Poste Italiane
Digital Signature and Electronic Seal Certification Authority
Certification Practice Statement and Certificate Policy

Copia Archiviata Elettronicamente	Certificate Practice Statement and Certificate Policy_ Digital Signature

Copia cartacea Controllata in distribuzione ad enti esterni	N°:
Rilasciata al	
Copia cartacea non Controllata in distribuzione ad enti esterni	N°:

Versione n.	Redazione	Verifica	Approvazione	Data
1.10	Damiano Perciballi	Damiano Perciballi Luca Gramigna Rocco Mammoliti Tiziana Pittoni Nicola Sotira Sandra Stefani Francesco Tavone Alessandra Toma Carlo Vona	Fabio Sensidoni	10/03/2023

Summary

Document History

Document Change Control

Version	Page	Change	Release date
1		First release	17/02/2017
1.1	51,52	Url for Disclosure Statement Digital Signature document	14/06/2017
1.2	18	Specific agreements with the QTSP Poste Italiane in order to certificate's renewal	05/03/2018
	42	Certificate's profile for verified signature	
1.3	46	Certificate's profile for PosteID	04/09/2018
1.4	51,52	Reference to the rules on the protection of personal data introduced by the GDPR	07/01/2019
	Section 7	Url for CP	
1.5	7.1.10	Certificate's profile for PosteID updated to AgID's public notices n.12 and n.17	18/02/2019
1.6	Section 7.1	Added oid policy agIDcert	06/07/2019
	7.1.2	Policy for EU qualified certificate issued to a legal person	
1.7	Section 7	Certificate's profile for Verified Poste Account	16/07/2020

1.8	Section 4.1	Certificate requests ways	16/02/2021
	7.1	Starting date for oid policy agIDcert	
	9.1	Url for publishing fees of the service	
1.9	Whole Document	Minor changes	06/07/2022
	7.1.2	Certificate Policy Update	
1.10	Whole Document	Minor changes	10/03/2023
	4.6	Certificate Renewal	

1 Introduction

1.1 Overview

This document describes the Digital Signature and Electronic Seal services provided by Poste Italiane.

The procedures adopted to issue the Digital Certificates are reported on the website http://www.postecert.it/ and https://www.poste.it/prodotti/firma-digitale-remota.html .

This document represents the CPS and CP adopted by Poste Italiane to manage the certificates and the encryption keys related to Digital Signature and Electronic Seal.

This Document describes techniques, policies and procedures of the CA personnel in some services and in the entire life cycle of certificate solutions that are issued by Poste Italiane. The structure and contents of this CPS and CP are based on the guidelines specified by the **RFC 3647** standard.

In addition, Poste Italiane ensures its compliance with the requirements identified in the documents: **ETSI EN 319 411-1** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates" from ETSI (available on the website http://www.etsi.org).

1.2 Document Name and Identification

Poste Italiane ensures compliance of its certificates with the requirements and assertions of this document.

Poste Italiane Certification Authority takes control in order to guarantee the CPS and CP deals, which is identified by the unique Object Identifier (OID), in the form required in Recommendation ITU-T X.509 is 1.3.76.48.1.4.1.1.

1.3 PKI Participants

1.3.1 Certification Authority

The Certification Authority is a third and trusted part that issues the certificates and signs them with its private key (CA key). In addition to that, the CA manages the certificates

status. The role of the CA, with reference to the service described, is performed by Poste Italiane, a company that can beidentified as follows:

Company Name	**Poste Italiane S.p.A.**
VAT Number and Tax Code	01114601006
Registered Office	VIALE EUROPA 190 ROMA (RM) 00144
Telephone	+39 06 59581
Certified e-mail address	poste@pec.posteitaliane.it
Indirizzo Internet	http://poste.it

1.3.2 Registration Authority

The Registration Authority (RA) is the person, the structure or the organization that performs the following activities:

- Acceptance and validation of requests related to certificates issuance and management;
- Registration of the Subscriber and the related organization;
- Authorize the CA to issue the requested certificates;
- Certificate provision and subsequent notification to the client.

