



Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

QTSP

QUALIFIED CERTIFICATION SERVICES

CERTIFICATION PRACTICE STATEMENT E

CERTIFICATE POLICY



Title	Typology	REGISTRATION	Code	LTIS-05-00006/18
		QTSP QUALIFIED CERTIFICATION SERVICES	Revision	5.0
		- CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Date	08/02/2021

Classification: PUBLIC

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

INDEX

1	SCOPE	8
1.1	OVERALL	8
1.2	DOCUMENT NAME AND IDENTIFICATION.....	8
1.2.1	Identification Name	8
1.3	PKI PARTICIPANTS.....	10
1.3.1	Certification Authorities	11
1.3.2	Registration Authorities.....	12
1.3.3	Subscribers and Relying Parties.....	12
1.3.4	Other participants	13
1.4	USE OF THE CERTIFICATE	13
1.4.1	Allowed use of the certificate	13
1.4.2	Unauthorized use of certificate.....	15
1.5	POLICY ADMINISTRATION	15
1.5.1	Administration of the document	15
1.5.2	Responsibility of the suitability	16
1.5.3	Approval procedures	16
1.6	DEFINITION AND ACRONYMS	16
1.6.1	Definitions	16
1.6.2	Acronyms	18
2	PUBLICATION	20
2.1	REPOSITORY	20
2.2	PUBLICATION OF CERTIFICATION INFORMATION	20
2.3	PUBLICATION FREQUENCY.....	20
2.3.1	Frequency of publication of terms and conditions	20
2.3.2	Certificate publication frequency	20
2.3.3	Revocation status publication frequency	20
2.4	CHECK ON REPOSITORY ACCESS.....	20
3	IDENTIFICATION AND AUTHENTICATION.....	21
3.1	DENOMINATION	21
3.1.1	Types of Name	21
3.1.2	Identification requirements.....	22
3.1.3	Anonymous subscribers and pseudonyms	22
3.1.4	Rules for the interpretation of names.....	22
3.1.5	Uniqueness of names.....	22
3.2	VALIDATION OF THE IDENTITY.....	22
3.2.1	Methods to prove ownership of the private key	22
3.2.2	Physical token delivery processes	23
3.2.3	Authentication of an organizational entity	23
3.2.4	Authentication of an individual entity	23
3.2.5	Unverifiable subscription information	25
3.3	IDENTIFICATION AND AUTHENTICATION FOR REISSUE.....	25
3.3.1	Identification and authentication for reissuing in the case of a valid certificate	26
3.3.2	Identification and authentication for reissuing after revoked/expired certificate ...	26
3.4	IDENTIFICATION AND AUTHENTICATION FOR CERTIFICATE CHANGE REQUESTS	26

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

3.5	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS.....	26
4	CERTIFICATE LIFE CYCLE REQUIREMENTS	28
4.1	REQUEST OF A CERTIFICATE.....	28
4.1.1	Submission of the certificate request	31
4.1.2	Registration/ Enroll process and responsibility	31
4.1.3	Activation of the certificate	32
4.2	CERTIFICATE REQUEST MANAGEMENT PROCESSES	32
4.2.1	Performing identification and authentication fuctions.....	32
4.2.2	Approval or rejection.....	32
4.2.3	Execution time of the request.....	33
4.3	ISSUING THE CERTIFICATE.....	33
4.3.1	CA action during certificate issuance	34
4.3.2	Notifications to the holder about the issuing of the certificate.....	34
4.4	ACCEPTANCE OF THE CERTIFICATE	34
4.4.1	Conduct on acceptance of the certificate	34
4.4.2	Publication of the certificate by the CA.....	34
4.5	KEY PAIR AND CERTIFICATE USAGE	34
4.5.1	Subscriber private key and certificate usage	34
4.5.2	Interested parties – Public key and use of the certificate	35
4.6	REISSUE.....	35
4.6.1	Requirements for renewing the certificate.....	35
4.6.2	Submission of reissue request.....	36
4.6.3	Reissue request process.....	36
4.6.4	Registration on QTSP Platform and Authorization of the Certificate.....	36
4.6.5	Activation of the certificate	36
4.6.6	Notifications about issuing the certificate	37
4.6.7	Conduct on the acceptance of the reissue of the certificate	37
4.6.8	Publication of the renewed certificate by the CA	37
4.7	MODIFICATIONS TO THE CERTIFICATE.....	37
4.8	REVOCATION AND SUSPENSION OF THE CERTIFICATE.....	37
4.8.1	Circumstances of revocation	37
4.8.2	Submission of revocation request	38
4.8.3	Processes for revocation management.....	38
4.8.4	Grace Period request for revocation	39
4.8.5	Time within which the CA must process the request for revocation	39
4.8.6	Requirements on the control of revocation by interested parties	39
4.8.7	Frequency Issuing CRL	39
4.8.8	Maximum latency on CRL.....	39
4.8.9	Availability of OCSP service	39
4.8.10	OCPS service requirements	39
4.8.11	Special requirements on key compromise.....	39
4.9	CERTIFICATE STATUS VERIFICATION SERVICES.....	40
4.9.1	Operational features	40
4.9.2	Service availability.....	40
4.10	END OF SUBSCRIPTION	41
4.11	KEY ESCROW E RECOVERY.....	41
4.11.1	Policy and practices Key Escrow and Recovery	41
4.11.2	Encapsulation key symmetrical encryption policies recovery	41
5	FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS	42

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

5.1	PHYSICAL CONTROLS	42
5.1.1	Location site and features	42
5.1.2	Physical access	42
5.1.3	Power supply and air conditioning	43
5.1.4	Exposure to water	44
5.1.5	Prevention and fire protection	44
5.1.6	Media Storage	45
5.1.7	Provisions on the disposal of apparatus	45
5.1.8	Off-Site Backup	45
5.2	PROCEDURAL CONTROLS	45
5.2.1	Roles	45
5.2.2	Number of people required for task	46
5.2.3	Identification and authentication for roles	46
5.2.4	Roles requiring segregation	46
5.3	PERSONNEL CONTROL	46
5.3.1	Qualifications, experience and clarity of requirements	47
5.3.2	Background verification procedures	47
5.3.3	Training requirements	47
5.3.4	Update frequency	48
5.3.5	Sanctions on unauthorised shares	48
5.3.6	Requirements on consultants	48
5.3.7	Documentation provided to staff	48
5.4	AUDIT PROCEDURES	48
5.4.1	Types of events stored	49
5.4.2	Frequency of audit processes	49
5.4.3	Audit log retention period	49
5.4.4	Audit log protection	49
5.4.5	Audit log backup procedures	49
5.4.6	Audit event collection system	49
5.4.7	Notification in case of identification of suspicious events	49
5.4.8	Vulnerability Assessment	50
5.5	STORING RECORDS	50
5.6	CA KEY CHANGEOVER	50
5.7	COMPROMISE AND DISASTER RECOVERY	50
5.7.1	Incident and compromise management procedures	51
5.7.2	Computing Resources, Software, and/or corrupted data	51
5.7.3	Private key compromise procedures	51
5.7.4	Capacity of business continuity in case of disaster	52
5.8	CESSATION OF ACTIVITY	52
6	TECHNICAL SECURITY CONTROLS	53
6.1	GENERATING AND INSTALLING KEY PAIR	53
6.1.1	Generating key pair	53
6.1.2	Private key release to subscribers	53
6.1.3	Issuing the public key to the certificate	53
6.1.4	Issuing the CA public key to interested parties	54
6.1.5	Key length	54
6.1.6	Key generation parameters and quality control	54
6.1.7	Key usage purposes (see key usage field X. 509 v3)	54
6.2	PRIVATE KEY PROTECTION AND CONTROLS ON CRYPTOGRAPHIC COMPONENT	54
6.2.1	Standard and cryptographic module controls	54

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

6.2.2	Private key segregation control (MofN).....	55
6.2.3	Key Escrow private key	55
6.2.4	Key storage.....	55
6.2.5	Key storage.....	55
6.2.6	Transfer of the private key to/from the cryptographic module	55
6.2.7	Storing the private key on the cryptographic module	56
6.2.8	Private key activation method.....	56
6.2.9	Method of deactivating private key	56
6.2.10	Method of destruction of the private key.....	57
6.2.11	Cryptographic module evaluation.....	57
6.2.12	Validity of the certificate and keys	57
6.3	ACTIVATION DATA	58
6.3.1	Activation data generation and installation.....	58
6.3.2	Activation data protection	58
6.3.3	Other aspects of the activation data	58
6.4	COMPUTER SECURITY CONTROLS	58
6.4.1	Specific technical security requirements on IT system.....	58
6.4.2	Assessment of IT system security	59
6.5	LIFE CYCLE OF ROADWORTHINESS TEST	59
6.5.1	Control of development system	59
6.5.2	Security management controls.....	59
6.5.3	Life cycle of security controls.....	60
6.6	NETWORK SECURITY CHECKS	60
6.7	TIME-STAMPING	61
7	CERTIFICATE, CRL, AND OSCP PROFILES	62
7.1	CERTIFICATE PROFILE	62
7.1.1	Specification X509	62
7.1.2	Certificate extensions.....	62
7.1.2.1	Continuity management of Lottomatica S.p.A. certificates.....	75
7.1.2.2	Continuity management of Lottomatica Holding certificates following VAT change	76
7.1.3	Object Identifier algorithms	76
7.1.4	Composition of the name	76
7.1.5	Constraints on name.....	77
7.1.6	Certificate policy object identifier	77
7.1.7	Usage of policy constraints extension	77
7.1.8	Syntax and semantics of policy qualifiers	77
7.1.9	Gestione della semantica per estensioni di certificate policy critiche.....	77
7.2	CRL PROFILE.....	77
7.2.1	Version	77
7.2.2	Specifying CRL extensions.....	77
7.3	OCSP PROFILE.....	78
7.3.1	Version	78
7.3.2	OCSP extensions.....	78
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	79
8.1	FREQUENCIES OR ASSESSMENT REQUIREMENTS.....	79
8.2	IDENTITY/QUALIFICATION OF ASSESSOR	79
8.3	INDIPENDENCE OF THE ASSESSOR	79

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

8.4	TOPICS COVERED BY THE ASSESSMENT	79
8.5	ACTIONS TAKEN IN THE EVENT OF NON-COMPLIANCE	80
8.6	COMMUNICATING THE RESULT	80
9	LEGAL ECONOMIC ASPECTS	81
9.1	RATES	81
9.2	FINANCIAL LIABILITIES.....	81
9.2.1	Insurance coverage	81
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	81
9.4	PROTECTION OF PERSONAL DATA	81
9.4.1	Methods of protection of personal data	82
9.5	INTELLECTUAL PROPERTY RIGHTS	86
9.6	DECLARATIONS AND WARRANTIES	86
9.6.1	Statements and warranties of the CA	86
9.6.2	Declarations and guarantees of RA	87
9.6.3	Declarations and warranties of the subscriber	88
9.7	WARRANTY STATEMENTS.....	90
9.8	LIABILITY LIMIT.....	90
9.9	ALLOWANCES	91
9.10	SERVICE LIFE AND TERMINATION	91
9.10.1	Duration	91
9.10.2	Resolution.....	91
9.10.3	Effects of cessation.....	91
9.11	NOTIFICATIONS AND COMMUNICATIONS WITH USERS	91
9.12	CHANGES TO THE CPS	92
9.12.1	Procedures for the dissemination of CPS	92
9.12.2	Notification and timing mechanism.....	92
9.12.3	Circumstances under which it is necessary to change OID	92
9.13	DISPUTE RESOLUTION	92
9.14	GOVERNMENT LAWS	92
9.15	COMPLIANCE WITH LAWS IN FORCE	92
10	REFERENCES	94

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

1 SCOPE

This document contains the policies for issuing qualified certificates (Certificate Policy - hereinafter referred to as CP) and describe process, methodology and operating process (Certification Practice Statement –hereinafter referred to as CPS) defined for the Lottomatica Holding S.r.l. qualified trust service provider and concerning the subscription service.

This document is compatible with the requirements set out in European Regulation 910/2014 – eIDAS [27], and the activity described is compatible with the provisions for 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 changes to procedures due to legal or regulatory requirements or to optimisation of the work cycle.

Each new version of the manual annuls and replaces the previous versions, which remain applicable to certificates issued during their validity and until their expiration date.

