsible for the certification authority and time stamp;
- Responsible for Registration Authority;
- Security officer;
- Responsible of verifications and inspections (auditing);
- Responsible for the technical management of the systems;
- Technical and logistical services manager;
- Technical Services Manager of time stamp.

### 5.2.2 Number of people required for task

The QTSP applies a policy aimed at ensuring the simultaneous presence of at least 2 persons, with specially approved roles, during the following critical security operations:

- The generation of the TSA private key of the QTSP;
- Backup of the QTSP TSA private key;
- Activation of the QTSP TSA private key;
- Destruction of the QTSP TSA private key

At least one of the persons present must play an administrative role.

The above-mentioned operations must be carried out only in the presence of the persons expressly authorized.

### 5.2.3 Identification and authentication of roles

Users who manage the QTSP IT services have a unique and personal identification.

Users can have access to critical systems, only after identification and authentication.

Access permissions are immediately revoked in the event of termination of the user's behalf.

Each use of IT systems and every actor who manages the processes is identified individually.

Physical access to environments where systems are placed is protected as specified in 5.1.2.

Logical access is controlled by an internal monitoring system for access tracing and non-compliance notification.

### 5.2.4 Roles required segregation

The QTSP applies as specified in DPCM February 22, 2013 [24], art. 38 paragraph 3 and 4.

In this area:

- Security officer cannot assume other roles among those defined in 5.2.1;
- Responsible of verifications and inspections (auditing) cannot assume other roles among those defined in 5.2.1.

## 5.3 PERSONNEL CONTROL

Lottomatica Holding S.r.l. defines and applies criteria and methods through which:

- Takes into account the aspects related to the security of information in the human resources management process;
- Improves the sensitivity and levels of staff awareness about information security issues.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

These criteria and modalities apply to the activities of selection, incorporation into the company, training of staff and cessation of employment relationship.

### 5.3.1 Qualifications, experience and clarity of requirements

As part of the selection, training and human resources management processes, Lottomatica Holding S.r.l. ensures:

- That all staff have the necessary skills, reliability, experience and qualifications and have received adequate training in security and rules on the protection of personal data, depending on the function carried out;
- That, where possible, staff meet the requirements of experience and qualification through qualifications, training courses and/or demonstrated experience;
- that the relevant levels of the Organization are made available at least yearly updates on possible new threats, methodologies and tools to protect the security.

### 5.3.2 Background verification procedures

As part of the recruiting activity, the breeders pay attention, in addition to the potential compatibility of candidates with the professional needs of Lottomatica Holding S.r.l., to the relevant elements in terms of security, such as:

- The duration of previous professional experiences and the reasons for justifying the conclusion of the report;
- The sector of activity and the undertakings within which the previous professional activities have been conducted (with particular attention to those which may be regarded as supplying, customers or, where appropriate, competitors);
- In the case of a non-EU worker, a copy of the valid residence permit, or, if this is expired, a copy of the renewal request made in the terms of the law.

### 5.3.3 Training requirements

Lottomatica Holding S.r.l. is responsible for implementing employees, an appropriate training plan aimed at improving the processes related to the activity of the QTSP.

While respecting those that may be the contingent requirements that lead to planning a training course, the objectives common to all courses are:

- Increase the level of awareness about the security issues associated with the activity of the QTSP;
- To make the staff aware of the company's policies and guidelines, roles and corporate responsibility for security.

Lottomatica Holding S.r.l. carries out training activities in compliance with the following requirements:

- The staff responsible for preparing and delivering training must have the necessary qualifications and experience in terms of training;
- Where deemed necessary, the training activity can also be extended to suppliers and collaborators;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- The programming and delivery of all the courses required by the regulations applicable to the business of the company must be ensured;
- It is necessary to ensure the knowledge of the regulations in force regarding qualified trust services, as well as best practices and standards;
- The definition of training plans for qualified trust services must comply with the provisions of EU Regulation No 2016/679 [27] on the protection of individuals with regard to the processing of personal data.

#### 5.3.4 Refresh rate

Lottomatica Holding S.r.l. program trainings on a regular basis, based on the results of testing the course participants and/or on the basis of internal requirements.

#### 5.3.5 Sanctions on unauthorized actions

In relation to sanctions in case of different behavior than is required by the company in the documents concerning security (work instructions, policies, procedures etc.), Lottomatica Holding S.r.l. will reference the system of penalties provided for by the National Collective Labour Agreement.

#### 5.3.6 Requirements on consultants

The aspects connected with the control of the staff belonging to the external consultants and collaborators area, it is governed by internal business procedures, which define the criteria and processes for the identification of rules and requirements that Lottomatica Holding S.r.l. considers relevant in the field of supply and conclusion of contracts with third parties, taking into account the characteristics of the relationship that Lottomatica Holding S.r.l. establishes with them.

#### 5.3.7 Documentation provided to staff

When a candidate is selected and included in Lottomatica Holding S.r.l.'s staff, the human resources Management Area guarantees:

- Letter of recruitment;
- Any letter of posting C/O other Lottomatica Holding S.r.l. companies;
- Information on the treatment of personal data collected (Ctrl. 2); Information to workers on health and security at work;
- Code of Conduct;
- Behavioural rules for the safe management of company assets.

The "Code of conduct", in particular, includes:

- References to all the rules to which it is adhered and which violations or breaches of the code could result in disciplinary action;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Indications that employees are required to declare any conflict of interest with the work they perform, as soon as this occurs;
- Specific examples of conflict of interest;
- Information on hospitality/donations/gifts provided by third parties with whom Lottomatica Holding S.r.l. has contractual and economic relations.

## 5.4 AUDIT PROCEDURES

In order to maintain a secure IT environment, QTSP can implement an event management system that cover IT systems involved in the provision of the service.

### 5.4.1 Types of events stored

The QTSP, through specialised instruments, implements an action to monitor the events associated with the activity of the QTSP, in accordance with the provisions of the CAP. 6.4.5 of the standard EN 319 411 2 v 2.1.1 [4].

For the specific qualified Timestamp service, the controls specified in the standard EN 319 421 v 1.1.1 cap. 7.7.2 and 7.12 are also implemented and listed below:

- TSU Key Management:
  - Recording of key lifecycle events;
  - Registration of the events related to the life cycle of the certificate.
- Time Synchronization:
  - Recording of events connected with the TSU synchronization to the UTC clock, including recalibration and synchronization events;
  - Recording of synchronization loss events;
  - Recordings of events connected with the management of the leap second.

All events are stored and stored in accordance with what is specified in 5.4.3.

### 5.4.2 Frequency of audit processes

#### *Technical audit*

Lottomatica Holding S.r.l. activates the test processes and technical security tests against the following case:

- New Releases;
- Periodic planning;
- Specific requests or events.

The typology of such tests and verifications depends on the cases that activates the process.

#### *Systems audit*

All business structures affected by the activities of QTSP are subject to verification inspection at least once a year in relation to the activities prescribed by the information security management system.

The frequency of the checks is defined by:

- The importance and/or the criticality of the activities carried out by the individual structures;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- The results of previous audits;
- Any significant changes in the company organization and/or the activities carried out.

#### 5.4.3 Audit log retention period

The audit log retention period is 20 years, according with the DPCM 22 February 2013 [24].