The RA activity is performed by Poste Italiane employees as indicated in Internal Organization and Responsibility Procedures.

1.3.3 Subscriber

The Subscriber is a natural person or a legal person that requires a certificate and holds the related private key.

1.3.4 Relying Parties

Relying parties are natural or legal persons that rely on a certificate and/or on a digital signature, that is verifiable with reference to a public key listed in a subscriber's certificate. In order to verify the validity of a digital certificate, relying parties must always refer to Poste Italiane CA revocation information such as a Certificate Revocation List (CRL).

Relying parties meet specific obligations as described in this document.

1.4 Certificate Usage

Certificates issued by Poste Italiane are valid in order to apply Digital Signatures and Electronic Seals on electronic documents (i.e. such as electronic mail and retail transactions).

It is forbidden any misuse of the certificates issued by Poste Italiane in relation to this document and Disclosure Statement. If Poste Italiane gains knowledge of any misuse, the certificate is immediatly revoked.

It is assumed that the client has the competence and the necessary knowledge to properly use the certificate.

1.5 CPS and CP Administrations

This document is edited, published and updated by Poste Italiane. Any change to this document is submitted to the internal review process, is approved by the Top Management and notified to Italian Digital Agency (AgID) and to the certification body.

Any question or clarification concerning this document may be forwarded by mail to poste@pec.posteitaliane.it.

1.6 Definitions and acronyms

AgID: National Digital Agency

Certification Authority (CA): authority trusted by one or more users to create and assign certificates.

Certification Body: Third party auditor, part of national supervisory body's processes.

Certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates.

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.

Digital Signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Electronic Seal: 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.

Hardware Security Module (HSM): An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.

Public Key Infrastructure (PKI): entity that is responsible for identification and authentication of subjects of certificates mainly.

PKI Disclosure Statement (PDS): a supplemental instrument of disclosure and notice by a Certification Authority.

Public Key Infrastructure (PKI): set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Qualified electronic Signature/Seal Creation Device (QSCD): device responsible for qualifying a digital signature.

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates.

Relying party: Person or organisation acting upon a Certificate, typically to verify signatures by the Subscriber or to perform encryption towards the Subscriber. The Relying Party relies upon the accuracy of the binding between the Subscriber public key distributed via that Certificate and the identity and/or other attributes of the Subscriber contained in that Certificate.

Subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Subscriber: Person or organisation contracting with the Certification Authority, for being issued one or more Certificates.

1.7 References

[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
[2] ETSI EN 319 411-1: "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 – "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] ETSI EN 319 412-1 – "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures"
[5] ETSI EN 319 412-2 – "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons"
[6] ETSI EN 319 412-3 – "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"
[7] ETSI EN 319 412-4 – "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations"
[8] ETSI EN 319 412-5 – "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements"
[9] IETF (RFC3647) https://www.ietf.org/rfc/rfc3647.txt

2 Publication and Repository Responsibilities

2.1 Repository Management

Poste Italiane "repository" consists in the CA services website http://postecert.poste.it/ and https://www.poste.it/prodotti/firma-digitale-remota.html in the Italian and English version.

The CA manages the repository independently and it is directly responsible for it.

2.2 Publication of certification information

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

- Certification Practice Statement (CPS);
- Certificate Policy (CP);

- Terms of Service;
- Operating instructions
- Application forms.

2.3 Time and frequency of publications

This Document and the attached documents are published on the CA's website every time they are updated.

2.4 Access control on published information

This Document and the attached documents are publicly available in the "pdfa" format.

3 Identification and Authentication (I&A)

3.1 Naming

Poste Italiane issues each Certificate in compliance with the following Standards:

- ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

The certificates report the value "*no repudiation*" for the *key Usage* extension. The field "subject" on the certificate reports understandable information which may allow to identify the certificate owner (legal or natural person).