1.1 OVERALL

The qualified signature document contains the definition of rules that specify the usability of a certificate for a community and / or class of applications with common security requirements.

The information in this document is structured to be compatible with what is included in the public specification in RFC 3647.

This document consists of 10 chapters that contain the security requirements, processes, and practices defined by the QTSP to be followed during the service delivery.

Certificates issued in accordance with this CPS have policy identifiers (OIDs) to which certificates must conform.

This document defines basic requirements for certificates with particular reference to the QTSP certificate. The way these requirements are met and the detailed descriptions of the methods mentioned in this document are included in the Certificate Practice Statement document (CPS) issued by QTSP.

1.2 DOCUMENT NAME AND IDENTIFICATION

1.2.1 Identification Name

This document is called "*QTSP Qualified Certification Services – Certification Practice Statement and Certificate Policy*" and is characterized by the document code: LTIS-05-00006/18. The version and the release level can be identified on the title page at the bottom of each page.

Certificates issued to holders are issued with the limitations of use specified in chap. 1.4.

The document is reviewed at least annually as well as the related applicability criteria.

All the Certificates 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.

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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Table 1 - Policy Lottomatica

In the table below, can be found the OID of specification of this document:

OID	Description
(1.3.76.49)	Lottomatica Holding S.r.l.
(1)	Lottomatica Holding S.r.l. Certification Authority
(2)	Documents
(1)	Public Documents
(11)	Lottomatica Holding S.r.l. Certification Services– Certification Practice Statement and Certificate Policy

Table 2 – Document Policy

For the purposes of the QTSP activity, Lottomatica Holding S.r.l. defines the following OIDs pertaining to as many types of certificates:

OID	Descrizione	Abbreviazione
(1.3.76.49)	Lottomatica Holding S.r.l.	-
(1)	Lottomatica Holding S.r.l. Certification Authority	-
(1)	Certificates	-
(1)	Public	-
(20)	Certificate of signature Qualification issued to a natural person on an HSM device – B2B - Games / Services Area	IGTCP01
(22)	Certificate of signature Qualification issued to a physical person on an HSM device for internal use - Games / Services Area	IGTCP03
(23)	Certificate of signature Qualification issued to a physical person on HSM device for Automatic Signature - Games / Services Area	IGTCP04
(24)	Certificate of signature Qualification issued to a natural person on an HSM device for Master-RAO/RAO use - Games / Services Area	IGTCP05
(25)	Certificate of signature Qualification issued to a natural person on an HSM device – B2B - Services Area	IGTCP06

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021

Classification: PUBLIC

OID	Descrizione	Abbreviazione
(26)	Certificate of signature Qualification issued to a natural person on an HSM device for Master-RAO/RAO use - Services Area	IGTCP07
(27)	Certificate of signature Qualification issued to a physical person on an HSM device for internal use - Services Area	IGTCP08
(28)	Certificate of signature Qualification issued to a physical person on HSM device for Automatic Signature - Services Area	IGTCP09
(1)	Main version	-
(0)	Sub version	-

Table 3 – Certificate Policy

The certificate policy in table 3 refers to certificates issued to natural person.

The certificate policies present in table 3, provide for the release of keys on HSM; In this sense, the QTSP:

- Ensures that the private key associated with the certificate is stored only on a safe device that complies with the certification specifications in 6.2.1;

The qualified trust service provider shall provide the identification processes, compliance with the provisions of the EU Regulation 679/2016 [25] (hereinafter "the Regulation" or also "GDPR"), described in the relevant CPS.

About this document:

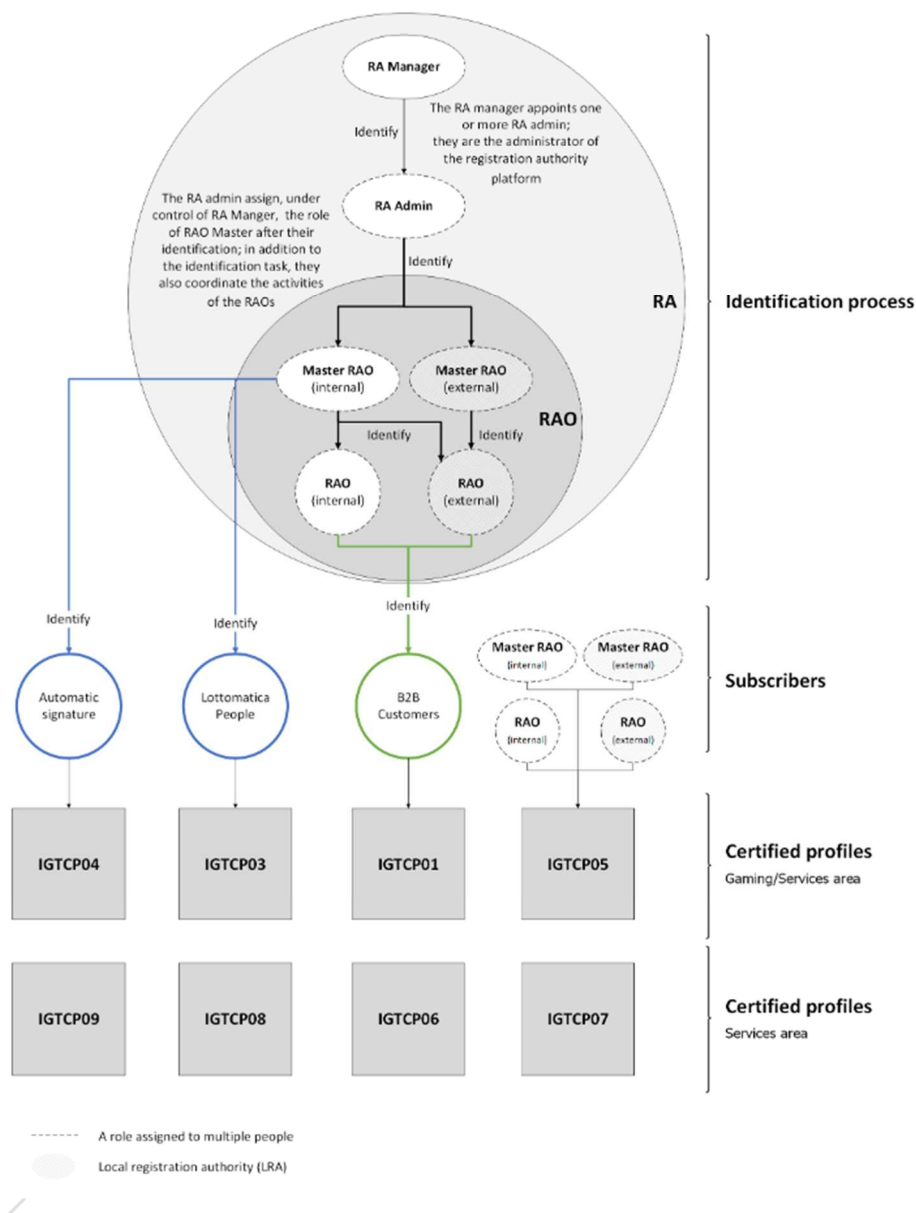
- Each certificate policy complies with the [QCP-n-qscd] policy defined in the standard [4].

1.3 PKI PARTICIPANTS

Below is a summary scheme that wants to briefly describe the organization of the registration authority (RA) for the purposes of the identification process, the subscribers and the profiles of certificates issued.

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC



1.3.1 Certification Authorities

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

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Lottomatica Holding S.r.l. is a qualified trust service provider (QTSP), qualified according to the European 910/2014 regulation in force since 1 July 2016 [27], and adhering to the provisions of Chapter 8.

1.3.2 Registration Authorities

The Registration Authority is a component of QTSP, which carries out the identification and registration of subscribers. The QTSP is in all cases fully responsible for the correct operation of the Registration Authority.

The QTSP can make use of external personnel to identify certified applicants, as defined in chapter 1.3.3

The functioning of the Registration Authority complies with the requirements described in this CP CPS. The tasks related to RA's services are:

- The identification of the Subscriber or the Applicant;
- Recording of the Subject's data;
- The forwarding of the Subject's data to the CA systems;
- The collection of the qualified certificate request;
- Collect requests for revocation / suspension, reissue or renewal of certificates;
- The activation of the certification procedure of the public key.

1.3.3 Subscribers and Relying Parties

Subscribers are end users who benefit from the service. The subject is the natural person, whose data are indicated on the certificate.

In the case of a certificate for qualified electronic signature purposes, the subject is the signatory. For the purposes of the limitations set out in Chapter 1.4, the following subscribers are defined grouped into four categories:

1. **B2B:** Users belonging to the business channel (following user B2B); these are individuals, legal representatives of points of sale, equipped with the qualified electronic signature for the subscription of contractual documents connected with activities attributable or conveyed by Lottomatica Holding S.r.l and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A;
2. **RAO Operators:** (RA Admin, Internal Master-RAO, External Master-RAO, Internal RAO and External RAO): These are natural persons delegated by Lottomatica Holding S.r.l. to operate the identification and Request registration/registration of subscribers; In particular:
 - a. **RA Admin:** they have the task of identifying the Master-RAO, registering on the QTSP platform the subscribers (Master-RAO, RAO, Internal User, Automatic Signature User) and coordinating the activities, under control of RA Manager, of the other RAO as well as managing the QTSP platform; it is not mandatory to issue a certificate for this subscriber. With the supervision of the RA Manager, can proceed with the registration of another RA Admin.
 - b. **Master-RAO:**
Internal Master-RAO have the task of identifying and request registration of internal RAO and external RAO, of subjects for automatic signing and Lottomatica

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

staff (employees and collaborators); they can use the qualified signature certificate to countersign the registration requests of the subjects they identify.

External Master-RAO: have the task of identifying and request registration of external RAO; they can use the qualified signature certificate to countersign the registration requests of the subjects they identify.

- c. **Internal RAO and External RAO:** they are subjects who have signed a specific contract/appointment and have the task of identifying and registering B2B subscribers; use the qualified signature certificate to countersign the registration requests of the subjects they identify;

3. **Lottomatica People:** Employees or collaborators of Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A (hereinafter Internal User)
4. **Automatic Signature:** Employees or collaborators of Lottomatica Holding S.r.l and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A certificate holders for Automatic Signature (hereinafter Automatic Signature User);

The relationship between QTSP and Subscribers is governed by specific documents governing the terms and conditions, signed by the holders to the release of the service as specified in chapter 9.6.3.

The external actors Master-RAO and RAO are part of the company / organizations with which a specific contract is signed, where together with this document are registered, responsibilities and methods of supervision and control (for example periodic audits) by the QTSP.
Internal RAOs are Lottomatica agents.

The identification and appointment of RAO operators takes place according to the directives and / or internal procedure of the QTSP.

The interested parties are the subjects who want to rely on the information required in the digital certificate for the verification of the documents digitally signed by the subscribers.

1.3.4 Other participants

Not defined.

1.4 USE OF THE CERTIFICATE

The certified usability area is determined by what is contained in the certificate extensions itself. Limitations of use are also specified within this document.

1.4.1 Allowed use of the certificate

The certificates are issued with the use restrictions listed in two languages as stated below.

Certificate of the Subscriber B2B (IGTCP01)

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo

Certificate of the Subscriber Internal User (IGTCP03)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo.

Certificate of the Subscriber Automatic Signature User (IGTCP04)

The certificate to which IGTCP04 is issued with the limitations of use in double language as specified below:

- The certificate may only be used for unattended/automatic digital signature;
- Il presente certificato è valido solo per firme apposte con procedura automatica.

Certificate of the Subscriber Master-RAO, RAO (IGTCP05)

- The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued;
- Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato.

Certificate of the Subscriber B2B (IGTCP06)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo.

Certificate of the Subscriber Master-RAO, RAO (IGTCP07)

- The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued;
- Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Certificate of the Subscriber Internal User (IGTCP08)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo

Certificate of the Subscriber Automatic Signature User (IGTCP09)

The certificate to which IGTCP09 is issued with the limitations of use in double language as specified below:

- The certificate may only be used for unattended/automatic digital signature;
- Il presente certificato è valido solo per firme apposte con procedura automatica.

1.4.2 Unauthorized use of certificate

QTSP Certificate

The Lottomatica Holding S.r.l. root certificate and its private key cannot be used before the actual publication in the Trust List of qualified certifiers published by AgID.

User Certificate

It is not permitted to use the certificate issued, and its private keys, for purposes other than that specified in 1.4.1.