#### 5.4.4 Audit log protection

The audit log protection is in accordance with the standard EN 319 401 v 1.1.1 [28] in Cap 7.10. In particular, the QTSP guarantees that the events connected with the delivery of the service, are stored in a way that ensures the protection of the modification, insertion or deletion of the entries. Archived logs are protected by backups that ensure recovery as a result of accidental (or malevolent) deletion, or loss of data. Appropriate security rules ensure that only staff in charge can access the data, or perform backup or archiving operations.

#### 5.4.5 Audit log backup procedures

Backup procedures for log management systems ensure that logs are stored in accordance with chapter 5.4.3.

#### 5.4.6 Audit event collection system

The QTSP adopts automated systems that ensure the collection activity on a continuous basis.

#### 5.4.7 Verbosity error notification

The QTSP adopts internal communication procedures, following the detection of an error message in the system.

#### 5.4.8 Vulnerability Assessment

The activity of vulnerability assessment consists in evaluating the level and effectiveness of the security of the ICT system through automatic scans aimed at detecting known vulnerabilities of ICT systems in relation to operating system components and middleware software (eg. Application server) and infrastructure (e.g. system monitoring) resident. This activity is accomplished through the use of specific automatic tools that, starting from a specific set of tests (Baseline/template):

- Conduct technical checks on the known vulnerabilities of ICT systems;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Produce reports detailing the test results and vulnerabilities detected.

Considering the entire set of technical tests that the specific automatic scanning tool can operate, specific subsets of these technical checks, called the baseline/template, are defined and adopted, which are suitable and applicable to the type of target systems to be verified.

Lottomatica Holding S.r.l. activates the processes of VA in the face of the following case:

- new Releases;
- Periodic planning (1 time per quarter for site A and B);
- Specific requests or events.

Penetration Test activities are also carried out at least annually.

## 5.5 STORING RECORDS

Record archiving complies with the standard EN 319 401 v 2.1.1 [1] in Cap 7.10. The retention period applied to logs is 20 years.

The QTSP implements mechanisms that ensure:

- Compliance with the log retention policy;
- Compliance with the requirements of confidentiality and integrity of the data, providing procedures to guarantee the verification of the authenticity of the data;
- Compliance with the requirements on the availability of information, ensuring the usability of them over time.

## 5.6 TSA KEY CHANGEOVER

In order to guarantee its operation, the QTSP ensures that the renewal of its certificate is carried out long enough before the expiry of the certificate itself.

The QTSP ensures that in case of renewal, a new key pair is generated in accordance with the regulations in force.

It is also specified that:

- The new certificate is published in the public repository of certificates, in compliance with what is specified in this CPS in Chapter 6.1.4;
- That the old keys and their certificate are kept under the law, guaranteeing mechanisms of verification until the natural maturity of the same.

## 5.7 COMPROMISE AND DISASTER RECOVERY

In the event of a disaster, the QTSP shall take all necessary measures to minimize the damage caused by the lack of service, and implement an operational plan designed to restore the services within the time stated in this document, in line with the QTSP's internal Business Continuity procedures.

The recovery point objective (RPO) must allow a limited loss of data, commensurate with business objectives. The RPO set for this infrastructure, is 5 minutes.

Based on the assessment of the accident, the QTSP will take all corrective measures to prevent future recurrence of the incident.

The QTSP adopts an inside plan for security to ensure that DR test are carried out regularly, ensuring that the observations resulting from technical problems or non-compliance associated with the reactivation of the services, are subject to revision and improvement of the said plan.

The QTSP directs the resolution of each vulnerability considered critical within 48 hours of its discovery, through an appropriate plan of re-entry.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

The QTSP provides, within internal procedures, the implementation of an emergency plan in case you detect a security breach or a loss of data integrity with a significant impact on trust services provided or on personal particulars stored ("data breach"). In particular, in accordance with article 19 of regulation eIDAS [28] security incidents are classified with 5 levels of severity:

1. No impact;
2. No significant Impact (impact on assets but not on services core);
3. Significant impact (impact on a clientele);
4. Severe Impact (impact on a large part of the clientele)
5. Disastrous (impact on the entire organization and on all certificates issued)

This plan allows to limit the impact of the security breach and to notify:

- Stakeholders (AgID, guaranteeing Privacy and holders) within 24 hours of detection of the violation, in case of security incidents are classified with a severity level 3, 4 and 5.

#### 5.7.1 Incident and compromise management procedures

The QTSP has a business continuity plan that adopts in case of incident and management of the compromise.

The QTSP adopts prevention criteria, implementing design systems aimed at preventing the single point of failure, while ensuring the operational continuity, even in fault situations of a system or apparatus.

#### 5.7.2 Computing Resources, Software, and/or corrupted data

The QTSP must adopt and maintain the same HW/SW systems between the Site A and the Site B, in order to avoid problems in the restore of the service data between the sites.

The QTSP must adopt backup policies to ensure the operational transfer on the Site B, consistent with the RPO stated in this document. The backup activities are performed by the authorized personnel ("system operators"), consistent with the 6.4.8 C clause of the ETSI en 319411-1 standard.

#### 5.7.3 Private key compromise procedures

The QTSP has a disaster recovery plan that follows in emergency conditions resulting from the compromise of the private key. The Action plan addresses:

- The circumstances of the compromise in addition to the withdrawal of the public key of the QTSP;
- Organizes notifications of all stakeholders;
- Immediately ceases to use that particular key, providing a new key to the service unit.

The informations with the revocation of the TSA certificate are published on the **QTSP Portal**.

#### 5.7.4 Capacity of business continuity in case of disaster

The tasks to be performed in the event of a disaster must be defined in the QTSP Business continuity plan.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 5.8 CESSATION OF ACTIVITY

The cessation of the activity of the QTSP complies with what is specified in the code of the Digital Administration, published with D. LGS. Of March 7, 2005, N. 82 and updated with the D. LGS 179/2016.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 6 TECHNICAL SECURITY CHECKS

The QTSP uses systems that are predisposed with high reliability criteria applied to the individual element, or connected with the service provided. The systems provide protections on the management of cryptographic keys, and on the activation data for the entire lifecycle of the same. In particular, the QTSP uses HSM to manage the lifecycle of the keys, and ensures that they are treated in accordance with the management manuals provided by the vendor, and in accordance with the certification milestone under which they are configured and operate the apparatus.

The technical security controls applied to the IT systems involved in the internal processes of the QTSP are covered by certification complying with the ISO 27001 standard.

The capacity of the systems is connected with demand, and is monitored on a continuous basis. Growth is estimated to ensure the availability of systems and storage media.

### 6.1 GENERATING AND INSTALLING KEY PAIR

The QTSP ensures that the production and management of private keys complies with the standards laid down by the standards in force.

In particular, the QTSP uses HSM to manage the lifecycle of the keys, and ensures that they are treated in accordance with the management manuals provided by the vendor, and in accordance with the certification milestone under which they are configured and operate the apparatus.

#### 6.1.1 Generating key pair

The QTSP is responsible for the generation of the following key types:

1. Certification keys, associated with TSA service;
2. Subscription keys, intended for TSU;

All keys are generated through an HSM-type device, complying with the certification standards listed in Chapter 6.2.1.

The TSA key generation process complies with what is specified in the EN319 411 01 v 1.2.2 [3] Standard, with particular reference to the 6.5.1, 6.5.2 and 6.5.3 chapters.