In case of certificates for natural person, the field "subject" contains, at least:

- countryName;
- givenName and surname
- commonName

In case of certificates for legal person, the field "subject" containss, at least:

- countryName;
- organization Name
- organizationIdentifier

- commonName (OID 2.5.4.3)

3.2 Initial Identity Validation

The identity validation process involves the verification by Poste Italiane of the identity of the Subscriber or the identity of a natural person representing the organisation. Poste Italiane will ask the Subscriber to provide identity information and supporting documents as required to perform the identification.

The procedures to release a qualified certificate are:

- Registration
- Identification

The employees of the Registration Authority or a delegate office conduct the registration and identification which is under Poste Italiane control and responsability.

The delegate office can be conducted:

- By the Poste Italiane employees;
- By the entity to which Poste Italiane delegates the identification activities.

The identification is based on documents that are applicable in the local country, such as a valid personal identification document. Poste Italiane stores the identification documents and retains this information for the required period (20 years).

Poste Italiane can issues certificates to itself, according to ETSI EN 319 411-1 clause 6.2.2 q, because the organization runs all the RA tasks.

Poste Italiane can issue qualified certificates with OIDs 1.3.76.16.5 identifying the Subscriber through Sistema Pubblico di Identità Digitale (SPID), according to public notice n. 12 and n. 17 by supervisor body AgID (cf. 7.1.10).

3.3 I&A for Re-key Requests

The renewal of the certificates (where provided for in specific agreements with the Subscribers) must respect 2 conditions: the certicates must not be expired and the renewal request must be presented within the last 60 days of validity.

Subscribers will receive an email 60 days before reminding them of the certificate's expiration.

3.4 I&A for Revocation Requests

Subscribers, Third parts and Applicants may request the certificate revocation; the procedures for the revocation requests are:

- on-line procedure: online revocation service that is accessed through the code of practice and an appropriate revocation code. This option is only available to the subscriber because it is the only one who is expected to know the confidential personal codes.
- Digital Signature and Electronic Seal procedures: sending to Poste Italiane an email containing the digital revocation request signed by the subscriber and/or the organization representive.
- Printed format procedure:
    - Subscriber: presentation to a Delegate Office of the signed request;
    - Delegate office sends the request to Poste Italiane by email or fax;
    - Third part: sending to Poste Italiane by mail the identity documents and the signed request.

According to Standards ETSI 319 411-1:

- The maximum delay between the receipt of a revocation or suspension request or report and the communication of the decision to change its status information to all the relying parties is at most 24 hours.
- The maximum delay between the confirmation of a certificate revocation, or its suspension, and the the communication of the certificate information status change to all the relying parties is at most within 60 minutes.

4 Certificate Life-Cycle Operational Requirements

Unless differently stated in this document and in accordance with the ETSI 319-411, the following operational requirements are applied to certificates' lifecycle. All the entities included in the Poste Italiane domain (RA, Subscribers or other participants) must notify to Poste Italiane CA all the changes to the information reported on a certificate during its operational period and until it expires or it is revoked. Poste Italiane CA will issue, revoke or suspend the certificates only in response to authenticated and approved requests.

4.1 Certificate Application

The Certificate Requests may be submitted in two ways:

- On-line: through Poste.it portal https://www.poste.it/prodotti/firma-digitale-remota.html, after authentication with personal access credentials.

- direct relationship: through an agreement signed with the physical presence of the organization representative and Poste Italiane delegate.

In both cases, the Subscribers are subject to a registration process, which requires the following requirements:

- Filling out an application form;
- Acceptance of the "Subscriber Agreement" or the "Terms of Service".

4.2 Certificate Application Processing

Upon receipt of a request for certification, Poste Italiane (or its delegate) carries out appropriate verification activities, such as verifying the registration and the identity of the subscriber.

After the registration, the subscriber shall go to the delegate office carring documents required for the identification and contractual and registration documentation. Additional documentation is also required in relation to the type of Certificate. The employee receives the documentation submitted by the subscriber and verifies the validity of the document. In case of the issue of certificates is carried out on the request of the Applicant, the request will be subject to specific agreement between the Certification body and the Applicant.