1.5 POLICY ADMINISTRATION

1.5.1 Administration of the document

The staff data that administers this Certificate Policy 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
Fax	-

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Email	firmaqualificata@pec.lottomatica.it → from 01 March 2021 the reference address will be caigt@pec.it
-------	---

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 Italy Agency).

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

1.5.3 Approval procedures

Where provided for or in the face of amendment to the regulations, the QTSP shall apply the review and approval criteria of this CPS in accordance with the internal procedures for revising and approving the document, and in accordance with the specified in 9.12.

In particular, this document is subject to a review process, at least annually, revised by the managers of the organizational structure of the digital signature service and changes made are subject to the final approval of the CTO.

1.6 DEFINITION AND ACRONYMS

1.6.1 Definitions

From the European Regulation 910-2014 eIDAS [27], Art.3:

- (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(1) of Directive 2014/24/EU of the European Parliament and of the Council;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- (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;
- (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;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- (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.

1.6.2 Acronymis

AgID	Agenzia per l'Italia Digitale: Supervisory authority on QTSP
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale
CRL	Certificate Revocation List
HA	High Availability
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
LIS	Lottomatica Italia Servizi S.p.A.
OCSP	Online Certificate Protocol Status
OID	Object Identifier
OTP	One Time Password
PIN	Personal Identification Number
PdV	Point of Sales
PKI	PKI Public Key Infrastructure
PUK	Personal Unlock Key
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
MRAO	Master Registration Authority
RAO	Registration Authority Officer

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

RA Registration Authority
 RAA Registration Authority Administrator
 SN Serial Number
 SSL Secure Socket Layer
 TSA Time Stamp Authority
 TSU Time Stamp Unit
 VPN Virtual Private Network
 WS Web Service

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			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 its service is based.

Certificates, documentation and CRLs are published and available 24 hours a day, 7 days a week.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

CA Certificate is available on the QTSP Portal:

<https://ca.firmadigitale.lottomaticaitalia.it/RAweb/Strumenti/Software.do>

The CA publishes at least the following documentation on its website:

- Certification Practice Statement (CPS);
- PKI Disclosure Statement;
- Certifications;
- CRLs;
- Forms.

2.3 PUBLICATION FREQUENCY

2.3.1 Frequency of publication of terms and conditions

This document and the annexed documentation are published in the manner described in the paragraph for each update.

2.3.2 Certificate publication frequency

The QTSP publishes the CA root certificate before the startup. The QTSP does not publish the subscriber's certificate.

2.3.3 Revocation status publication frequency

The state related to certificates issued to subscribers by the QTSP, must be immediately available as required for the OCSP service.

Information about the status of the revoked certificates shall be published in the certificate repository, within the revocation list (CRL). Updating the revocation list is in accordance with what is specified in chap. 4.8.7.

2.4 CHECK ON REPOSITORY ACCESS

The published information is modified or deleted only and exclusively by QTSP. The QTSP also ensures controls aimed at preventing unauthorized modifications to the aforementioned repository through various protection mechanisms.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021

Classification: PUBLIC

3 IDENTIFICATION AND AUTHENTICATION

3.1 DENOMINATION

This Chapter establishes the requirements of the data indicated in the certificate issued to the subscribers, in accordance with this document.

3.1.1 Types of Name

This document requires the specification of the Subject field consistent with the following:

- Common Name (CN) – OID: 2.5.4.3 The name of the Subject;
The Common Name field specifies the name of a physical person.
- Surname – OID: 2.5.4.4 – Surname of the natural person
This field must be the last name of the Subject.
- Given name – OID: 2.5.4.42 – The name of the natural person.
The Subject name must be specified in this field.
- Pseudonym – OID: 2.5.4.65 pseudonym of the Subject.
The pseudonym of the Subject can be specified in this field.
The possibility to use a pseudonym is managed by law.
- Serial number – OID: 2.5.4.5 Unique identifier of the Subject.
This field specifies a unique reference that is associated with a Subject's tax code. In compliance with the specified in en 319 412 01 v 1.1.1, the SubjectDN of the holder includes the SerialNumber field specified as follows:
 - **"TIN": a unique identifier field associated with the person; the tax code of the holder;**
 - **"IT": ISO 3166 encoding of country code for Italy;**
 - **"-": Character 0x2d (ASCII)**
 - **Identification: The value of the owner's tax code;**
- Organization – OID: 2.5.4.10 The name of the organization
- Organization identifier – OID: 2.5.4.97 – Organization ID.
Normally this field contains a numeric identifier associated with the organization, such as the VAT.
- Organizational unit (OU) – OID: 2.5.4.11 – The name of the OU.
This field can specify the name of an organizational unit that belongs to the organization. The "ou" field can be specified only if the "O", "L", and "C" fields are present.
- Country (c) – OID: 2.5.4.6 – Country ID.
The field includes the two-letter code of the country to which the organization belongs. For Italy This field has value "it"
- Locality name (L) – OID: 2.5.4.7 – Name of the location
For an organization, the field expresses the detail of where the location is located. In the case of a certificate that is not associated with an organization, the field is not used.
- DN Qualifier – OID: 2.5.4.46 – attribute DN Qualifier specifies disambiguation information to add to DN Certificate.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

3.1.2 Identification requirements

The acknowledgement of the Subscriber must take place through the verification of the validity of the identity documents provided by the holder and verifying the operation of registration of the master data reported therein.

The identity validation process is specified in 3.2.

3.1.3 Anonymous subscribers and pseudonyms

Lottomatica Holding S.r.l. releases qualified certificates to holders using data contained in personal document provided by the holders.

3.1.4 Rules for the interpretation of names

See chapter 3.1.2.

3.1.5 Uniqueness of names

The subject must be uniquely identifiable within the QTSP systems. In order to address the requirement, the holder's personal data is accompanied by a serial Number as specified in chapter 3.1.1.

The uniqueness of the name must comply with those specified in document EN 319412p02 v 2.1.1 cap 4.2.4.

Disputes related to the name

The QTSP, when registering subscribers, verifies the credentials provided by the Subscriber that must be included in the certificate. The subscriber confirms the data through explicit consent (see Chapter 9.6.2).

The QTSP reserves the right to revoke the certificate in the case of illegal use of names or data.

3.2 VALIDATION OF THE IDENTITY

The following paragraph describes how to verify the identity for the different types of certificates. The QTSP stores all information provided in the Subscriber identification phase, and in particular the identification number and expiration of the ID document.

3.2.1 Methods to prove ownership of the private key

Before issuing a certificate, the QTSP must ensure and verify that the applicant has exclusive control of the private key corresponding to the public key of the certificate.

At the time of registration, the subscriber is associated with a mobile phone, assigned a Token device if provided, and delivered secret codes for the activation/use of the service via the owner's private email or phone number specified by the owner himself during request/registration. The possession of the private key is proven through a dual authentication mechanism provided through 1) password/PIN provided to the holder by the mode described above or chosen by the Owner; 2) Thanks to the

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

technological performance of the network GSM, and a system of OTP (One Time Password): The QTSP verifies the identity of the subscriber making sure that he is using exactly the mobile phone (or physical token) users that he stated at the time of his registration. To this end, the Subscriber receives an OTP numeric code that is used for verifications as the second authentication factor via mobile.

3.2.2 Physical token delivery processes

Delivery processes of physical token devices

QTSP implements internal procedures in order to assign to the subscriber at the time of registration, or subsequently, the physical Token for the generation of OTP codes for the use of signature services. QTSP delivers the physical Tokens through its offices, registering the delivery, and associating the unique serial number of the OTP Token to the user. The physical token for the generation of OTP codes for the use of signature services can be alternatively sent by registered letter in a sealed envelope to the address indicated during the identification phase. In the latter case, the devices are released inactive, and before their use, the authorization procedure must be carried out, which includes:

- Login with your credentials to the URL: <https://ca.firmadigitale.lottomaticaitalia.it/RAweb>
- Access to "Token-Queries" section and perform the OTP device enabling procedure by following the instructions provided.

QTSP registers on the Registration Authority system all the information necessary for the correct activation of the device.

3.2.3 Authentication of an organizational entity

The QTSP issue certificates of electronic signatures qualified exclusively to natural persons.

3.2.4 Authentication of an individual entity

The process of verifying the identity associated with the issuance of a qualified electronic signature certificate, in accordance with article 24 of the 910/2014 Regulation (eIDAS) [27], is ensured through the concrete presence of the natural person or through prior knowledge based on what is specified in paragraphs 3 and 4 of this document.

RA Admin, Master-RAO, RAO, Lottomatica People and Automatic Signature identification mode

The process involves de visu recognition. Below is a table that identifies, for the different types of subscribers, the subjects who can carry out the identification and validation of the identity:

Subscribers	Identified by
RA Admin	RA Manager
Internal/External Master-RAO	RA Admin
Internal RAO	Internal Master-RAO
External RAO	Internal/External Master-RAO

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Automatic Signature	Internal Master-RAO
Lottomatica People	Internal Master-RAO

The process involves the following activities:

- Identification through identity documents in state of validity;
- Master data collection and verification of compliance;
- Fill specific identification / appointment form;

If the subject is successfully identified, it is possible to proceed by checking the training skills if required for the role.

If the subscriber "Lottomatica People" type is an employee of Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A. and the subject that identifies him is a Master-RAO who works within the HR function of Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A., in this context, the user has already been subject to procedures aimed at identification in fulfillment of the stipulation of the employment / collaboration contract with Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A. The data relating to the Identity of the Holder are therefore acquired, verified and kept up to date as part of the activities normally carried out by the Human Resources Function and the relevant administrative offices.

All resources (Company Employees) are therefore identified in the hiring processes and registered within the Human Resources Management System (SAP-HCM: Master Registry System of Employees). Furthermore, each new hiring is communicated by HR through a mail flow to the IT functions that carry out specific support activities, such as: the Security Function, the Office Automation Function and Trusted Services.

In addition to being registered in the DB-HR, the Employees are included in the company Active Directory which manages a unique "identification" for each identity, which allows access to company systems and devices such as PCs and e-mails; the company email address or mobile number are therefore entered in the Active Directory.

In any case, before sending the certificate request, according to the procedures described in the paragraph. 4.1, the Master-RAO who works within the HR function asks the Employee a copy of a valid identity document (front and back), tax code (front and back) and mobile number.

B2B identification mode

Subscribers	Identified by
B2B	Internal/External RAO

De visu identification is carried out as follows

- RAO requires the B2B user the Tax Code, a valid identity document, a mobile number and an e-mail address;
- Make "de visu" recognition of the B2B user by verifying the validity of the document and the actual correspondence of the data with the tax code;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- Acquires, by entering them via terminal, the data of the identity document indicated (document type, document number, document issuer, document issue date, document expiration date, image of the document), e-mail and mobile phone.

The B2B user, as a legal representative of a PdV (Point of Sales), is subject to further checks aimed at accepting its requirements to establish a contractual relationship, including:

- Checks on the goodness of the provided personal data;
- Verification of B2B presence in anti-money laundering (AML) and counterterrorism;
- Chamber of commerce registration.
- Credit checks.

For the purpose of issuing a certificate from the Reseller Portal in the manner described in par. 4.1, if the B2B has contractual relationships already in place with Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A, the B2B user appears to have already been subject to procedures aimed at identifying in compliance with the sector regulations / laws (eg AML) and the verification of the possession of the requisites required by company standards (eg Credit).

The process of activating a Point of Sale, involves the carrying out, as a preventive measure, of checks aimed at verifying the possession of the requisites of respectability, integrity and solvency on the part of the same, as well as a due diligence on the connected natural persons.

In particular, the Point of Sale is automatically subjected to chamber inspections, as well as reputational checks on open sources (Worldcheck). The outcome of these checks allows attributing to the Point of Sales a Compliance-AML risk score, based on specific rules and criteria defined in line with Legislative Decree 231/07 (geographical criteria, type of activity performed, presence in the lists, ...).

With reference to the continuous monitoring of the continuation of reputational requirements, it is first of all emphasized that, when Lottomatica Holding S.r.l. becomes aware of prejudicial events (seizures, other precautionary measures, negative news from the press, ...), a process of reviewing the relationship with the interested operator is activated which leads to the execution of an investigation, based on which the management decide the appropriate actions to be taken.