The TSU key generation process complies with what is specified in the standard EN 319 421 v 1.1.1 [25], with particular reference to chapter 7.6.2.

Lottomatica Holding S.r.l. confirms that the process of generating the keys is carried out in accordance with the technical rules in relation to what is in force; In particular: The TSA key generation process complies with the EN 319 411 01 v 1.2.2 [3] Standard, with particular reference to the chapters 6.5.1, 6.5.2 and 6.5.3; The TSU key generation process complies with the standard EN 319 421 v 1.1.1 [25], with special reference to the 7.6.2 chapter.

#### 6.1.2 Key size

The QTSP uses policy related to the use of algorithms and key sizes as specified in the standard ETSI TS 119 312 [10].

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

In particular:

- The RSA root TSA key is 4096 bits long;
- The RSA keys of the TSU are 2048 bits long.

### 6.1.3 Key generation parameters and quality control

Requirements on key generation parameters are listed in cap 6.1.1.

The QTSP ensures that all security operations carried out with the HSM, with particular reference to key generation, are carried out in accordance with the security target.

### 6.1.4 Key usage purpose (see key usage field X.509 v3)

The TSA certificate includes the following key usage:

- Digital Signature
- Certificate Signing
- Off-line CRL Signing,
- CRL Signing (86)

The subscription certificate issued to TSU contains the following Enhanced key usage:

- Timestamp.

## 6.2 PRIVATE KEY PROTECTION AND CONTROLS ON CRYPTOGRAPHIC COMPONENT

The QTSP must ensure safe management of private keys and must prevent the publication, copying, deletion, modification and unauthorized use.

### 6.2.1 Standard and cryptographic controls

The TSA present in the certification infrastructure, which ensures the issuance of the subscription certificates, the signing of the CRL, and the TSU components that provide the qualified Timestamp, stores their private keys within a secure device certified as follows:

- Certificate of Conformity OCSI certification ISO/IEC 15408 (Common Criteria) version 3.1 for the warranty level EAL4 +;
- FIPS 140-2 Level 3 certification.

It is specified that the HSM device used by the QSCD is included in the list of devices published by the European Commission under the title "**Compilation of member States notification on SSCDs and QSCDs**".

The QTSP protects the operation of the apparatus in a safe datacenter, accessible only by authorized personnel.

The QTSP implements a continuous monitoring aimed at ensuring compliance with the standards in force. In the event of a regulatory change as a result of a vulnerability or a strengthening of standards, the QTSP ensures compliance by implementing a maintenance or upgrade plan with respect to what is required.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 6.2.2 Private key segregation control (MofN)

The QTSP ensures the simultaneous presence of at least 2 persons operating on the HSM, with specially approved roles, during the conduct of critical security operations.

### 6.2.3 Key Escrow private key

The QTSP does not provide key escrow tools applied to the private key of your TSA, and TSU.

### 6.2.4 Backup private key

The QTSP makes secure copies of the TSA's private key, and at least one copy is kept in a different place than the one in operation.

Backup procedures are carried out in accordance with the segregation criteria specified in chap. 6.2.2.

The security measures applied to production systems are the same as those that apply to backups.

QTSP does not make copies of the private subscription keys associated with TSU.

### 6.2.5 Key storage

The QTSP does not store the private key of the respective TSA/TSU components.

### 6.2.6 Transfer of the private key to/from the cryptographic module

The private key of the respective TSA/TSU components of the QTSP are maintained securely through the protection mechanisms provided by the HSM, covered by the certifications specified in the CAP. 6.2.1.

The private key of the respective TSA/TSU components is never kept in clear.

The QTSP can export the private key outside the perimeter of the HSM only and exclusively for backup purposes.

In the case of physical transfer of the TSA private key, the QTSP ensures all the segregation and security criteria to ensure the integrity of the restore operation. The procedure is carried out under the strict observance of the product manual and the configurations envisaged by the certification targets. The segregation criteria are aimed at ensuring the eventual dispatch of the HW components of the key transport, and the secrets for the restore.

### 6.2.7 Storing the private key on the cryptographic module

The QTSP stores the private key of the respective TSA/TSU components used for the services provided, in accordance with this document, exclusively on HSM.

The technical and security aspects related to the storage of the private key are defined by the technical specifications of the product, and verified by the certification tests.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 6.2.8 Private key activation method

The private key of the respective TSA/TSU components of the QTSP must be activated in accordance with the procedures and requirements defined in the product manuals, and as specified in the certification documents.

The services associated with the keys contained in the HSM can only be activated when the latter are active. The keys that allow the activation of the apparatus, are securely guarded and protected by adequate access mechanisms.

### 6.2.9 Method of deactivating private key

The private key of the respective TSA/TSU components of the QTSP must be deactivated in accordance with the procedures and requirements defined in the product manuals, and as specified in the certification documents.

In particular, the key can be disabled:

- When operators implement the key deactivation procedure;
- When the electricity supply is interrupted;
- When the device goes into error;

### 6.2.10 Method of destruction of the private key

#### *TSA Private Keys*

The TSA key of the QTSP can be cancelled in accordance with the procedures specified in the HSM user manual, and as specified in the certification documents. The procedures must ensure that the private key so deleted cannot be recovered in any way.

The cancellation operation must be carried out under the control of authorized operators and consistent with the segregation criteria specified in chapter 6.2.2.

Each backup copy of the private key must be destroyed in accordance with the procedures specified in the HSM user manual, and as specified in the certification documents. This procedure should prevent the possibility of retrieving the private key.

#### *TSU Private Keys*

The private subscription key can be deleted in accordance with the procedures specified in the HSM user's manual, and as specified in the certification documents.

### 6.2.11 Cryptographic module evaluation

The evaluation of the certifications associated with the cryptographic module used by the QTSP, are compatible with what is specified in Chapter 6.2.1.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 6.3 OTHER ASPECTS OF KEY MANAGEMENT

### 6.3.1 Public key storage

The QTSP publishes on the archive each certificate issued by its own TSA.

### 6.3.2 Validity of the certificate and keys

#### *TSA certificates and keys*

The validity period of the TSA certificate of the QTSP, and its key pair, is 25 years. The validity period of the certificate and its keys shall in no case be greater than the validity of the algorithms used as determined by the authorities concerned.

#### *TSU certificates and keys*

The validity of the subscription certificate issued to the TSU components:

- It is valid for no more than 3 years, with the renewal of keys within a maximum limit of 3 months, in compliance with the Prime Ministerial Decree of 22 February 2013 [24];
- It must not in any case be greater than the validity of the algorithms used as determined by the authorities concerned;
- It must not in any case be greater than the validity of the TSA certificate of the QTSP that issued it.

## 6.4 ACTIVATION DATA

### 6.4.1 Activation data generation and installation

The private key of the respective TSA/TSU components is protected in accordance with the procedures specified in the HSM user manual, and as specified in the certification documents.

### 6.4.2 Activation data protection

The QTSP defines internal measures to ensure that private key activation data is protected by authentication and authorization mechanisms, in order to ensure that only appointed personnel can access it.