Certificate Application is processed within 30 days.

4.3 Certificate Issuance

If the results of the verifications reported on the previous section are positive, the RA will send to the CA a certificate issuance request. The process of generating key occurs inside the signature device.

4.4 Certificate Acceptance

By using the certificate generation activation described in internal procedure (Certificate Life Cycle Management), the Certificate is automatically generated and accepted.

4.5 Key Pair and Certificate Usage

The certificate Owner must safeguard its private key, paying attention to avoid its disclosure to third parties.

Poste Italiane will provide an appropriate subscription agreement, which highlights the owner's duties regarding the private key protection. The private keys must be used only as specified in the fields "*keyUsage"* and "*extendedkeyUsage"*, as reported on the related

digital certificate. If it is possible a backup of the private key, the owner must safeguard it with the same level of care and protection given to the private key. Once the key service life is ended, the owner must safely eliminate the key and the sections, which had been split into it during the backup process.The responsibilities related to the use of keys and certificates include the ones addressed below. Certificates shall be only used as prescribed by the CP and Terms and Conditions. Any different usage is forbidden. Specifically, they may not be used for infringing rights or for violations of any kind of laws or regulations.

4.6 Certificate Renewal

The renewal service is not available for certificates issued on smart card devices and HSMs.

The Subscriber who intends to continue using the certification service must request a new smart card and certificate.

Alternative frequency and methods may be defined in agreements between the parties.

4.7 Certificate modification

A certificate being signed by the issuer CA cannot be modified. In order to remediate to potential inaccuracies incurred during the generation process, it is necessary to issue a new certificate and, for security reasons, revoke the previous one. In case of the issued certificate reports incorrect information, due to mistakes made by the CA or the RA, the wrong certificate will be revoked and a new one will be promptly issued without any additional charge for the client and without requesting further information to the client. On the other hand, if the issued certificate reports incorrect information due to mistakes made by the Subscriber (e.g. incorrect compilation of one or more fields on the application form), the wrong certificate will be revoked.

4.8 Certificate Revocation and Suspension

The suspension of a certificate causes a temporary block of its validity, starting from a given time (date/time).

The revocation of a certificate causes the anticipated expiration of its validity, starting from a given time (date/time). The revocation of the certificate is irreversible and not backdated. The suspension and the revocation of a certificate are carried out by generating and publishing a new CSL (Certificate Suspension List) or CRL (Certificate

Revocation List) which includes the serial number of the suspended/revoked certificate.

The CSL and CRL are freely available to anyone who needs to verify the certificate state.

The publication of CRL and CSL takes place, however, at maximum every 24 (twenty-four) hours.

4.9 Circumstances for revocation

The following conditions may cause the revocation of a digital certificate:

- loss, theft, modification, not authorized disclosure or any other damages of the certificate subject's private key;
- alteration of information reported on the certificate and related to the certificate subject;
- errors during registration process;
- existence of judicial proceedings (e.g. following illegal activities committed by the certificate owner entity);
- cessation of business by the certificate owner entity;
- specific request made by the owner (e.g. due to end of use of the certificate);
- breach of contract by the client (e.g. failure to pay).
- Poste Italiane can revoke the certificates in case of non-compliant suspect uses, upon notice to the relying parties, except in urgent cases.

4.9.1 Circumstances for suspension

The following conditions may cause the suspension of a digital certificate:

- The subscriber, the applicant and the third part, for any reasons and in any moment, may request the certificate suspension.
- Poste Italiane can suspend the certificates in case of non-compliant suspect uses, upon notice to the relying parties, except in urgent cases.

4.10 Certificate Status Services

Poste Italiane CA provides control services to verify the state of the certificate, such as CRL, CSL and OCSP. The status of the certificate (which could be active, suspended or revoked) is made available to all the involved entities by publishing the Certificate Revocation List (CRL) or the Certificate Suspension List (CSL). The CA makes also available an OCSP (On-line Certificate Status Provider).