Lottomatica Holding S.r.l. adopts an IT solution aimed at automating this monitoring process. In particular, through this solution, the Points of Sale database is subject to reputational and compliance scoring, through the use of decision tables based on the principles of risk approach of Legislative Decree 231/07. Furthermore, the monitoring implemented foresees that the networks of Lottomatica Holding S.r.l. is subject daily to both chamber of commerce checks (aimed at acquiring any personal and corporate updates) and to "compliance" analysis (aimed at intercepting possible changes in the risk profile and any negative news in terms of reputation).

3.2.5 Unverifiable subscription information

Please refer to Chapter 3.1.3.

3.3 IDENTIFICATION AND AUTHENTICATION FOR REISSUE

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

The reissuing of the certificate is the process in which the QTSP releases a new certificate, in place of the previous one, for contractual needs or to guarantee the continuity of its activities and services where:

- Are arising limits of validity;
- For the revocation of the previous certificate;
- For variation of one of the information (for example, one of the data of the certificate's subject, mobile number, e-mail) connected with the certificate or with the use of the signature.

For the B2B subscriber, the reissue of the certificate takes place only in the event of a change in one of the data of the subject of the certificate, mobile number, e-mail while for all other cases, a reissue is not carried out but a revocation is carried out by the QTSP.

In the event of reissue, the QTSP always verifies the existence and validity of the certificates of the holder.

3.3.1 Identification and authentication for reissuing in the case of a valid certificate

This method is performed if the certificate is valid at the time of the reissue request and if the reissue operations can be completed before its expiration date.

If the subscriber's information is valid and sent to the CA / RA no later than 39 months before, it can be used for validation, otherwise the subscriber must send/provide it again.

For the B2B subscriber, if the reissue request occurs due to a change in at least one of the following data:

- First name;
- Surname;
- Tax Code;
- E-mail;
- Mobile phone.

Proceed with the reissue in the same way as the first release.

3.3.2 Identification and authentication for reissuing after revoked/expired certificate

The reissue of the certificate following for revocation/expiration, provides as specified in 3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR CERTIFICATE CHANGE REQUESTS

As specified in 3.3

3.5 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The QTSP processes the request for revocation of the signature certificate. Requests can be forwarded via accessible functionality from the Linked Site on the Certicator Portal, subject to the subscriber authentication.

Authentication mechanisms include both the use of access credentials.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Requests can also be sent through the contact details of the QTSP by the subscriber or by the operators RAO. The QTSP always verifies the identity of the applicant and the veracity of the request.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

4 CERTIFICATE LIFE CYCLE REQUIREMENTS

4.1 REQUEST OF A CERTIFICATE

The qualified electronic signature certificate issued by Lottomatica Holding S.r.l., is used compatibly with the limitations of use specified in the chap. 1.4.

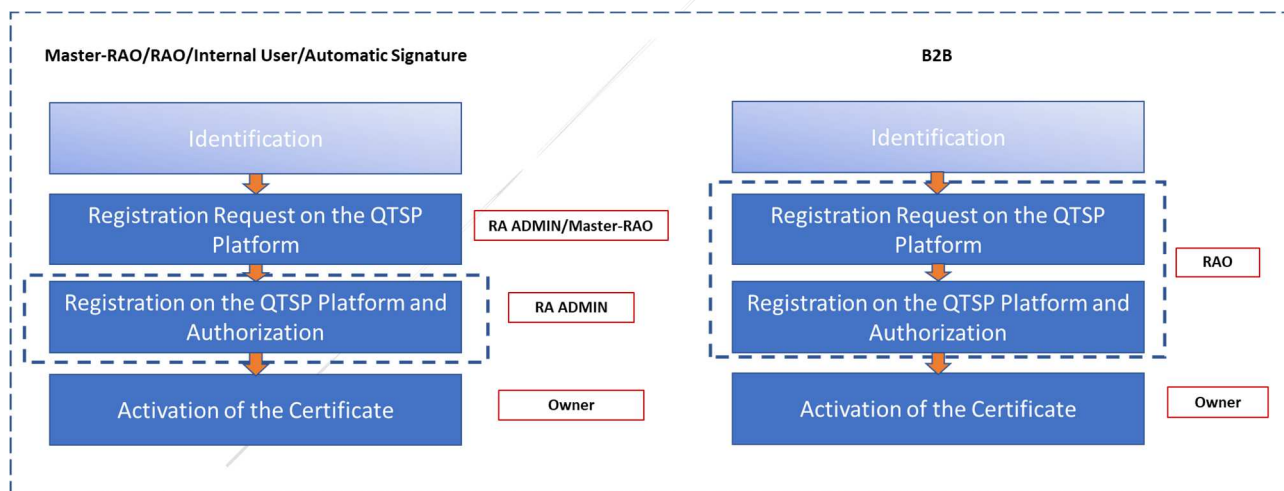
Each new process of issuing a subscription certificate is subject to verification of the identity of the subject compatibly with what is specified in chapter 3, and in particular in the ways described in chapter 3.2.

The identification and registration of the owner's data are validated in different ways depending on the type of membership in the subscription channel (Master-RAO, RAO, B2B, Internal User, Automatic Signature).

The procedure for generating the keys and the relative certificate is subject to acceptance by the subscriber of the conditions and terms of use of the service. The acceptance document is proposed in an understandable format and gives the owner the possibility of being able to download it in electronic format, in order to be able to print it. Acceptance by the subscriber of the proposed data constitutes acceptance of the validity of the personal data displayed in the document.

Together with the contract document, the applicant provides the documents, certifications, powers of attorney or declarations necessary for the validation of the identity of the natural person who will be the holder of the qualified certificate.

The flow and the actors involved for the various subscribers are described below, described in detail in the following paragraphs:



For the B2B user, the activation of the certificate can also take place through the Reseller Portal in the manner described in the following paragraphs.

Certificate request RA Admin, Master-RAO, RAO, Lottomatica People and Automatic Signature

Through appropriate internal tracking tools, the request of certificate is inserted.

The approval workflow includes the following authorization steps:

- Registration Authority Manager;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- Certification and Time Validation Service Manager.

If, in accordance with the Business Continuity Plan or specific delegation documents / communication, the previous managers are unavailable, the approval process will be conducted by the substitutes.

For the registration request on the QTSP Platform, an email will be sent to calottomatica@igt.com and to the Registration Authority Manager containing at least:

- front / back identification document (identity card, driving license or passport).
- Tax code front / back;
- outcome of the training test (where applicable);

All documents are kept in a network folder accessible only to persons authorized by the Trusted Services function and to the RA Manager.

Following the closure of the approval workflow and upon receipt of the required documentation, the data are registered by the RA Admin within the QTSP platform including email, mobile phone, document type, document number, document expiry date, release date, document issuer.

The RA Admin authorizes the request for the certificate, through the QTSP platform.

The activity ends with the sending of an automatically generated email to the subscriber containing the first access credentials and instructions on how to proceed.

Received the email, the subscriber proceeds with the activation of the certificate:

- then accesses the "Enroll" section and activates the signature by confirming the details of the personal data shown on the screen, including the mobile number (required for OTP via SMS); then based on the type of OTP:

➤ **OTP via SMS:**

The user then proceeds:

- Entering a new PIN code and confirming it;
- Upon reading the general conditions of the service;
- At the start of the activation procedure.

The system then proceeds with:

- The generation of the subscription keys using the PIN specified by the owner, in accordance with what is specified in chapter 6.1.1;
- Sending the certificate request to the CA;
- The installation of the certificate generated by the CA;
- The initialization of the OTP system referred to in point 6.3;
- The sending of the OTP credential via SMS, to unblock the Signature operation. The SMS is sent to the phone number provided during the identity validation phase (par.3.2).

➤ **Physical token:**

- The user enters a new personal signature PIN code confirming the data;
- The user reads the general conditions of the service;
- The system generates the subscription keys using the PIN specified by the owner, in accordance with what is specified in chapter 6.1.1;
- The system sends the certificate request to the CA;
- The system installs the certificate generated by the CA;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- The user is assigned a physical Token for the generation of OTP codes for unlocking signature operations;
- The user accesses the OTP section by enabling their system physical Token;
- The user accesses the Enroll section by entering the OTP code generated by the physical Token enabling the generation of OTP codes to unlock the signature operations.
- The user, with his PIN and OTP Token, signs the general conditions of the service previously read.
- The QTSP maintains the declaration digitally signed by the Data Controller with which he certifies the data and the acceptance of the general conditions of the service.
- The activity ends with the sending of a mail generated automatically by the QTSP to the subscriber with the confirmation of the creation of the certificate.

Request for B2B certificate

After validating identity with one of the procedures described in chap. 3.2 of this document, the RAO user confirms the start of the procedure during the contractualization of the Sales Point. Through the specific contractualization tool, requires registration/ registers the B2B subscriber's registry on the QTSP Platform, authorizes the certificate, and:

- Makes sure that the subscriber has read and accepts the general conditions of the service;
- confirmation by digitally signing (with remote signature) the certificate release document to the store owner.

The system then proceeds with:

- The generation of the subscription keys in accordance with what is specified in chapter 6.1.1, using a random PIN generated at the time;
- Sending the certificate request to the CA;
- The installation of the certificate generated by the CA;
- The initialization of the OTP system referred to in point 6.3;
- The sending of the PIN and the OTP credential through 2 separate SMS, to unlock the Signature operation.

The user, with his PIN and the OTP received via SMS, signs the general conditions of the service previously set out.

The SMS are sent to the phone number provided during the identity validation phase (par.3.2).

The QTSP maintains the declaration digitally signed by the Owner with which it certifies the data it has provided to the RAO for registration at the time of identification and acceptance of the general conditions of the service, accompanied by the digitally signed declaration by the RAO that certifies the execution of the identification operation according to the instructions provided by the QTSP.

In the case of B2B subscribers who have contractual relationships already in place with Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A. The process allows legal representatives of Points of Sales having contractual relationships already in place with Lottomatica Holding S.r.l. and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A, to obtain a Remote Digital Signature Certificate through the use of the Reseller Portal. In this case:

- The user accesses the Reseller Portal with the credentials already in his possession;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- The B2B user verifies his own data (including the mobile number) on the systems and requires the activation of a new certificate. These data, both personal and contact, are not changeable. If is necessary to modify some of them, he will benefit from services and processes for modifying and verifying the personal data created in compliance with the regulations / laws / industry standards (eg AML directives, convention agreements, etc.).
- If an active Certificate is not present, then the Legal Representative explicitly requests the creation of a certificate, this request generates 2 documents:
 - The first contains the personal and contact details of the Owner and is digitally signed through an automatic signature certificate;
 - The second are the General Terms of Service (CGS).
- The PDV Legal Representative receives the PIN code and the OTP code on 2 separate text messages;
- The Legal Representative of the Point of Sales has the possibility therefore to view / read the CGS (General Service Conditions) and sign them by entering PIN and OTP received on their mobile phone, and complete the process.

The scope release method of this paragraph allows the B2B user to obtain a Remote digital signature certificate within the limitations of use of the certificate.

4.1.1 Submission of the certificate request

The request of the certificate may only be validated following the procedures for ascertaining the identity of the holder.

The confirmation of the validity of the data is processed according to the channel of belonging of the holder to which the qualified certificate is issued. In any case, the submission of the request for registration on the QTSP platform for the certificate issuance is performed by:

Subscriber	Request validated by
RA Admin	RA Manager
Internal/External Master-RAO	RA Admin
Internal RAO	Internal Master-RAO
External RAO	External/Internal Master-RAO
Automatic Signature	Internal Master-RAO
Lottomatica People	Internal Master-RAO
B2B	Internal/External RAO

The B2B subscriber can also proceed with the request through the Reseller Portal in the manner described above.

4.1.2 Registration/ Enroll process and responsibility

The registration/enroll process has the main task of issuing the subscription certificate.

The QTSP, received confirmation of the initiation of the issuing procedure, must record the information relating to the owner's master, before proceeding to the generation of the certificate.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Before the start of the procedure, the Subscriber is called to check his/her personal data and to review the terms and conditions of the service.

Registration on the QTSP platform and subsequent authorization of the request is performed by:

Subscriber	Registration and e authorization Certificate Request
RA Admin	RA Admin
Internal/External Master-RAO	RA Admin
RAO	RA Admin
Automatic Signature	RA Admin
Lottomatica People	RA Admin
B2B	Internal/External RAO

Registration and subsequent authorization of the certificate for the subscribers Master-RAO, RAO, Automatic Signature, Lottomatica People is carried out by the RA Admin directly from the QTSP Platform.