## 6.5 COMPUTER SECURITY CONTROLS

### 6.5.1 Specific technical security requirements on IT system

Configuration, maintenance or consulting on IT systems of QTSP, is performed by ensuring the following requirements:

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- The user's identity is verified before access to the system or application;
- That roles are assigned to users in order to ensure that they have appropriate permissions;
- Whether registered security relevant log events that are subsequently stored in accordance With the rules in force, with specific reference to the contents in the standard EN 319 421 [25] Chapter 7.12;
- That critical processes of QTSP are protected by adequate network policies, in order to prevent unauthorized access;
- That there are adequate recovery systems to ensure business continuity as a result of malfunctioning of the primary systems.

### 6.5.2 Assessment of IT system security

The technical security controls applied to the IT systems involved in the internal processes of the QTSP, provide for certification coverage conforming to the ISO 27001 standard.

## 6.6 LIFE CYCLE OF ROADWORTHINESS TEST

### 6.6.1 Control of development system

The QTSP, in its systems, adopts commercial-type solutions. These solutions are not used for any other purpose than those envisaged for the certification activity of Lottomatica Holding S.r.l. QTSP. Lottomatica Holding S.r.l. also adopts prevention tools that can protect its systems from executing dangerous code. The search for dangerous code is carried out on a continuous basis, through internal security assessments.

The QTSP uses adequate and up-to-date personnel for the installation or maintenance of its SW/HW systems.

### 6.6.2 Security management controls

The QTSP ensures that the programs, or security patches, are installed in the correct version and that they do not contain any unauthorized modifications.

Lottomatica Holding S.r.l. defines, applies and verifies criteria and procedures for the planning, safe development, testing, acceptance and operational management of ICT systems.

The technical areas of Lottomatica Holding S.r.l.:

- Monitor the use of resources by ensuring, through appropriate projections and estimates, the current and future performance of ICT systems. These estimates address the retrieval of new resources to ensure future operations;
- In collaboration with areas requiring the development or acquisition of new systems or features, establish acceptance criteria, including specific security criteria, for new ICT systems, for upgrades and for new versions; These criteria support and guide testing tests
- Perform a code review activity (static code analysis) aimed at identifying vulnerabilities within the source code followed by any remediation activities with code modification;
- Perform systems testing, in a dedicated test environment using data that is appropriately selected and separated from those used in production environments.
- Perform dynamic analysis of software reactions to various input types for Web applications;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Define and evaluate the acceptance criteria of ICT systems based on the requirements and resources used, recovery procedures, emergency measures, business continuity conditions and impact analysis
- Perform patch management activities, as a result of vulnerability detection, patch release communication from software vendors or major accredited sector bodies, in order to mitigate, where necessary, system vulnerabilities.
- Manage the activities of change management and capacity management in order to ensure that the application of the necessary changes on ICT environments take due account of the potential risks introduced by the changes, ensure the availability/performance of the systems and network and security apparatus used to identify any problems on such systems or apparatus, at the same time, defining the relevant corrective actions, and optimize the physical resources of systems and apparatus.

The production environments are suitably separated and isolated from the environments dedicated to testing and testing. This separation is carried out on a physical, logical, procedural and organizational level through a clear attribution of responsibilities.

### 6.6.3 Lyfe cycle of security controls

The QTSP ensures the protection of security components in their life cycle. In particular, as regards the HSM:

- Verifies scope certifications;
- When receiving apparatus, they are not in "tampered" status;
- That the tamper protection is assured during the operation;
- Continue to be observed as contained in the user manual or in the certification documents;
- That the private keys are deleted from devices not in use, in a way that the restore is not possible.

## 6.7 NETWORK SECURITY CHECKS

In order to ensure a level of security of the Lottomatica Holding S.r.l. corporate network:

- Establishes responsibilities and procedures for the management of network equipment;
- Implements controls to ensure the security of data transit through the network and protection from unauthorized access to connected services. This objective is achieved through the logical division in separate networks and the proper use of advanced security management tools (eg. Firewalls, traffic monitoring probes,...);
- Defines and implements specific controls to safeguard the integrity and confidentiality of critical data in transit on the public network and in particular on wireless networks;
- Enables monitoring and logging capabilities to control and record anomalies. Network management activities are coordinated both to optimize business services, and to ensure that controls are effectively applied across the entire infrastructure;
- Configure the firewall and router devices appropriately so that only the ports strictly necessary for the operating services are left open.
- Adopts rules for assigning privileges to personnel accessing the configuration and diagnostic ports. The configuration of perimeter logic security devices is subject to periodic revision and update activities;
- Adopts principles of segregation of networks according to the following criteria:
  - A logical segregation between the network offering corporate services and the network hosting the QTSP systems;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- A logical segregation of departmental type within each of the two subnets according to the types of service offered.
  - Use of secure channels, or encrypted information exchange tools to protect communications between physically separate networks using the Internet as a means of communication (https over internet or encrypted VPN tunnels);
  - Ensures that devices that manage high-critical data or infrastructure reside on dedicated hardware, and in particular do not live with other services that can compromise their security;
  - The test and operating devices are correctly sized according to the specifications of the services to be supplied and the amount of data/traffic that will be handled;
- The networks are physically safe with regard to cabling (electrical and data transport), placement of machines and presence of uninterruptible power supply units.

## 6.8 TIME-STAMPING

Lottomatica Holding S.r.l. guarantees the integrity and protection of log files, by managing them in a log management system within the ICT infrastructure.

Furthermore, pursuant to article 41, paragraph 3 of the DPCM of 22 February 2013 [24] The time assigned to time references must correspond to the UTC (IEN) timescale, referred to in the decree of the Minister of Industry, Trade and Crafts 30 November 1993, No. 591, with a difference not exceeding one minute.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 7 CERTIFICATES, CRL, AND OCSP PROFILES

### 7.1 CERTIFICATE PROFILE

The QTSP has a TSA root for issuing certificates for TSU Timestamp Service, and related certification services.

The TSA certificate and the TSU component certificate are compatible with the following standards:

- ITU X. 509 information technology-Open Systems Interconnection-The directory: Public key and attribute certificate frameworks [19];
- RFC 5280 [16];
- RFC 6818 [17];
- ETSI en 319 421 [25];
- ETSI en 319 412-1 [5];
- ETSI en 319 412-2 [6];
- ETSI en 319 412-5 [9];

#### 7.1.1 Specification X509

The X. 509 standard adopted for root CA and subscription certificates are of type "V3".

The QTSP uses the following basic extensions:

- version  
The certificate is compatible with the version "V3"
- Serial Number  
The application of the serial Number field is in accordance with what is specified in the document en 319 412 01 v 1.1.1 [5]
- Algorithm identifier  
The OID of the algorithm used for certificate certification;
- signature  
Electronic signature performed by QTSP for certificate certification, performed as specified in the "Algorithm identifier" field;
- Issuer  
The distinguished name of the entity that issued the certificate.
- Valid from & valid to  
The validity period of the certificate. The time is recorded according to the UTC reference in accordance with RFC 5280.
- subject  
The unique identifier of the subject.
- Subject Public Key value  
The public key associated with the subject.

#### 7.1.2 Certificate extensions

The QTSP uses certificate extensions that are compatible with the X. 509 standard [19].