4.11 End of Subscription

The service contract, subscribed by the CA and the client, is considered terminated at the following dates:

- certificate expiration date;
- certificate revocation date.

4.12 Key Escrow and Recovery

Key escrow is not allowed for the CA key. The private keys are backuped by Poste Italiane to ensure continuity solutions through disaster recovery site.

5 Facility, Management, and Operational Controls

Policies, responsibilities and operating procedures are defined to access in protected areas of Poste Italiane and to access to information and application system.

In these areas, physical protection devices are implemented to minimize risks related to unauthorized accesses. The protection is implemented by access control systems and video surveillance systems located in the most critical points and marked by specific signs.

A Disaster Recovery Site is placed in Turin with the same level of physical security of the primary site.

5.1 Physical Controls

The working areas are under different control measures, related to risks, goods' value and information in the environment. An organized authorization process, related to the kind of accessed area, manages all theaccesses.

5.1.1 Site Location And Construction

Poste Italiane performs its CA operations from secure, geographically diverse, data centers that are equipped with logical and physical controls that make Poste Italiane's CA operations inaccessible to non-trusted personnel. Poste Italiane operates under a security policy designed to detect, deter, and prevent unauthorized access to Poste Italiane's operations.

5.1.2 Physical Access

Poste Italiane protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of Poste Italiane

CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals.
Access to secure areas of the buildings requires the use of a secure device. The buildings are under constant video surveillance.

DATACENTER
Access to Datacenter requires smartcard authentication and CMP (a device containing authorizations to access the protected room). Regulations on how to access and behave in the Data Center are affixed outside the Data Center.

5.1.3 Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and electrical generators provide redundant backup power. Poste Italiane's Datacenter facilities use multiple systems for heating, cooling and air ventilation.

5.1.4 Water Exposures

A detection system that detects the presence of liquid through sensors and alarms in case of flooding.

5.1.5 Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6 Media Storage

Poste Italiane protects its media from accidental damage and unauthorized physical access.

5.2 Procedural Controls

5.2.1 Trusted roles

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel related to identity vetting and the issuance and revocation of certificates. The functions and duties performed by persons in trusted roles are distributed to allow that just a person cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations by himself. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the Poste Italiane

PKI's operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.
Trusted roles include roles that involve the following responsibilities:

- **Security Officers (Security Practicers):** Overall responsibility for defining security practices. Security Officers ensure the confidentiality, integrity and availability of data and business applications related to the Digital Signature.
- **Security Officers (Authorization):** Overall responsibility for authorizing System Administrator and System Operators in the implementation of the security practices
- **System administrators:** Authorized to install, configure and maintain the Poste Italiane trustworthy systems for service management
- **System operators:** Responsible for operating the Poste Italiane trustworthy systems on a day-to-day basis. Authorized to perform system backup.
- **System Auditors:** Authorized to view archives and audit logs of the Poste Italiane trustworthy systems.
- **Registration and revocation officers:** Responsible for keys management life cycle with reference to revocation and suspension services of certificates for Digital Signature and Electronic Seal keys.
- **Service Responsible:** Responsible for Digital Signature and Electronic Seal Service, operating manual and the processes for the life cycle management, in according with specific regulatory aspects.
- **Marketing Responsible:** Responsible for Digital Signature and Electronic Seal evolution in according with regulatory constraints and indications of the market.
- **Development Responsible:** responsible for development projects of digital signature and timestamping.

More information can be found in internal policies.

5.2.2 Number of Persons Required per Task

In case of tasks related to critical functions, Poste Italiane requires that at least two people acting in a trusted role to avoid that a person can act by himself. When this mechanism is active, two authorised persons arerequired to apply it where appropriate. More information can be found in internal policies.

5.2.3 Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA and RA systems before accessing to systems necessary to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

Roles requiring a separation of duties, thatinclude:

1. The verification of information in certificate applications;
2. The approval of certificate applications;
3. The approval of revocation requests;
4. Most duties related to CA key management or CA administration.