Registration for the B2B user takes place through the contractualization tool, authorization can take place through the contractualization tool or the Reseller Portal.

The events resulting from the confirmation of the data and that relating to the terms of use of the service are recorded by the QTSP and stored for a period of 20 years.

If the identity of the Subscriber is not validated by the Subscriber, the enroll process should not be executed.

4.1.3 Activation of the certificate

The activation of the certificate can be done exclusively by the Owner and always provides the acceptance of the general conditions of service, digitally signed, through unlocking the associated private key through the choice, if it is not a B2B for which it is generated automatically and randomly, of PIN code and entering an OTP code, as in par. 4.1.

4.2 CERTIFICATE REQUEST MANAGEMENT PROCESSES

4.2.1 Performing identification and authentication functions

The QTSP identifies the subscriber in accordance with what is published in chap. 3.2

4.2.2 Approval or rejection

The approval of the request may take place if:

- The holder has the requirements related to the verification of his identity;
- The owner accepts the terms and conditions on the delivery of the service.

The rejection of the request may take place if:

- None of the conditions for approval have been verified;
- The holder has another valid certificate (with the same certificate profile) in his name, which is not close to maturity.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

4.2.3 Execution time of the request

The certificate shall be issued at the end of positive feedback following the procedures for ascertaining the identity of the holder.

Execution time of the request Master-RAO/RAO

There are no timing related to the handling of the request, if not those related to the validation of data by staff responsible, and the electronic transaction necessary to run the enroll procedure.

B2B channel request execution time

No time is defined for the management of the request, except those related to the validation of data by Rao, and to the telematic transaction necessary for the execution of the Enroll procedure.

Request execution times for the automatic signing certificate

There are no timing related to the handling of the request, if not those related to the validation of data by staff responsible and the electronic transaction necessary to run the enroll procedure.

Run time for the internal user request

There are no time-limits related to the management of the request, except those related to the validation of data, and the telematic transaction required to carry out the enrollment process.

4.3 ISSUING THE CERTIFICATE

For all types of subscriptions:

- The QTSP issues the certificate to the user subsequently:
 - To the validation of the identity of the subject, with one of the systems described in 3.2;
 - Upon acceptance of the terms and conditions of use before issue;
- To successfully execute the necessary IT processes:
 - To the validation of the subscriber's identity, with one of the systems described in 3.2;
 - Upon acceptance of the terms and conditions of use by the subscriber;
 - To the validation of personal data;
 - When choosing, if it is not a B2B for which it is automatically and random generated, its own PIN code associated with the Signature operation;
 - All the technical operations connected with the generation of subscription keys and the related certification by CA Lottomatica Holding S.r.l.;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- Upon initialization of the OTP system referred to in point 6.3.

4.3.1 CA action during certificate issuance

The certificate shall be issued with the security measures in accordance with the rules in force. The CA is obliged to issue the certificate on the basis of the personal data contained in the request received.

4.3.2 Notifications to the holder about the issuing of the certificate

The QTSP informs the holder about the issuing of the certificate through a notification to the email address provided by the holder when managing the request.

4.4 ACCEPTANCE OF THE CERTIFICATE

4.4.1 Conduct on acceptance of the certificate

The issuing of the certificate, the related keys and the activation parameters, are issued under the exclusive control of the holder in accordance with the terms and conditions accepted by him.

4.4.2 Publication of the certificate by the CA

The QTSP does not make public the generated certificates. The related conditions are contained in the general conditions of the service accepted by the owner.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber private key and certificate usage

The subscriber uses his or her private key corresponding to the certificate issued to him only for the purposes in accordance with the conditions specified in chapt. 1.4. Any other use of the certificate is prohibited.

The subscription operation is used by the holders according to the following scheme:

- For B2B users, the subscription is only for the signature of PDF and PDF/A files, exclusively in the context of a process related to the contractualization of the user or processes attributable/conveyed according with the limitations of use, realized through IT solutions (eg web portals, systems for use Internal) devoted to this purpose;
- The Master-RAO/RAO user signs documents in compliance with the limitation of use detailed in paragraph 1.4.1 through IT solutions (eg web portals, systems for internal use) devoted to this purpose; the RAO signs the B2B user registration form;
- For the internal user, it is allowed to sign documents through IT solutions dedicated to this purpose and can only be used for activities in compliance with the limitation of use detailed in paragraph 1.4.1. Specifically, such IT solutions accept any document or file format, allowing the signature to be applied in the formats:
 - PAdES / PAdES-T for PDF documents;
 - CAdES / CAdES-T for all other documents.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- For the User Automatic Signature, the signature of documents is carried out only by systems of Lottomatica Holding S.r.l and/or LIS - Lottomatica Italia Servizi S.p.A. or companies under common control of Lottomatica Holding S.r.l. or LIS - Lottomatica Italia Servizi S.p.A. appropriately configured to use the Automatic Signature certificate. These systems accept any document or file format, allowing the signature to be applied in the formats:
 - PAdES / PAdES-T for PDF documents;
 - CAdES / CAdES-T for all other documents.

The QTSP warrants that the signed document, 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].

The QTSP establishes that a private key corresponding to an expired, revoked or suspended certificate must not be used for the creation of a qualified electronic signature.

The subscriber must ensure adequate protection of qualifying electronic signature activation data (password and OTP code); In particular, when the following conditions are met:

- Loss of signature unlock tools control;
- Loss of mobile phone ownership or change of number supplied;
- Cell phone number change.

Following the aforementioned events, the holder is required to request the revocation and subsequent re-issue of the certificate.

4.5.2 Interested parties – Public key and use of the certificate

The parties concerned with the verification of a qualified electronic signature must proceed as contained in this CPS with particular reference to the following:

- Stakeholders must verify the validity and status of the certificate; in particular, it is recommended that the verification of the certificate be carried out through the complete validation of the certificate chain, ensuring that the certificate of qualified electronic signature was issued by Lottomatica Holding S.r.l. By means of recognition of the root CA certificate of Lottomatica Holding S.r.l., published by Agid on its site;
- The qualified electronic signature certificate and the corresponding public key must only be used for the validation of the signature;
- The parties concerned must take account of the limitations of use indicated in the certificate, in accordance with the provisions of Chapter 1.4.

The QTSP exposes services to allow subscribers and stakeholders to verify certificates issued, in accordance with the provisions specified in chap. 4.9.

4.6 REISSUE

Reissuing the certificate refers to the regeneration of the keys and the certificate, provided in the cases specified in 4.6.1.

4.6.1 Requirements for renewing the certificate

Reissue of the certificate can only be performed when the following conditions are verified:

- The previous qualified electronic signature certificate is revoked;
- The previous qualified electronic signature certificate is expired;
- The identity of the holder indicated in the certificate is still valid;
- The specified in 3.3 has been executed.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

4.6.2 Submission of reissue request

Reissue request

The submission of the request for reissue of the certificate, must be initiated or approved by the owner.

The activation of the certificate can only be done by the Owner, in the same way as described for the first issue, through the contact data provided by the same.

After the QTSP has authorized the request for a certificate, the Owner proceeds with its activation.

4.6.3 Reissue request process

In the process of evaluating the reissue request, the QTSP ensures that:

- The reissue request is authentic;
- The applicant is authorized to proceed;
- A correct evaluation of the master data present in the system has been performed.

The methods used for identifying and authenticating the reissue process are described in chap. 3.3.

The authorization of the certificate request takes place in the same way as for the first issue, as specified in par. 4.1

4.6.4 Registration on QTSP Platform and Authorization of the Certificate

In the event of a reissue, the owner is already registered in the QTSP platform. In this case, in case of modification of the owner's data, an update of the master data is made before authorization of the certificate request.

The RA Admin updates the master data, if necessary, for the following subscribers:

- Master-RAO;
- RAO;
- Internal User;
- User Automatic Signature.

The RAO, through the specific contractualization tool, updates the master data, if necessary, for the B2B subscriber.

Subsequently, through the QTSP platform or through the contracting application / Reseller Portal, the authorization of the certificate request is started as provided for the first issue.

4.6.5 Activation of the certificate

The process of activation of the Certificate by the Owner requires what is specified for the first issue, how described in par. 4.1

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

4.6.6 Notifications about issuing the certificate

The QTSP notifies the subscriber of the issuing of the certificate through the email address provided by the holder when managing the request.

4.6.7 Conduct on the acceptance of the reissue of the certificate

Once the certificate is issued, the Subscriber is called upon to confirm the data it contains through the qualified electronic signature to which the certificate is connected (CGS Signature).

4.6.8 Publication of the renewed certificate by the CA

QTSP does not publish subscription certificates, but makes them available to the holder.

4.7 MODIFICATIONS TO THE CERTIFICATE

The QTSP does not make or allow changes to be made to the certificate.

4.8 REVOCATION AND SUSPENSION OF THE CERTIFICATE

Revocation of the certificate means the procedure by which the QTSP terminates the validity of a certificate before its natural expiration date. The revocation of a certificate is permanent and not reversible; a revoked certificate cannot return.

In the event of revocation of the certificate, the QTSP may delete the keys of the subscriber using the procedures in accordance with the HSM user manual, and with what is specified in the certification documents.

Following the revocation of the certificate, the QTSP notifies the holder of the change in the status of the certificate.

The QTSP does not suspend the certificate.

4.8.1 Circumstances of revocation

The QTSP can revoke the Subscriber certificate in the following case:

- Change of the Subject data of the certificate;
- Change mail and mobile phone;
- Change of the limitations of use of the certificate;
- The QTSP verifies that the data relating to the certificate do not correspond to reality;
- The holder requires the withdrawal of the certificate in writing or by telematic means;
- The QTSP verifies that the private key is not under the exclusive control of the subscriber;
- The QTSP verifies that the certificate is used outside the permitted scope;
- The QTSP verifies that the public key contained in the certificate is not compatible with what is specified in the 6.1.5 and 6.1.6 chapters;
- The QTSP verifies that the certificate has not been issued in accordance with this CPS;
- The QTSP verifies that the private key of the subscriber has been or may have been compromised;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- The QTSP verifies the termination of the reasons for the release (for example termination of the employment relationship for internal user);
- The QTSP terminates its certifying activity;
- The law in force requires a compulsory withdrawal;

The mobile number provided by the Subscriber during request/registration of the registry must remain unchanged throughout the period of validity of the certificate, as it is used as a communication tool of the second authentication factor generated by the QTSP, and sent at the time of the qualified signature operation.

Upon the occurrence of this event (the change of mobile number), the Subscriber is obliged to notify the QTSP in order to proceed with the personal changes of the case, also by means of revocation accessible by link on the **portal of the certificate**.

Failure to communicate the variation, by virtue of the loss of control over the second authentication factor, allows the QTSP to enforce what is expected to revoke the certificate.

4.8.2 Submission of revocation request

The request for revocation may be requested by:

- The subscriber;
- The legal representative of the subscriber;
- The QTSP.

4.8.3 Processes for revocation management

The QTSP provides a tool to revoke the certificate, through its function revoking the certificate accessible, after authentication, on the **QTSP Portal**.

The procedure for the request for revocation is that:

- The holder of the certificate accesses the portal of the QTSP, through his credentials generated at the time of issuing the certificate;
- The holder accesses the revocation section, and fills in the form provided;
- The holder displays the data relating to the revocation operation, and confirms the transaction by sending the request;
- The holder, in case of withdrawal of the certificate for the use of digital signature services, if in possession of physical Token devices for the generation of OTP codes must provide for the return of the same at the offices of the QTSP located throughout the Territory National. The QTSP will implement the internal process to proceed with the withdrawal of the certificate and the return of the device;
- The system submits the request to the CA and, as soon as it executed, sends a confirmation email to the holder.

The revocation procedure can also be submitted by personnel appointed by the QTSP, after authentication, on the **QTSP Platform**, according to the circumstances defined in 4.8.1

The QTSP automatically takes into process all requests received, processing them within a maximum time of 24 hours.

The same procedure applies if the tokens are lost (if assigned):

- The holder reports the event to the QTSP at the **firmaqualificata@pec.lottomatica.it** inbox → from **01 March 2021** the reference address will be **caigt@pec.it**;
- The QTSP verifies the identity of the holder through the Registration Authority (RAA, Master-RAO, RAO);

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- The QTSP proceeds to disable the physical Token of the holder and binds to the same a new method of generating the OTP code (method via SMS) to guarantee the continuity of the service offered.