The following are the specific requirements regarding the above extensions:

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

#### Root TSA Certificate

Nome	Valore
Version	Version 3
Serial Number	(attribuite runtime)
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	DN del QTSP: <b>countryName</b> : "IT" <b>organizationName</b> : "Lottomatica Holding S.r.l." <b>organizationIdentifier</b> : "VATIT-02611940038" <b>commonName</b> : "Lottomatica EU Qualified Timestamp Authority"
Validity	25 years (expiry 25 years from the date of issue)
Subject	come Issuer
SubjectPublicKeyInfo	Public key 4096 bit Algorithm used: RSA
<b>Estensioni</b>	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critical)	Subject Type: CA Path Length Constraint: 0
KeyUsage (critical)	Certificate Signing, CRL Signing, Offline CRL Signing (06)
Authority Information Access	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Certificate Policies (non critico)	OID della policy: 1.3.76.49 Cp: URL: <a href="http://ca.firmadigitale.lottomaticaitalia.it/documenti">http://ca.firmadigitale.lottomaticaitalia.it/documenti</a>
crlDistributionPoint (non critico)	<a href="http://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl">http://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl</a>

#### TSU Certificate

Nome	Valore
Version	Version 3
Serial Number	(Attribuite runtime)
Signature Algorithm	sha256, RSA
Issuer	<b>countryName</b> : "IT" <b>organizationName</b> : "Lottomatica Holding S.r.l. " <b>organizationIdentifier</b> : "VATIT-02611940038" <b>commonName</b> : "Lottomatica EU Qualified Timestamp Authority"
ValiditY	3 years
Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier)	C = "IT" O = "Lottomatica Holding S.r.l." organizationIdentifier : "VATIT-02611940038" CN = TSU <id tsu>
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm used: RSA

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

Nome	Valore
<b>Estensioni</b>	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5)	qcStatements-5 QcEuPDS (0.4.0.1862.1.5) <a href="https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtsptsapds2020.pdf">https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtsptsapds2020.pdf</a>
enhancedKeyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)
KeyUsage (critical)	Digital Signature
Authority Information Access  REGULATION (UE) N. 910/2014 ANNEX I, h)	Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: <a href="https://ca.firmadigitale.lottomaticaitalia.it/strumenti/TSAH2020.crt">https://ca.firmadigitale.lottomaticaitalia.it/strumenti/TSAH2020.crt</a>
Certificate Policies (not critical) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	OID della policy 0.4.0.2023.1.1 <a href="https://ca.firmadigitale.lottomaticaitalia.it/documenti">https://ca.firmadigitale.lottomaticaitalia.it/documenti</a>
crlDistributionPoint (not critical)	<a href="https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl">https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl</a>

#### 7.1.2.1 Continuity management of Lottomatica S.p.A. certificates

Lottomatica Holding s.r.l. takes charge of the management of the Lottomatica S.p.A. CAs guaranteeing the continuity of all the services related to the old CA, thus not disregarding the following links:

- Ocsp – <https://ocsp.ca.firmadigitale.lottomaticaitalia.it>
- Verifier – <https://ver.ca.firmadigitale.lottomaticaitalia.it>
- Documents – <https://ca.firmadigitale.lottomaticaitalia.it/documenti>
- CRL TSA – <https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrl.crl>
- CRL CA – <https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrl.crl>
- PDS TSA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtsptsapds.pdf>
- PDS CA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapds.pdf>

that will remain available and usable even after the company change and relative change of CA.

All certificates issued by Lottomatica S.p.A. are to be considered valid in continuity with Lottomatica Holding S.r.l. also with respect to the current limitations of use.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 7.1.2.2 Continuity management of Lottomatica Holding certificates following VAT change

Lottomatica Holding s.r.l. takes charge of the management of the previous CAs of Lottomatica Holding ensuring the continuity of all services related to the previous CA, thus not disposing of the links related to:

- Ocsp – <https://ocsp.ca.firmadigitale.lottomaticaitalia.it>
- Verifier – <https://ver.ca.firmadigitale.lottomaticaitalia.it>
- Documents – <https://ca.firmadigitale.lottomaticaitalia.it/documenti>
- CRL TSA – <https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh.crl>
- CRL CA – <https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh.crl>
- PDS TSA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtsptsapdsh.pdf>
- PDS CA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh.pdf>

They will remain available and usable even after the change of VAT and its CA exchange.

All certificates issued by Lottomatica Holding S.r.l. (VAT 13044331000) are to be considered valid in continuity with Lottomatica Holding S.r.l. also with respect to the current limitations of use.

### 7.1.3 Object Identifier Algorithms

The QTSP adopts the following algorithm:

- "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).

### 7.1.4 Composition of the name

The composition of the name identifying the distinguish name, is composed according to the standards specified by RFC 5280 [16], ETSI en 319 421 [25], ETSI en 319 422 [26].

The certificate must contain a unique OID of the Subject as defined in chap. 3.1.1.

The CN is specialized with a numerical progressive, and assigned to each responder (TSU1, TSU2 etc.).

### 7.1.5 Constraints on name

Not present.

### 7.1.6 Certificate Object Identifier policy

The QTSP must include in the certificates issued the certificate policy in accordance with this document, marked non-critical, and as specified in chap. 7.1.2.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

### 7.1.7 Usage of policy constraints extension

Not present.

### 7.1.8 Syntax and semantics of policy qualifiers

Specified in 7.1.2.

### 7.1.9 Semantics management for critical policy extensions

Specified in 7.1.2.

## 7.2 CRL PROFILE

### 7.2.1 Version

The QTSP releases a Certificate Revocation List (CRL) with the "V2" version, in accordance with the RFC 5280 [16] standard.

### 7.2.2 Specification of CRL Extensions

In accordance with RFC 5280 [16], the CRL issued by TSA may include the following extensions:

- Version  
The value of the field is "1".
- Signature Algorithm Identifier  
The identifier (OID) of the algorithm used to create the electronic signature certifying the CRL. The expected algorithm is "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Signature  
The electronic signature certifying CRL.
- Issuer  
The entity issuing the CRL.
- This Update  
The date of entry into force of the CRL. The value must be in accordance with the UTC standard in accordance with RFC 5280 [16].
- Next Update  
The next release of the CRL. The value must be in accordance with the UTC standard in accordance with RFC 5280 [16].
- Revoked Certificates  
The list of revoked certificate serial numbers including time.  
The list of suspended or revoked Certificates with the serial number of the Certificate and with the suspension or revocation time.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

The mandatory extensions that must be present in the CRL are:

- CRL number - not critical  
A progressive serial number identifying the single CRL

The following extension can be used by TSA

- expiredCertsOnCRL - not critical  
The TSA indicates through this extension that the expired certificates are not removed from the CRL (see section 4.10). The notation is in accordance with the X.509 specification.

The list of revoked certificates includes the following extensions:

- Reason Code - not critical  
The reason for the revocation of the certificate.  
The time reference from which the key is considered compromised.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

QTSP's work towards compliance, is under the supervision of the AgID, **Digital Italian Agency**. Compliance verification activity shall be conducted in phase QTSP certification and thereafter annually, through inspection sites at which the QTSP delivers its services.

The Audit work aims to ensure that the work of QTSP is in accordance with the regulation eIDAS [28], and compliance to the applicable national laws and specifications of services set out in this document.