Poste Italiane specifically designates individuals to the trusted roles defined above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. Poste Italiane's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 Personnel Controls

The employees have many years of experience in definition, development and management of PKI services and have received an adequate level of training on procedures and tools, that canbe used in various operational phases.

Poste Italiane employees and contractors:

- possess the necessary expertise, reliability, experience, and qualifications and have received training regarding security and personal data protection rules as appropriate as the offered services and their job function;
- are able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of both;
- are updated on new threats and current security practices.

5.3.1 Qualifications, Experience, and Clearance Requirements

Poste Italiane hires personnel with the highest levels of integrity and competence. A comprehensive set of personnel screening activities and related evaluation criteria has been defined to be able to detect risks in this matter. There is no citizenship requirement

for personnel performing trusted roles associated with the issuance of other kinds of certificates.

5.3.2 Background Check Procedures

Poste Italiane verifies the identities and performs a background check of each person to schedule someone for a trusted role. Poste Italiane, also, requires that each person must appear in-person in front of a human resources employee who is responsible to verify identities. The human resources employee verifies the identities using the required forms of government-issued photo identification. The Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background.

5.3.3 Training Requirements

All new Poste Italiane personnel receive basic security awareness training during their introduction process. On top of that, a dedicated on-the-job training is provided to all Poste Italiane personnel involved in specific tasks as described throughout this Certification Practice Statement.

5.3.4 Retraining Frequency and Requirements

Personnel must maintain high skill levels through industry-relevant training sessions and performance programs in order to continue acting in trusted roles. Poste Italiane updates all individuals acting in trusted roles about any changes to Poste Italiane's operations. If Poste Italiane operations change, Poste Italiane will provide documented training, in accordance with an executed training plan, to all personnel acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

In case of job rotation, Poste Italiane performs a security check, including a verification of credentials at level of networks, systems, applications or other assets used as well as the facility and zone access authorizations.

5.3.6 Sanctions for Unauthorized Actions

Poste Italiane employees and agents, who don't comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions.

5.3.7 Independent Contractor Requirements

Independent contractors, who are assigned to perform trusted roles, are subject to specific duties and requirements for each role and are subject to sanctions as specified in this section.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the present document and operational documentation needed to maintain the integrity of Poste Italiane CA operations. Personnel have also access to information on internal systems and to security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4 Audit Logging Procedures

Poste Italiane records all relevant information concerning data issued and received by Poste Italiane and keeps the records accessible for an appropriate period, with the purpose of providing evidence in legal proceedings and ensuring service continuity. In particular:

- The confidentiality and the integrity of current and archived records concerning operation of services are maintained;
- Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices;
- Records concerning the operation of services are made available if required for the purposes of providing evidence of the services correct operation and for the purpose of legal proceedings;
- The exact time of significant Poste Italiane environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log shall be synchronized with UTC at least once per day;
- Records concerning services are held for an appropriate period in order to provide necessary legal evidence as notified in the Poste Italiane terms and conditions;
- The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period in that they are required to be held.

More information can be found in internal policies.

5.5 Records Archival

Poste Italiane does and keep accessible records including all the activities and all relevant information concerning data issued and received by Poste Italiane.

The CA keeps the records accessible for an appropriate period, with the purpose of providing evidence in legal proceedings and ensuring service continuity. These records are accessible even in the case in which Poste Italiane have ceased its activities.

The main evidence collected are:

- Issuance requests;
- The documentation provided by Subscribers;
- The CSR (Certificate Signing Request) provided by Subscribers;
- Subscribers and end users personal data (if they are different entities);
- Requests for revocation or suspension;
- All certificates issued;
- Audit logs for more than 20 years.

More information can be found in internal policies.

5.6 Key Changeover

In case of the end user (owner) decides to use a new key, he must necessarily request a corresponding new certificate.