4.8.4 Grace Period request for revocation

The "grace period" associated with verifying the validity of the certificate, is equal to the maximum expected value for the CRL update, and is 4 hours (see Chapter 4.8.7).

4.8.5 Time within which the CA must process the request for revocation

The QTSP must process withdrawal requests in accordance with ETSI 319 411-1 v1.2.2 Clause 6.2.4 [3].

4.8.6 Requirements on the control of revocation by interested parties

In order to comply with the revocation check, it is recommended to check all certificates included in the certification chain. Verification must include checking validity of certificates, policies contained in the certificate together with key usage, certificate status checking based on information contained in the CRL or the OCSP.

4.8.7 Frequency Issuing CRL

The publication frequency of the CRL is 4 hours, with 24 hours of validity.

4.8.8 Maximum latency on CRL

The maximum latency associated with publishing the CRL is 5 minutes.

4.8.9 Availability of OCSP service

The QTSP provides an OCSP service to validate the certificate. The service is available on the basis of what is specified in 4.9.2.

4.8.10 OCPS service requirements

The QTSP OCSP service is compatible with the requirements specified in Cap 4.9. The OCSP service can be queried by using the HTTP GET method.

4.8.11 Special requirements on key compromise

If the private key is compromised, the QTSP publishes the status change of the certificate and notifies the event to interested parties.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

In the case of an end-user's private key compromise, the QTSP revokes the certificate by specifying the value "KeyCompromise (1)" as Reasoncode.

4.9 CERTIFICATE STATUS VERIFICATION SERVICES

The QTSP, in order to verify the validity status of a digital certificate, provides the following services:

- OCSP – Online Certificate Revocation Status;
- CRL – Certificate Revocation Lists.

The revoked certificates are included in the CRL.

The revoked certificates cannot be canceled by the CRL, even after the expiration date.

In case of state change (active, suspended, revoked), at the completion of the process, the QTSP instantly updates the CRL, which is subsequently published in accordance with the latency times and frequency time specified in cap.4.8.7 and 4.8.8. Since then, the OCSP service provides information about the new status of the certificate.

The OCSP service contains the value "UNKNOWN" if the certificate is not present on the revocation list or has not been issued by the QTSP.

The QTSP also publishes a portal (online verifier) for validating a signed digital signature document, publicly available at the following url:

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

The user who needs to verify the validity of a qualified electronic signature of a document, accesses the above service and uploads (or uploads) the file. The service returns the outcome of the validation check.

The online verifier is a Java-implemented Web-based component, based on the DSS project, recommended by the European Commission for full recognition of computer documents signed in the different Member States.

4.9.1 Operational features

The QTSP CA updates the revocation list as specified in 4.8.7.

For operational reasons, the CRL may have validity that exceeds the default validity specified in this CPS (see Chapter 4.8.7); This value must not exceed 24 hours in any case.

The OCSP service is updated based on the publishing policies that are related to the CRL update.

The CRL is available to the following URL:

<https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl>

4.9.2 Service availability

Access to the CRL and OCSP service is available 24 hours a day.

The QTSP must ensure the availability of the CRL published on HTTP and the terms and conditions of the certificates issued at 99.7% on an annual basis, ensuring that unavailability of the system does not exceed 8 hours.

The QTSP must ensure the availability of the services associated with the verification of the revocation of the certificates issued, to 99.7% on an annual basis, ensuring that the unavailability of the service does not exceed 8 hours.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

4.10 END OF SUBSCRIPTION

The QTSP may revoke the holder's certificate in case of termination of the contractual arrangements with the subscriber or are verified the conditions of 4.8.1.

4.11 KEY ESCROW E RECOVERY

QTSP does not provide key escrow tools applied to the private key belonging to a subscriber.

4.11.1 Policy and practices Key Escrow and Recovery

QTSP does not provide key escrow tools applied to the private key belonging to a subscriber.

4.11.2 Encapsulation key symmetrical encryption policies recovery

The QTSP does not provide tools for key escrow applied to the private key belonging to a Subscriber.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			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 provides 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 4.9.2 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 made with the use of combustible. 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:

It is mandatory to:

- Access the workplace using access credentials (eg magnetic badges) from the prepared passes and the ways established by the company;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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);
- 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, subject to identification and authorisation by an internal Lottomatica Holding S.r.l. contact person;
- 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 Data Center, completely fenced, is illuminated in night time and constantly monitored by a CCTV system consisting of fixed cameras and sun, 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			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. Over the condensation system and the water supply to the humidifiers of the air-conditioning system is present the cage cooling system. These three systems are equipped with special precautions in order to avoid water leakage. In case of 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 distribution of the coolant 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Site B

The CED is equipped with a centralised 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, 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, the information present in it can be deleted, 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 or media medium, 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

In compliance with the DPCM 22 February 2013 [24], art. 38, these roles foresee the existence of at least the following figures:

- Responsible of the certification and temporal validation service;
- Responsible of the Registration Authority (RA Manager);
- Responsible of the security;
- Responsible for check and inspections (audit);
- Responsible for the temporal validation service;
- Responsible for the technical management of the systems;
- Responsible of the Technical and logistic services.

5.2.2 Number of people required for task

The QTSP ensures the simultaneous presence of at least 2 people, with specially approved roles, during the following critical security operations:

- The generation of the private key of the QTSP CA;
- Backup of the private key of the QTSP CA;
- Activation of the private key of the QTSP CA;
- The destruction of the QTSP CA private key.

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

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

5.2.3 Identification and authentication fo 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 requiring segregation

The QTSP applies the provisions of the DPCM 22 February 2013 [24], art. 38 paragraph 3 and 4. In this area:

- Security officer may not take any other roles as defined in 5.2.1;
- The auditing and inspection manager cannot take any other roles as 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			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 citizen 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:

- Staff responsible for preparing and delivering the training must have the necessary qualifications and experience in terms of company training;
- The Master-RAO/RAO appointees shall receive the training manual and the appropriate education to carry out the identification and registration activities of the customers correctly and carry out the verification of the effectiveness of the training;
- Where deemed necessary, the training activity can also be extended to suppliers and collaborators;
- The programming and delivery of all the courses provided by the regulations applicable to the company's activity must be guaranteed;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- The knowledge of the current legislation on qualified fiduciary services, as well as best practices and standards, must be ensured;
- The definition of training plans for qualified trust services must comply with the provisions of EU Regulation 679/2016 on the protection of individuals with regard to the processing of personal data [25].

5.3.4 Update frequency

Lottomatica Holding S.r.l. training program 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 unauthorised shares

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 report that Lottomatica Holding S.r.l. establishes with the same.

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 processing 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;
- 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

The QTSP can adopt it tools that ensure the collection of events associated with the Certification activity.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

5.4.1 Types of events stored

The QTSP, through specialized instruments, implements a monitoring of events associated with the activity of QTSP in accordance with specified in chap. v 1.1.1 6.4.5 standard EN 319 411 2 [4].

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.

System audits

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 in function of:

- The importance and/or the criticality of the activities carried out by the individual structures;
- 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, in agreement with the DPCM 22 February 2013 [24].

5.4.4 Audit log protection

The protection of audit logs must ensure:

- Protection: only authorized personnel can access the stored events;
- Availability: the events are kept in a way that can verify the content and the integrity over time, preventing the corruption of the data;
- Integrity: the data is retained in order to prevent the alteration of the data.

The audit log protection is in accordance with the standard EN 319 401 v 2.1.1 [1] in Cap 7.10.

5.4.5 Audit log backup procedures

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

5.4.6 Audit event collection system

The QTSP adopts automated systems that ensure the collection activity on a continuous basis. Each IT system involved, collects and sends events to the log system.

5.4.7 Notification in case of identification of suspicious events

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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;
- 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 (at least 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 complies with what is specified in Cap. 5.4.3.

5.6 CA KEY CHANGEOVER

In order to ensure its operation, the QTSP ensures that the renewal of his certificate is made sufficient time prior to the expiration of the same.

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

It also specifies that:

- the new certificate is published to the public repository of certificate, in compliance with as provided in this chapter CP 6.1.4;
- new user subscription certificates are issued using the new certificate renewed;
- the old keys and certificate are kept by law.

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 CPS.

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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

The QTSP adopts a plan inside 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 plan.

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

The QTSP provides, within internal procedures, the implementation of an emergency plan in case is detected 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 and IDAs [27] security incidents are classified with 5 levels of severity (according to the Enisa Guidelines):

1. No impact;
2. no significant Impact (impact on assets but not on core services);
3. Significant impact (impact on part of the 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 you 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, within 5 days with severity 1 and 2.

5.7.1 Incident and compromise management procedures

The QTSP has a Business Continuity Plan (BCP) 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 of the Sites, even in fault situations of a system or apparatus.

5.7.2 Computing Resources, Software, and/or corrupted data

The QTSP must adopt redundant system design criteria in order to avoid loss of service in the case of point of failure acronyms.

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 the CPS. 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 foresees the implementation of an emergency plan in case the key compromise occurs. This contingency plan reveals the circumstances of compromise and provides for:

- The notification of all interested parties;
- If necessary, revoke the compromise certificate and generate a new one with new keys associated with the service.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

5.7.4 Capacity of business continuity in case of disaster

The tasks to be performed in the event of a disaster are defined in the QTSP Business Continuity Plan.

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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021

Classification: PUBLIC

6 TECHNICAL SECURITY CONTROLS

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 throughout their entire life cycle. 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 milestones 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, provide for certification coverage conforming to 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 set out in the regulations 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 goals 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 the CA service;
2. Subscription keys, intended for holders;

All keys are generated through an HSM-type device, complying with the certification standards listed in Chapter 6.2.1. and in strict observance of what is specified in the respective security targets.

The QTSP confirms that the process of generating the keys of the CA and that of the owners, is carried out in accordance with the technical rules with respect to what is in force, as specified in the standard EN 319 411 01 v1.2.2, with particular reference to chapters 6.5.1, 6.5.2 and 6.5.3.

The process of generating the keys of the CA complies with what is specified in the standard EN 319 411 01 v 1.2.2, with particular reference to the chapters 6.5.1, 6.5.2 and 6.5.3.

6.1.2 Private key release to subscribers

In the context of a Qualified Remote Signaling Service, the release of the private subscription key consists in issuing credentials for the use of the same. QTSP guarantees that the credentials associated with the unlocking of the private key are released safely only and exclusively to the subscriber.

6.1.3 Issuing the public key to the certificate

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

The keys of the QTSP must be generated at the time of system initialization (key ceremony). Key generation and certificate request must be handled securely using the modes specified in the product manuals.

6.1.4 Issuing the CA public key to interested parties

Compatibly with what is specified in Chapter 2.2, the QTSP makes available the certificate containing the public key on its **QTSP Platform**.

In accordance with point H of annex I to the European regulation 910/2014 [27], the publication link of that certificate shall also be inserted within the underwriting certificates issued by the QTSP (see chap. 7.1.2).

6.1.5 Key length

The QTSP uses algorithms and policy on the key length as specified in the ETSI standard TS 119 312. In particular:

- The RSA root key CA is 4096 bits long.

6.1.6 Key generation parameters and quality control

The requirements for key generation parameters are given in Cap 6.1.1. The QTSP ensures that the HSM covered by certification, operate in compliance with what is foreseen by the achieved security milestone.

6.1.7 Key usage purposes (see key usage field X. 509 v3)

The CA certificate can be used in accordance with the following:

- Certificate signing;
- CRL signing;
- Offline CRL signing.

The qualified electronic signature certificate of the holder is generated in accordance with the requirements for the qualified electronic signature, the key-usage of which includes the following:

- Non-repudiation.

More details are listed in Chap 7.1.2.

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 module controls

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

The CA in the certification infrastructure, which ensures the issuance of subscription certificates, the signing of OSCP response, the signing of the CRL, stores its private keys within a secure device that is 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.

6.2.2 Private key segregation control (MofN)

The QTSP ensures the simultaneous presence of at least 2 people operating on the HSM, with specially approved roles, during the performance of critical security operations, in accordance with the specified in 5.2.2.

6.2.3 Key Escrow private key

The QTSP does not provide key escrow tools that are applied to the CA's private key.

6.2.4 Key storage

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

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.

The QTSP does not make copies of the private keys of the subscribers.

6.2.5 Key storage

The QTSP does not store the CA's private key.

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

The private key of the QTSP CA is maintained securely through the security mechanisms provided by the HSM, covered by the certifications specified in Cap 6.2.1.