The Audit work conforms to the following reference documents:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [28];
- DPCM february 22, 2013 [24];
- ETSI EN 319 403 V 2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment-Requirements for conformity assessment bodies assessing Trust Service Providers [2];
- ETSI EN 319 401 V 2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1];
- ETSI EN 319 411-1 V 1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [3];
- ETSI EN 319 411-2 v 2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing qualified certificates EU [4];
- ETSI EN 319 421-2 v1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [25].

The result of the Audit is confidential and can only be accessed by authorized persons. Lottomatica Holding S.r.l., within its qualified trust services, uses certified components.

As regards the protection of private keys, the QTSP declares that the HSM HW components are suitable for the implementation of the qualified services, as they possess the certifications specified in Chapter 6.2.1.

### 8.1 FREQUENCIES OR ASSESSMENT REQUIREMENTS

The QTSP compliance audit activity is conducted on a biennial basis with annual surveillance.

### 8.2 IDENTITY/QUALIFICATION OF ASSESSOR

The assessor must have conformity certification of trust service providers and the services they provide in the face of Regulation (EU) 910/2014 [28].

The unique body of accreditation of attestors of conformity for Italy is **Accredia**.

### 8.3 INDIPENDENCE OF THE ASSESSOR

The QTSP guarantees that the person/company performing the assessment is:

- Independent of the property and management of the QTSP;
- Has no business relationship with the QTSP.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

#### 8.4 TOPICS COVERED BY THE ASSESSMENT

The audit activity is carried out on the following areas:

- Compliance with the rules in force;
- Compliance with technical standards;
- Compliance with this document;
- Adequacy of the processes covered;
- Documentation;
- Physical security;
- Adequacy of staff;
- IT security;
- Compliance with data protection roles.

#### 8.5 ACTIONS TAKEN IN THE EVENT OF NON-COMPLIANCE

The auditor shall compile a report on the basis of the checks carried out. Any non-compliance can be handled as follows:

- Suggestions on changes to be taken into account;
- Derogations constituting a compulsory warning.

#### 8.6 COMMUNICATING THE RESULT

The auditor shall communicate the outcome of the report to the AgID certifying/confirming the state of QTSP, by issuing the certificate of Conformity for qualified trust service providers.

The QTSP CA's X. 509 certificate is published in the lists of Qualified Trust Service Providers.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 9 LEGAL ECONOMIS ASPECTS

### 9.1 RATES

The Qualified Timestamp service is provided by Lottomatica Holding S.r.l. free of charge. Therefore, the application of tariffs is not foreseen.

### 9.2 FINANCIAL LIABILITIES

Lottomatica Holding S.r.l. is responsible for the provision of services related to the activity of the QTSP. For the purposes of qualification and accreditation, in compliance with art 29 of CAD Comma 3a, Lottomatica Holding S.r.l. has a share capital of Euro 88.392.200,00.

#### 9.2.1 Insurance coverage

Lottomatica Holding S.r.l. has stipulated an insurance policy to guarantee a compensation limit of €5,000,000.00.

### 9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

The confidentiality of business-related information is managed in accordance with current legislation.

### 9.4 PROTECTION OF PERSONAL DATA

Lottomatica Holding S.r.l. has an organisational and regulatory system in place to ensure that all personal data processing is carried out in compliance with the provisions of the EU Regulation 2016/679 (hereinafter "regulation" or "GDPR") [27] and of the applicable Italian law of coordination on the protection of personal data and in full compliance with the principles of fairness and lawfulness declared in the code of ethics. [25]. This system is characterized by some important basic elements, including the following:

- Employees who have been appointed as persons in charge of processing personal data pursuant to art. 4 n. 10 of the Regulations, have received detailed instructions about the procedures and security measures to be adopted for the processing of personal data;
- The processing of personal data is carried out under the supervision of controllers, also formally appointed, who have in turn received the necessary instructions and operational indications;
- Specific company functions have the task of defining the policies for the security of information and of verifying, with the help of internal auditing functions, that they are actually applied;
- The policy system is based on the correct classification of assets. With the help of risk assessment tools, the most suitable security measures for the protection of individual assets, the definition of controls and the application of the most appropriate monitoring and verification systems are identified;
- The protection of personal data does not constitute an independent process, but it is fully integrated into the current management of the security of the company's assets;
- The physical security and the protection of the material assets of the company and the policies of management of the security incidents and the crises are defined keeping in mind the principles of protection of the personal data and the needs of protection of this data Fixed by law.

In the context of corporate security policies, technical and organizational solutions have been developed for the protection of data transmitted and stored on the network and on the company systems, including, but not limited to:

- Protection from viruses with continuous updating;
- Hardening of the systems used;
- Software distribution for automatic updating of security patches on business systems;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Tools and methodologies of vulnerability assessment and risk analysis;
- Data protection and access points to the company network (e.g. access control, authentication credentials, etc.);
- Partitioning and protection of internal networks;
- Monitoring of the network and the systems for the prevention and the contrast of the security accidents.

#### 9.4.1 Methods of protection of personal data

The purpose of this chapter is to illustrate the procedures and operational modalities adopted by the QTSP for the processing of personal data, in the conduct of its certification activity.

The personal data relating to the applicant for registration, to the certificate holder, to the third party concerned and to anyone accessing the service, are processed, stored and protected by the QTSP in accordance with the provisions of the Regulation and the applicable legislation Italian coordination on the protection of personal data and in compliance with the measures of the guarantor for the protection of personal data [27].

The terminology used in this chapter complies with that adopted by the Regulation [27]. In particular:

- The Holder of the treatment shall mean the natural or legal person, the public authority, the service or other body which, individually or together with others, determines the purpose and means of the processing of personal data;
- The Controller shall mean the natural or legal person, the public authority, the service or other body which treats personal data on behalf of the holder of the treatment;
- The Appointee shall mean the person entitled to the processing of personal data under the direct authority of the holder or manager;
- By Interested party, means the identified or identifiable natural person to whom personal data pertains (i.e. the registration applicant, the holder of certificates, or anyone who accesses the service);

In particular, the QTSP:

- Appointing, where appropriate, a responsible for the processing of the data within the company's own organization, him analytically and in writing the tasks it will have to fulfil. According to art. 28 paragraph 3 of the Regulation [27]. In particular, if designated, the controller:
  - It is identified between persons who, by experience, capacity and reliability, provide appropriate guarantee of full compliance with the existing treatment provisions, including the security profile (paragraph 2);
  - Carry out the treatment according to the instructions given by the holder, who, even through periodic checks, shall supervise the punctual observance of the provisions concerning the treatment and its instructions (paragraph 5).
- Identifies and appoints officials responsible for the processing of data (i.e. those responsible for identification and how many others will deal with the data relevant to the service), operating under the direct authority of the Service Manager, following the Instructions given;
- Appoints any external persons responsible for the processing of the data by analytically specifying the tasks in writing and carries out, also through periodical checks, checks on the punctual observance of the legal provisions and its instructions to accordance with art. 28 of Regulation.

#### Definition and identification of "personal data"

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

According to art. 4 No 1) of the Regulation [27], *personal data* shall mean "any information concerning an identified or identifiable natural person; The natural person who can be identified, directly or indirectly, with particular reference to an identifier such as the name, an identification number, location data, an on-line identifier or one or more Characteristic elements of his physical, physiological, genetic, psychic, economic, cultural or social identity; Therefore, the identification and security codes provided by the QTSP are also personal data.