5.7 Compromise and Disaster Recovery

Poste Italiane documents applicable incident, compromise reporting and handling procedures. Poste Italiane documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted. Poste Italiane establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

More information can be found in internal policies.

5.8 CA or RA Termination

Poste Italiane defined an up-to-date termination plan.

In particular, according to the internal procedure, Poste Italiane shall:

- inform at least 60 days before the termination the following entities entities about the termination: all subscribers and other entities with which Poste Italiane has

agreements or other form of established relations, among which relying parties, Poste Italiane and relevant authorities (AgID and the certification body). In addition, this information shall be made available to other relying parties;

- terminate all subcontractors authorization to act on behalf of Poste Italiane in carrying out any functions related to the process of issuing trust service tokens;
- transfer obligations to a reliable party for maintaining all the necessary information to provide evidence of Poste Italiane operation for a reasonable period, unless it can be demonstrated that Poste Italiane does not hold any information;
- private keys, including backup copies, shall be destroyed, or withdrawn, to assure that the private keys cannot be retrieved;
- make arrangements to transfer provision of trust services for its existing customers to another Poste Italiane.

More information can be found in internal procedure "Termination Plan".

6 Technical Security Controls

6.1 Key Pair Generation

The CA issues the qualified certificate in according with the Regulation (EU) No 910/2014. The certification keys used for signing certificates are generated by means of devices and procedures that ensure uniqueness, secrecy and resilience of the private key.

The CA uses at least 4096-bit cryptographic key pair generated within HSM (Hardware Secure Module).

The HSMs and procedures ensure that:

- the key pairs are generated individually, alwaysin single copy;
- the key pairs meet requirements imposed by generation algorithms and RSA verifications because the HSMs have a key pair generation internal engine of RSA and DSA;
- the generation of all possible key pairs is equiprobable;
- the owner who activates generation procedures is always identified;
- the generation of key pairs occurs exclusively inside the HSM, that is responsible for preservation of private keys;
- if the devices are prepared or managed by a third party, Poste Italiane verifies that this third party is meeting the appropriate requirements.

In the certificate activities, Poste Italiane uses the RSA algorithm.

The generation of key pairs of certification by CA is under dual control, in according to Key Ceremony procedure.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The key pairs used by the CA to sign certificates and CRLs are stored in a HSM (Hardware Security Module) of high quality, provided with safety certification in accordance with FIPS 140-2 EAL4 + AVA_VAN.5.

6.3 Other Aspects of Key Pair Management

Poste Italiane uses appropriately the CA private signing keys and don’t use them beyond the end of their life cycle.

In particular:

- CA signing key used for generating certificates and/or issuing revocation status information, is not used for any other purpose;
- The certificate signing keys are only used within physically secure premises;
- The use of the CA's private key is compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with section 6.1;
- All copies of the CA private signing keys will be destroyed at the end of their life cycle.

6.4 Activation Data

Activation Data consists in activation of all sistems involved in delivering of digital signature and electronic seal; these activities are managed by Operative Guide.

Certificate issuance by Poste Italiane is under at least dual control by authorized, trusted personnel.

6.5 Computer Security Controls

The operating systems used by the CA to manage certificates have a level of security appropriate and shall

follow the hardening procedures set out by Poste Italiane. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuses of Poste Italiane assets.

The access events to systems are recorded, as described in section 5.4 and 5.5.
Local network components are kept in a physically and logically secure environment and their configurations are periodically checked for compliance with the requirements specified by Poste Italiane.
Multi-factor authentication are implemented for all accounts capable of directly causing certificate issuance.
Access control on attempts to add or delete certificates and modify other associated information (e.g. revocation status information) are implemented.
Continuous monitoring and alarm facilities are provided to enable Poste Italiane to detect, register and react in a
timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.6 Life Cycle Security Controls

Poste Italiane uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
In particular:

- An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by Poste Italiane;
- Change control procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the Information security policy.
- The integrity of Poste Italiane systems and information are protected against viruses, malicious and unauthorized software.
- Media management procedures are defined and implemented in order to protect media from damage, theft, unauthorized access, obsolescence and deterioration of media within the period of time that records are required to be retained.
- Organizational Procedures are defined and implemented in order to manage all trusted and administrative roles that impact on the provision of services.