The private key of the CA is never kept in clear.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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 CA's 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 CA stores the private key 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.

6.2.8 Private key activation method

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

In the case of a subscriber's private key, QTSP ensures that the activation data is generated and managed in a secure manner to prevent unauthorized use of the private key.

The QTSP must also ensure that:

- The private key for the subscriber has not been used for qualified electronic signature before delivery to the holder;
- Before the signing procedure is performed, the Subscriber is required to authenticate to the slot protected by the HSM.

6.2.9 Method of deactivating private key

CA Private Keys

The key QTSP CA must be disabled in accordance with the procedures specified in the owner's Manual of the HSM, and with what is specified in the documents of certification.

End-User Private Keys

The private key issued to the Subscriber must be deactivated in accordance with the procedures specified in the HSM user's manual, and as specified in the certification documents.

The HSM must ensure that the keys are disabled in the following cases:

- Power failure of the device;
- The subscriber closes the signature application;
- For some reason, connecting to the signing application closes the connection unexpectedly.

The key that is disabled can be reused only after a new subscriber authentication to the device.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

6.2.10 Method of destruction of the private key

QTSP CA key

The QTSP CA key can be deleted 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 Chap 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.

Subscriber private key

The subscriber's private 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.

6.2.12 Validity of the certificate and keys

Certificate and CA root keys

The validity period of the CA certificate of the QTSP, and its key pair, is 30 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.

Certificate and key subscriber

The validity of the subscription certificate issued to the end user:

- It is valid for 3 years;
- 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 CA certificate of the QTSP that issued it.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

6.3 ACTIVATION DATA

6.3.1 Activation data generation and installation

The QTSP CA key is protected according to the procedures specified in the HSM user manual, and with what is specified in the certification documents.

In the context of password management, the QTSP applies sufficient complexity criteria in order to ensure an adequate level of protection.

In the event of activation of keys intended for the subscriber, the QTSP ensures:

- That the activation data used for the activation of the private key, are created using the number/letter generation criteria of adequate quality;
- That the activation data are communicated to the subscriber in a safe manner.

The authentication mechanism used as the second authentication factor is an OTP that is sent by SMS or generated using physical tokens. The OTP sent/generated, is based on the delivery of a one shot code to the mobile/display holder's Token at the time of signing.

The code generation engine is based on the development of the "Initiative for Open Authentication", and uses in particular the TOTP mechanism specified in RFC 6238.

6.3.2 Activation data protection

The activation data of the private keys associated with the subscriber's certificate is stored by the QTSP for the sole purpose of delivery to the holder. The data storage is made securely by encrypting the security information.

Sending the SMS is done via an SMS Gateway and SSL secure connection. The delivery application adopts appropriate repository encryption mechanisms, preventing at any time the data retention in the clear.

The security mechanisms of key activation data are also applied as regards the use of physical OTP Token.

6.3.3 Other aspects of the activation data

Not applicable.

6.4 COMPUTER SECURITY CONTROLS

6.4.1 Specific technical security requirements on IT system

The configuration, maintenance or consultation operations on the IT systems of the QTSP are carried out by ensuring the following requirements:

- That the user's identity is verified before accessing the system or application;
- That the roles are assigned to users in order to ensure that they have the appropriate permissions;
- That relevant security log events are recorded, which are subsequently stored in accordance with the rules in force, with specific reference to what is contained in the standard EN 319 411 02 v 1.2.2 Cap. 6.4.5;
- That the critical processes of the QTSP are protected by appropriate network policies in order to prevent unauthorised access;
- That there are adequate recovery systems that ensure operational continuity as a result of malfunctioning of the primary systems.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

6.4.2 Assessment of IT system security

In order to ensure the security and quality of the systems, the QTSP adopts control systems inspired by globally accepted international standards, the suitability of which is certified by an independent assessor.

6.5 LIFE CYCLE OF ROADWORTHINESS TEST

6.5.1 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.

6.5.2 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 the application and verification of policies 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;
- 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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.

6.5.3 Life cycle of security controls

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

- Has the correct certifications;
- When receiving apparatus, they are not in "tampered" status;
- That tampering protection is ensured during 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.

6.6 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,...);
- Define and implement 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;
 - 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 the machines and presence of uninterruptible power supply.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

6.7 TIME-STAMPING

The QTSP uses its own timestamp systems in accordance with this document issued specifically and separately for this service.

Furthermore, pursuant to article 41, paragraph 3 of the DPCM of 22 February 2013 [24] The time allotted 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 first.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021

Classification: PUBLIC

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

The QTSP has a root CA destined for issuing qualified electronic signature certificates and related certification services.

The CA certificate and the Subscriber certificate issued by the QTSP are compatible with the following standards:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Publickey and attribute certificate frameworks [19]
- RFC 5280 [16]
- RFC 6818 [17]
- 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
- Algorithm identifier
The OID of the algorithm used for certificate certification;
- The QTSP adopts the following algorithm:
"Sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
- 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 identifier
The QTSP supports the RSA algorithm in subscription certificates. The subscription key length is 2048 bits.
- The value included in this field is the value:
"RsaEncryption" (1.2.840.113549.1.1.1)
- 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].

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Following are the specific requirements regarding the above extensions:

Certificato di root CA

Nome	Valore
Version	Versione 3
Serial Number	(Attribuito a runtime)
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	DN del QTSP: countryName : "IT" organizationName: "Lottomatica Holding S.r.l." organizationIdentifier : "VATIT- 02611940038 " commonName : "Lottomatica EU Qualified Certificates CA"
Validity	30 years (expiry 30 years from the date of issue)
Subject	Vedi Issuer
SubjectPublicKeyInfo	Chiave pubblica 4096 bit Algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critica)	Subject Type: CA Path Length Constraint:0
KeyUsage (critica)	Certificate Signing, Offline CRL Signing, CRL Signing (06)
Authority Information Access	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it
Certificate Policies (non critico)	OID della policy: 1.3.76.49 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti
crlDistributionPoint (non critico)	http://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl

Certificate of the Subscriber B2B - Gaming/Services Area (IGTCP01)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	3 years
	C = IT,

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier)	SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.20.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl
------------------------------------	---

Certificate of the Subscriber Internal User - Gaming/Services Area (IGTCP03)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 ALLEGATO I, h) (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.22.1.0 Cp: URL: http://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh2020.crl

Certificate of the Subscriber Automatic Signature - Gaming/Services Area (IGTCP04)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.23.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il presente certificato è valido solo per firme apposte con procedura automatica

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

	The certificate may only be used for unattended/automatic digital signature
crIDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl

Certificate of the Subscriber Master-RAO, RAO - Gaming/Services Area (IGTCP05)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

	qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.24.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued
crIDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh2020.crl

Certificate of the Subscriber B2B - Services Area (IGTCP06)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	3 years

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.25.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo

 LOTTOMATICA	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

	Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl

Certificate of the Subscriber Master-RAO, RAO - Services Area (IGTCP07)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4)

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

	qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.26.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl

Certificate of the Subscriber Internal User - Services Area (IGTCP08)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"

Typology	REGISTRATION	Code	LTIS-05-00006/18
Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
		Date	08/02/2021

Classification: PUBLIC

Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.27.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text:

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

	<p>Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo</p> <p>Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control</p>
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhl2020.crl

Certificate of the Subscriber Automatic Signature - Services Area (IGTCP09)

Campi Base	
Version	Versione 3
Serial Number	(attribuito a runtime)
Signature Algorithm	sha256, RSA
Issuer	countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA"
Validità	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, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta>
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
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-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4)

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

	qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign
KeyUsage (critica)	Non Repudiation
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280)	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	1.3.76.16.6 1.3.76.49.1.1.1.28.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il presente certificato è valido solo per firme apposte con procedura automatica The certificate may only be used for unattended/automatic digital signature
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh2020.crl

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 CAs, thus not disregarding the following links:

- Ocsp – <http://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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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.

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:

- Ocsf – <http://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/qtspcacrhl.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

Only the identifier (OID) of the algorithms used must be used, in accordance with welcome specified in chapter 6.1.5.

The algorithms that can be used by the CA are listed in this document.

7.1.4 Composition of the name

The composition of the name identifying the distinguish name, is made in accordance to what is specified by RFC 5280 [16], ETSI EN 319 412-2 [6] standards.

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

The holder includes the serialNumber field SubjectDN specified as below:

- "TIN": unique ID field associated with the person; the tax code of the owner;
- "IT": ISO 3166 country code for Italy;
- "-": character 0x2D (ASCII)
- tax code value: Id of the owner.

DnQualifier, field contains the unique reference regarding an application created byQTSP and associated with the issue of the certificate.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

7.1.5 Constraints on name

Not present.

7.1.6 Certificate policy object identifier

The QTSP includes in certificates issued the certificate policy in accordance with CAP 7.1.2, marked non-critical.

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 Gestione della semantica per estensioni di certificate policy critiche

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 Specifying CRL extensions

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

- Version
The value of the field is "v2".
- Signature Algorithm identifier
The identifier (OID) of the algorithm used to create the electronic signature that certifies the CRL. The expected algorithm is "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Signature
The electronic signature that certifies the 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].

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- **Next Update**
The next release date of the CRL. The value must be in accordance with the UTC standard in accordance with RFC 5280 [16].
- **Revoked Certificates**
The list of serials of certificates suspended or revoked including the timetable.

The required 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 the CA:

- **ExpiredCertsOnCRL – not critical**
The CA indicates through this extension that expired certificates are not removed from the CRL (see chap 4.9). 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 revocation of the certificate.

The time reference from which the key is considered compromised.

- **Hold instruction – not critical.**

7.3 OCSP PROFILE

The QTSP provides an OCSP compliant service to RFC 2560 [13] and RFC 6960 [18] standards.

7.3.1 Version

The OCSP service provided is compatible with the version "v1" in accordance with what is specified in RFC 2560 [13] and RFC 6960 [18].

7.3.2 OCSP extensions

The extensions present in the OCSP protocol must be those provided in compliance with RFC 6960 [18].

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

QTSP's work towards compliance in force, is under the supervision of the **AgID, Italian Digital 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 and IDAs [27], 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 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [27];
- 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; [2]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1]
- ETSI EN 319 411-1 V1.1.1 (2016-02); 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 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; [4]

The result of the Audit is confidential and can only be accessed by authorized persons.

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

Compliance audits on the CA are carried out by a Conformity Assessment Body (CAB).

The assessor must be in possession of the Certification of Conformity of the Trustee Service Providers and the Services they have provided under Regulation (EU) 910/2014 and Regulation (EU) 765/2008. The only accrediting body of conformity attestations 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

8.4 TOPICS COVERED BY THE ASSESSMENT

The audit activity is conducted on the following aircraft:

- Compliance with the rules in force;
- Compliance with technical standards;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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 controls 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

9 LEGAL ECONOMIC ASPECTS

9.1 RATES

The digital signature service is provided by Lottomatica Holding S.r.l. a 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 the CAD [26] paragraph 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 entered into an insurance policy to guarantee a compensation limit of € 5.000.000,

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

In Lottomatica Holding S.r.l. an organizational and normative system is operational to ensure that all personal data processing is carried out in compliance with the provisions of the EU Regulation 679/2016 (hereinafter "the Regulation" or also "GDPR") [25] 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 This system is characterized by some important basic elements, among which the following are recalled:

- Employees who have received the appointment of appointees/persons entitled to the processing of personal data pursuant to art. 4 No 10 of the Regulation [25], have received detailed instructions on the security modalities and measures to be taken 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;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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 taking into account 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;
- 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.

The terminology used in this chapter complies with that adopted by the Regulation in particular:

- a. 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;
- b. 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;
- c. The appointee shall mean the person entitled to the processing of personal data under the direct authority of the holder or manager;
- d. 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. In particular, if designated, the controller:

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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 the Regulation.

Definition and identification of "personal data"

According to art. 4 No 1) of the regulation, 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 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.

Application of Regulation

General Fulfillment

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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 user subscribers. This register is kept inside a safe arranged in the area of the CTO Italy and Global Communication 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.

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 classification 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 security of the QTSP. In this regard, it is clarified that, in the event 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 [25];

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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.);
- 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 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.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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 that provided for by the Regulation 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 [25], 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. 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 CA

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

The QTSP is responsible:

- 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:

- To cover damages resulting from non-compliance by the Subscriber of what is contained in the terms and conditions of the service accepted by it.