Personal data, may also be, those related to the user, or, to eventual third parties and content in the information fields present on the forms and in the archives-electronic or paper-registration, revocation, exchange of records and certificates, of which to the relevant chapters of this document. In order to ensure proper treatment, the security measures prepared by the QTSP and analytically described in the security plan shall be carried out in accordance with the provisions of the Regulation [27] and the applicable Italian co-ordination legislation on the protection of personal data.

### Protection and rights of stakeholders

As regards the processing of personal data, the QTSP guarantees the protection of the rights of the persons concerned in compliance with the Regulations, in particular:

- The interested parties are given the necessary information according to art. 13 of the Regulation (such as the holder, the modalities and aims of the treatment, the scope of communication and dissemination, and all the rights provided for in articles 15 to 22 of the Regulation, where applicable, and in particular: the right of access to Data (art. 15), the right to rectify its data (art. 16), the right to cancellation/right to oblivion (art. 17), the right to limitation of treatment (art. 18), the right to data portability (art. 20), the right of opposition (art. 21) , the right not to be subjected to automated decision-making for individuals, including profiling (art. 22);
- Interested parties are required, where necessary, to consent to the processing of their personal data for one or more specific purposes within the meaning of art. 6 Paragraph 1 of the Regulation [27].

### Application of Regulation

#### General Fulfillment

From the general point of view, the QTSP:

- Predisposes, preserves and updates, in the framework of the certification activities, a Register of certificates and a register of the paper archives, containing personal data, incorporated in the data banks of the holder and Used in the management of all phases of the certification activity.

In particular, the Register of paper Archives consists of the copies of the documentation obtained during the identification phase of the RAO subscribers and the internal use subscribers. This register is kept inside a safe arranged in the area of the CTO Italy function, whose access is allowed to a small number of Lottomatica Holding S.r.l. employees authorized to perform this task. The key to the safe is kept at the Supervisory Office (24h) located inside the building of via Campo Boario 56. To get the access key to the safe, a person must be included in the list of authorized personnel and is recorded the taking charge and the return of the key.

As far as the certificate register is concerned, it is an internal function of the RA and not publicly exposed, containing all the issued certificates. The interface (Web-accessible via HTTPS) requires access credentials, and applies role-based policies, which enable the operator to access the requested data, provides search functions to facilitate the need. Certificates are physically stored on the media Database, located within the CED where the QTSP infrastructure is hosted, which is accessed exclusively by authorized personnel.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## Technical and organizational fulfillment

From a technical point of view, the QTSP, (the person responsible if appointed) through its appointees, shall take appropriate measures in relation to the registration, processing, preservation, protection of personal data, deletion/destruction, according to the Modes shown below.

### 1. Registration

- Guarantees the preservation of the technical data relating to the structure and format of the computer and paper archives containing personal data, as well as to their physical location;
- Supervises the organization and classifies of archives in a unique way, as well as their backup copies, taking care to reduce to the minimum essential copies, total or partial, of each archive according to the modalities described in the plan for the QTSP security plan. In this regard, it is clarified that, in case of events that would compromise the operational capacity of the QTSP at the main place of activity, it guarantees the availability of the register of certificates and the functionality of revocation of certificates in the course of validity, Consistent with the Business Continuity procedures within the QTSP;
- Supervises the organization and classification in a unique manner of registration, acceptance, request revocation, change of records and any other document containing personal data, taking care to minimize the necessary copies, Total or partial, of each archive according to the modalities described in the QTSP security plan.

### 2. Processing

- Check that the processing of these archives and the personal data contained therein is carried out exclusively for the purposes indicated in the information provided pursuant to art. 13 of the Regulation [27];
- Verification, depending on the type of processing, the output formats and the final destination of the data in order to guarantee its protection, as provided in the following;
- Detects the possible generation of new archives in the context of the processing phases, supervising their classification

### 3. Storage

- Supervises the classification of any archives – and the data they contain – subject to pure and simple preservation (historical and/or backup archives), reporting the duration of the preservation (including initial and final date), the nature of the support and the seat of preservation;
- Ensures that all archives belonging to temporarily blocked or suspended procedures are treated as personal data retention files;
- Ensure that the procedures for storing all documents used within the certification activity are consistent with the protection of personal data.

### 4. Deletion/Destruction

- Check the registration – possibly in an automated manner – of the deletion/destruction of individual personal data from the archives, bringing back the type of data, the archive concerned, the date of deletion/destruction, as well as the origin Cancellation/destruction (at the request of the person concerned, procedural, accidental, etc.);

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- Check the registration of the deletion/destruction of whole archives, in accordance with the procedures described in the preceding paragraph and in accordance with the provisions of the Regulation [27] and the applicable Italian law of coordination on data protection. Personal attention also to the updating of the Register of computer and paper archives.

## 5. Protection

- It protects the confidentiality of personal data by establishing the modalities of access to the computer and paper archives by the authorized entities belonging to the organization of the QTSP. In particular:
  - Classifies the access-enabled subjects according to their tasks. In particular, it is specified that the QTSP has defined and implements specific authentication credentials management policies and for the construction and use of passwords;
  - Records the data protection modalities, both with regard to the logical security of the computer archives (security software, methods of generation of the processing log, etc.) and physical (supervision of the premises, archiving of documents, management of the security copies);
  - It assures the confidentiality of the personal data contained in the different output formats of the processing phases (paper, on terminal, etc.) by establishing the necessary operating modalities, both manual and automated;
  - Supervises the internal circulation of information contained in printed matter (tabulated) or in other media;
  - Ensures distribution of output to terminal in accordance with user profiles designated by the security officer.
- Protects the integrity of the data individually considered and the archives as a whole, during all the phases of treatment, establishing the necessary operating modalities, both manual and automated;
- Guarantees the availability of data, so that the holder can fulfil the requests for consultation/verification by the interested parties under current legislation.

Further modalities for the processing of data, beyond the one provided for by the Regulation [27] and the applicable Italian law of coordination on the protection of personal data may be provided at contractual level between the QTSP and the organization, public or which requires the issuance of several certificates, on behalf of subscribers to you. In this case, these agreements are given within the agreement of purchase of the certificates by the organization itself.

### Circumstances of the release of personal data

Without prejudice to the right of the person concerned to request and obtain from the QTSP information relating to his personal data, as provided by ART. 15 of the Regulation [27], the QTSP, in carrying out its certification activities, may carry out communication and dissemination of personal data.

In particular:

- Personal data may be communicated to the judicial authority, in accordance with the provisions of current legislation;
- Special contractual agreements may provide additional recipients and forms of communication compared to the provisions of the current legislation. These communications will however be in compliance with the current legislation.

## 9.5 INTELLECTUAL PROPERTY RIGHTS

This document is the property of Lottomatica Holding S.r.l. which reserves all the rights to it.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

The holder of the certificate retains all rights to its trademarks (brand name) and its domain name. In relation to the property of other data and information the applicable laws apply.

## 9.6 DECLARATIONS AND WARRANTIES

### 9.6.1 Statements and warranties of the TSA

The QTSP is responsible for the obligations contained in this document and in the contractually supplied services to the subscribers.

The QTSP is responsible for:

- For compliance with the procedures stated in this document;
- To cover damages resulting from non-compliance with the terms and conditions of the service accepted by the Subscriber, through the covers specified in this document.