In the nature and limitations of use of the qualified electronic signature service, QTSP is launching a plan to improve the accessibility of the service for disabled people through Web content accessibility solutions.

The QTSP is responsible for the obligations referred to in Art. 32 CAD (Obligations of the holder and the qualified electronic signature service provider).

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

9.6.2 Declarations and guarantees of RA

The QTSP through the services provided by RA, is responsible for compliance with the requirements contained in this document.

Statement of the RAO

The RAO operator, following the instructions received from Lottomatica Holding S.r.l. declares:

1. To have kept to the instructions received by Lottomatica Holding S.r.l.;
2. To have punctually provided the holder with all the information necessary for the use of the service, to have assured himself that he has understood the procedures for the correct use of the service, of the obligations he will take with respect to the protection of the private key and the provisions of the general terms and conditions of the service and this document;
3. To have carried out the activities of identification and registration in compliance with the rules of the Anti-Money Laundering law (D.Lgs. 231/2007 and subsequent amendments and related implementation regulations), the EU Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data (hereinafter "Regulations"), verifying that the ID presented by the holder is valid and does not present any signs that make him doubt his authenticity;
4. To have carried out the registration activities in accordance with the documents exhibited by the proprietor and in accordance with the provisions of the EU Regulation 2016/679 ;
5. To have informed the holder that the issue of the requested certificate is subject to the accuracy and completeness of the information provided by him;
6. To have informed the holder about the methods of handling the data as illustrated in the information on the processing of personal data available to us by Lottomatica Holding S.r.l. - as data controller of personal data - before signing this request and the general conditions of the service and available on the portal <https://ca.firmadigitale.lottomaticaitalia.it>.

Statement of the Master-RAO

The Master-RAO operator following the instructions received from Lottomatica Holding S.r.l. declares:

1. To have kept to the instructions received by Lottomatica Holding S.r.l.;
2. To have punctually provided the holder with all the information necessary for the use of the service, to have assured himself that he has understood the procedures for the correct use of the service, of the obligations he will take with respect to the protection of the private key and the provisions of the general terms and conditions of the service and this document;
3. To have carried out the activities of identification and request registration in compliance with the rules of the Anti-Money Laundering law (D.Lgs. 231/2007 and subsequent amendments and related implementation regulations), the EU Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data , verifying that the document of Identity presented by the proprietor is valid and does not present any signs that make him doubt his authenticity;
4. To have carried out the request registration activities in accordance with the documents exhibited by the proprietor and in accordance with the provisions of the EU Regulation 2016/679;
5. To have informed the holder that the issue of the requested certificate is subject to the accuracy and completeness of the information provided by him;

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- To have informed the holder about the methods of handling the data as illustrated in the information on the processing of personal data available to us by Lottomatica Holding S.r.l. - as data controller of personal data - before signing this request and the general conditions of the service and available on the portal <https://ca.firmadigitale.lottomaticaitalia.it>.

9.6.3 Declarations and warranties of the subscriber

Statement of the RAO

The owner Rao in the acceptance phase:

- Certifies the truthfulness and accuracy of the data connected in these General Conditions, assuming all responsibility pursuant to and for the purposes of the art. 46 of the D.P.R 445 of December 28, 2000;
- Confirms that the data used for issuing the qualified digital signature certificate are accurate and have been correctly registered;
- Confirms its willingness to want to activate and use the service requested to Lottomatica Holding S.r.l.;
- Declares that it has received the information for the use of the service and has consulted the Documents on the QTSP Portal: <https://ca.firmadigitale.lottomaticaitalia.it>;
- Declares to have been informed by Lottomatica Holding S.r.l., as Data Controller, about the primary purposes and the legal basis of the processing of their personal data, using the specific privacy information provided, pursuant to art. 13 of EU Regulation 2016/679 (hereinafter the "Regulation" or also "GDPR"), in the identification phase. The aforementioned privacy information is, however, always available on the website <https://ca.firmadigitale.lottomaticaitalia.it>;
- Declares to have received and read, before signing, the terms and conditions of use of the Qualified Electronic Signing Service and to approve the contents of General Conditions and in the descriptive documents of the Service, having fully understood how the service is used and the legally binding effects that derive from its use.

Statement of the Master-RAO

The owner Master-RAO in the acceptance phase:

- Certifies the truthfulness and accuracy of the data connected in these General Conditions, assuming all responsibility pursuant to and for the purposes of the art. 46 of the D.P.R 445 of December 28, 2000;
- Confirms that the data used for issuing the qualified digital signature certificate are accurate and have been correctly registered;
- Confirms its willingness to want to activate and use the service requested to Lottomatica Holding S.r.l.;
- Declares that it has received the information for the use of the service and has consulted the Documents on the QTSP Portal: <https://ca.firmadigitale.lottomaticaitalia.it>;
- Declares to have been informed by Lottomatica Holding S.r.l., as Data Controller, about the primary purposes and the legal basis of the processing of their personal data, using the

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

specific privacy information provided, pursuant to art. 13 of EU Regulation 2016/679 (hereinafter the "Regulation" or also "GDPR"), in the identification phase. The aforementioned privacy information is, however, always available on the website [**https://ca.firmadigitale.lottomaticaitalia.it;**](https://ca.firmadigitale.lottomaticaitalia.it;)

6. Declares to have received and read, before signing, the terms and conditions of use of the Qualified Electronic Signing Service and to approve the contents of General Conditions and in the descriptive documents of the Service, having fully understood how the service is used and the legally binding effects that derive from its use.

Statement of the B2B

The owner B2B in the acceptance phase:

1. Certifies the truthfulness and accuracy of the data connected in these General Conditions, assuming all responsibility pursuant to and for the purposes of the art. 46 of the D.P.R 445 of December 28, 2000;
2. Confirms that the data used for issuing the qualified digital signature certificate are accurate and have been correctly registered;
3. Confirms its willingness to want to activate and use the service requested to Lottomatica Holding S.r.l.;
4. Declares that it has received the tools and information for the use of the service and has consulted the Documents on the QTSP Portal: [**https://ca.firmadigitale.lottomaticaitalia.it;**](https://ca.firmadigitale.lottomaticaitalia.it;)
5. Declares to have been informed by Lottomatica Holding S.r.l., as Data Controller, about the primary purposes and the legal basis of the processing of their personal data, using the specific privacy information provided, pursuant to art. 13 of EU Regulation 2016/679 (hereinafter the "Regulation" or also "GDPR"), in the identification phase. The aforementioned privacy information is, however, always available on the website [**https://ca.firmadigitale.lottomaticaitalia.it;**](https://ca.firmadigitale.lottomaticaitalia.it;)
6. Declares to have received and read, before signing, the terms and conditions of use of the Qualified Electronic Signing Service and to approve the contents of General Conditions and in the descriptive documents of the Service, having fully understood how the service is used and the legally binding effects that derive from its use.

Statement of the Internal User/Automatic Signature

Internal User/Automatic Signature in the acceptance phase:

1. Certifies the truthfulness and accuracy of the data connected in these General Conditions, assuming all responsibility pursuant to and for the purposes of the art. 46 of the D.P.R 445 of December 28, 2000;
2. Confirms that the data used for issuing the qualified digital signature certificate are accurate and have been correctly registered;
3. Confirms its willingness to want to activate and use the service requested to Lottomatica Holding S.r.l.;
4. Declares that it has received the information for the use of the service and has consulted the Documents on the QTSP Portal: [**https://ca.firmadigitale.lottomaticaitalia.it;**](https://ca.firmadigitale.lottomaticaitalia.it;)

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021

Classification: PUBLIC

5. Declares to have been informed by Lottomatica Holding S.r.l., as Data Controller, about the primary purposes and the legal basis of the processing of their personal data, using the specific privacy information provided, pursuant to art. 13 of EU Regulation 2016/679 (hereinafter the "Regulation" or also "GDPR"), in the identification phase. The aforementioned privacy information is, however, always available on the website <https://ca.firmadigitale.lottomaticaitalia.it>;
6. Declares to have received and read, before signing, the terms and conditions of use of the Qualified Electronic Signing Service and to approve the contents of General Conditions and in the descriptive documents of the Service, having fully understood how the service is used and the legally binding effects that derive from its use.

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

The QTSP Lottomatica Holding S.r.l. will in no way be liable for the following:

- Damages of any kind, direct and / or indirect, or prejudice caused by anyone caused by:
 - a) Incomplete, false or incorrect information by the proprietor of the information for which the Certification Authority has not stated or is otherwise required to carry out specific checks and verifications;
 - b) Tampering or service interventions made by the Owner or by third parties not authorized by the Certification Authority;
 - c) Impossibility to use the Service determined by a total or partial interruption of call termination or data transmission provided by telecommunications operators solely for facts not attributable to the Certification Authority;
 - d) Erroneous use of identification codes by the Owner;
 - e) Delays, interruptions, errors or malfunctions of the Service attributable to the Certification Authority or arising out of the incorrect use of the Service by the Owner;
 - f) The use of the Service outside of current regulatory requirements;
 - g) Failure to disclose information that the Owner should have communicated to the Certification Authority and / or to the Custodian under the terms of the Contract;
 - h) Breach of obligations that, under the provisions of this document or the law in force, are borne by the Owner;
 - i) Damages of any kind, whether direct or indirect, or prejudiced by anyone who suffered, insofar as they could have been avoided or restricted by the Owners through the proper use of the Service

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

Except as provided for by applicable law, Lottomatica Holding S.r.l. will in no case be liable for direct and / or indirect damages and / or 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 Owner following and / or during the use of the Service due to malfunction of the Service not attributable to Lottomatica Holding S.r.l..

Notwithstanding the foregoing, Lottomatica Holding S.r.l.'s overall liability is limited to compensation for direct and / or indirect damages and / or consequential damages in cases of fraud, guilt or negligence, within the limits set forth in clauses 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 document to the extent specified in chapter 9.2.1.

9.10 SERVICE LIFE AND TERMINATION

9.10.1 Duration

The service Life is aligned at the end of the duration of the certificates issued by QTSP (ref. par. 6.3.2).

9.10.2 Resolution

In the event of a breach of only one of the obligations imposed on the holder, the contract relating to the service shall automatically be construed in accordance with and for the effects referred to in art. 1456 C.C., with contextual revocation of the certificates issued, without prejudice to any action to be taken against the perpetrators of the infringements.

The contract for the service will also be automatically resolved in all cases of revocation of the certificate.

The QTSP has the right to terminate the Service Agreement at any time by giving the Owner 10 (ten) days' notice and, consequently, to revoke the certificates issued.

9.10.3 Effects of cessation

The term "termination" means the process by which the QTSP ceases its activity as a qualified trust service provider.

The QTSP publishes in this document the details of the information connected with the termination procedures, as a result of which the CA certificate is revoked along with all valid certificates at that time.

9.11 NOTIFICATIONS AND COMMUNICATIONS WITH USERS

All communications of a general nature, and possibly urgent ones, are communicated by the QTSP through the **certification portal**.

All personal notifications (certificate issuing, status change, etc.) are notified to subscribers through personal email communication, confirmed by the owner at the time of registration.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

9.12 CHANGES TO THE CPS

QTSP reserves the right to modify the terms included in this document 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 at least 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 associated with the same 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 can accept comments related to the published, through the email address:

firmaqualificata@pec.lottomatica.it → from **01 March 2021** the reference address will be **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.

However, any dispute which arises between the parties in connection with the contract relating to the service will be the exclusive competence of the Court of Rome. In the event that the holder is qualified as a consumer under the Consumer Code (Legislative Decree No. 206 of 2005), the disputes relating to this service contract will be the responsibility of the Court of the place of residence or domicile of the qualified owner as a consumer.

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:

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- 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 [27];
- DPCM 22 Febbraio 2013 [24];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1];
- Regulation (UE) 2016/679 (GDPR) [25].

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

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;
- [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] 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: Publickey and attribute certificate frameworks.

	Typology	REGISTRATION	Code	LTIS-05-00006/18
	Title	QTSP QUALIFIED CERTIFICATION SERVICES - CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY	Revision	5.0
			Date	08/02/2021
Classification: PUBLIC				

- [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 febbraio 2013.
- [25] Applicable national regulation and EU Regulation No 2016/679.
- [26] Codice dell'Amministrazione Digitale (CAD) d.lgs. n.82 7 marzo 2005, e successive modificazioni (d.lgs. 179/2016).
- [27] 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.