The QTSP is not responsible for:

- To cover the damage resulting from the non-compliance by the subscriber of the content of the terms and conditions of the service accepted by the subscriber.

Due to the nature and limitations of using a qualified electronic signature service, QTSP is launching a plan to improve accessibility of the service for the disabled through Web Content Accessibility solutions.

The QTSP is responsible for the obligations referred to in Art.32 of the CAD (Obligations of the Qualified Holder and Qualified Electronic Services Provider).

## 9.7 WARRANTY STATEMENTS

The QTSP excludes its responsibilities related to the following:

- Subscribers who do not respect what is contained in the terms and conditions of use of the service;
- Failure to provide information or communication obligations due to problems associated with the availability of the Internet, or any part thereof;
- Vulnerabilities or errors associated with cryptographic algorithms used for regulatory compliance.

## 9.8 LIABILITY LIMIT

Lottomatica Holding S.r.l. will not be responsible in any way for the following:

- Damage of any kind, direct and/or indirect, or prejudiced by anyone suffering from:
  - a. Communication by the holder of incomplete, false or error-containing information, for which the QTSP has not declared or is otherwise obliged to carry out specific checks and inspections;
  - b. Tampering or intervention on the service carried out by the holder or by third parties not authorized by QTSP;
  - c. Inability to use the service determined by a total or partial interruption of the call termination services or the transport of data provided by telecommunications operators, only for facts not attributable to the QTSP;
  - d. Erroneous use of identification codes by the proprietor;
  - e. Delays, interruptions, errors or malfunctions of the service not attributable to the QTSP or resulting from incorrect use of the service by the owner;
  - f. Use of the service outside current regulatory forecasts;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- g. Non-communication of information that the holder should have communicated to the QTSP and/or the person responsible under the obligations under the contract;
- h. Breach of obligations which, by virtue of the provisions of this document or by applicable law, are charged to the holder;
- i. Damages of any kind, direct or indirect, or prejudiced by any person suffering, to the extent that they could be avoided or limited by the owners through a correct use of the service.

Except in the cases provided for by applicable law, Lottomatica Holding S.r.l. shall not be liable in any way for direct and/or consequential damages (including, but not limited to, loss of profit, loss of productivity, overheads, lost earnings, loss of information and any other economic loss) suffered by the holder following during the use of the service and due to malfunction of the service not attributable to Lottomatica Holding S.r.l.

That being said, the overall liability of Lottomatica Holding S.r.l. is limited to compensation for direct damages and/or consequential and/or consequential damages in cases of fraud, guilt or negligence, within the limits of compensation provided for in chapter 9.2 and 9.2.1.

## 9.9 ALLOWANCES

The coverage of allowances associated with damages to all parties (holders, third parties concerned, and recipients) is guaranteed in this CPS to the extent specified in chapter 9.2.1.

## 9.10 SERVICE LIFE AND TERMINATION

### 9.10.1 Duration

The QTSP has the right to terminate at any time from the contract relating to the service by notifying the holder with a notice of 10 (Ten) days and, consequently, to revoke the certificates issued. The service lifetime is aligned with the duration of the certificates issued by the QTSP (ref. par. 6.3.2).

### 9.10.2 Resolution

In the event of a violation of only one of the obligations hanging over the Owner, the Service Agreement will automatically be considered automatically terminated pursuant to and for the purposes of art. 1456 c.c., with simultaneous revocation of the certificates issued, without prejudice to any eventual reparation in respect of those responsible for the violations. The Service Agreement will also be automatically terminated in all cases of revocation of the certificate. The QTSP has the right to withdraw at any time from the Service Agreement by giving notice to the Holder with a notice of 10 (ten) days and, consequently, to revoke the issued certificates.

### 9.10.3 Effects of cessation

The term "termination" refers to the process by which the QTSP ceases its activity as a Qualifying Trustee. The QTSP publishes information about the cessation procedures in the CPS, which causes the CA certificate to be revoked with all valid certificates at that time.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

## 9.11 NOTIFICATIONS AND COMMUNICATIONS WITH USERS

The QTSP communicates with its subscribers using the **QTSP Portal**.

## 9.12 CHANGES TO THE CPS

QTSP reserves the right to modify the terms included in this CPS in the event of:

- Modification of standards;
- Changes to security requirements;
- Various and eventual.

In exceptional cases, any changes can be taken with immediate effect.

### 9.12.1 Procedures for the dissemination of CPS

The QTSP reviews this document on an annual basis.

A new version is associated with the modified document, and the validity date is changed, taking into account any processes that are connected with the approval.

The new document, as amended, is also sent to the supervisory body, for Italy, the AgID.

Approved document is published on **QTSP Portal**.

The QTSP may accept comments related to the published, by the email address [firmaqualificata@pec.lottomatica.it](mailto:firmaqualificata@pec.lottomatica.it) → from **01 March 2021** the reference address will be [caigt@pec.it](mailto:caigt@pec.it)

### 9.12.2 Notification and timing mechanism

The QTSP notifies interested parties of the publication of the new version of the document, as specified in Chap. 9.12.1.

### 9.12.3 Circumstances under which it is necessary to change OID

The QTSP releases a new version in the case of integration of the OID specified in this document.

## 9.13 DISPUTE RESOLUTION

The QTSP aims at a peaceful and negotiated settlement of disputes arising from the provision of its services.

## 9.14 GOVERNMENT LAWS

The QTSP operates at all times in accordance with the Italian and European laws on the subject.

## 9.15 COMPLIANCE WITH LAWS IN FORCE

This document complies with the following regulations in force:

- 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 [28];
- DPCM 22nd February 2013;

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- ETSI en 319 401 v 2.1.1 (2016-02); Electronic signatures and infrastructures (ESI); General policy requirements for trust service providers [1];
- ETSI en 319 421 v 1.1.1 (2016-03); Electronic signatures and infrastructures (ESI); Policy and security requirements for trust service providers issue time-stamps. (Replaces ETSI TS 102 023) [25];
- ETSI en 319 422 v 1.1.1 (2016-03) [26]; Electronic signatures and infrastructures (ESI); Timestamping protocol and time-stamp to Ken profiles (replaces ETSI TS 101 861) [26];
- Regolamento EU n.2016/679 [27].

## 10 REFERENCES

- [1] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- [2] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

- [3] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [4] ETSI EN 319 411-2 v2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; (Replaces ETSI TS 101 456).
- [5] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [6] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; (Replaces ETSI TS 102 280).
- [7] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (Replaces ETSI TS 101 861).
- [8] ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for weSite B certificates.
- [9] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- [10] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [11] MSZ/ISO/IEC 15408-2002 "Information Technology - Methods and Means of a Security Evaluation Criteria for IT Security".
- [12] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- [13] IETF RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999.
- [14] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- [15] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.
- [16] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [17] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [18] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- [19] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks.
- [20] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [21] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.
- [22] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- [23] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.
- [24] DPCM 22 February 2013.
- [25] ETSI TS 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamp.
- [26] ETSI TS 319 422 V1.1.1 (2016-03) [26]; Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

	Type	REGISTRATION	Code	LTIS-05-00007/18
	Title	QTSP QUALIFIED TIMESTAMP SERVICE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Version	3.0
			Date	08/02/2021
Classification: Public				

[27] Applicable national regulation and EU Regulation No 2016/679

[28] 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.