In order to issue and manage CA keys in a secure way, Poste Italiane use HSM (Hardware Security Module), which:

- Are tamper-proof and guarantee the protection of the Keys According to the Security Levels expected from the Regulation and the high technological standard;
- prevents any unauthorized attempt of Reading, duplication, extraction of the private key;
- keeps the Private Key to ensure its protection, privacy and safe storage for the whole Life Cycle;
- identifies operators;

6.7 Network Security Controls

Poste Italiane's network architecture is structured on several levels in order to create separated network environments, addressed to host systems related to different functions and characterized by different levels of criticality.

The access and the network traffic security is realised by the application of protection policies implemented on the firewall systems located on different network levels.

The implementation requests of new rules on the firewall, are managed through a change request.

The activation of rules that cause a high impact level, is dealt with the Security Officer.

The CA private network security is realised not just by the perimeter protection systems described backwards, but also by a specific configuration, which maintains the internal addresses as reserved. The communication between the management stations and the systems are protected by means of tools which assure the authentication among the parts and their privacy.

Potential remote links take place on an encrypted VPN channel and request the authentication through Usename, Password and an authentication token (OTP).

The communication among application forms of Poste Italiane's PKI platform occurs through cryptographic channels.

The communication among users who access to the online services takes place through SSL connections with SHA-256 algorithm.

The system implemented to manage users' accesses gives both AAA (authentication, authorization, access) and profiling mechanisms and the communication channel encryption with TLS/SSL protocol.

The sistem is also supposed to manage the accesses that come from the consultants who work on the internal Poste Italiane Network.

6.8 Timestamping

All processing systems used by the CA are aligned with the UTC time and synchronized with a reliable source (through NTP server).

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates are compliant with:

- international standard ISO/IEC 9594-8:2005 [X.509 version 3] ;
- public specification IETF RFC 5280 management of reliable public certificates;
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles (Part 1, 2, 3, 5).
- Determinazione N. 121-147/2019 of AgID, Italian superbody, starting from July 2019.

The issuing CA fills the issuer and the subject fields of each certificate issued after the adoption of requirements, defined above, in accordance with what is stated in the Certificate Policy.

With the issuance of the certificate, the CA declares to have followed the procedure described in its CP to prove that, at the date of certificate issuance, all information related to the subject were accurate.

7.1.1 Qualified Certificates CA "Poste Italiane EU Qualified Certificates CA"

Version	Version 3
Serial Number	Serial number of the certificates
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName** : "IT" **organizationName**: "Poste Italiane S.p.A." **organizationIdentifier** : "VATIT-01114601006" **commonName** : "Poste Italiane EU Qualified Certificates CA"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit

	Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critical)	Subject Type: CA Path Length Constraint:0
KeyUsage (critical)	CertSign, cRLSign
Authority Information Access	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA
Certificate Policies (not critical)	Policy OID, 1.3.76.48.1.4.1.1 Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl
Policy Constraints	requireExplicitPolicy : 0

7.1.2 QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (eSeal)

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	3 Years
Subject (ETSI 319 412-3 par. 4.2.1 - Subject) (ETSI 319 412 -1 par.5.1.4 - Legal person semantics identifier)	**countryName (OID 2.5.4.6):** *CountryName contains the ISO 3166 country code of the holder's residence* **organization Name (OID 2.5.4.10):** *OrganizationName contains full registered name of the subject (legal person).* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 -1): *VAT or NTR||Code country||-|| identifier* **commonName (OID 2.5.4.3):**

	Organization name Holder of the certificate or process / office of competence within which the Seal is issued **Dn_Qualifier (OID: 2.5.4.46):** *'4'||y where y represents the unique identification code of the Subject at the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Subject Alternative Name RFC822 Name certificate holder e-mail	certificate holder e-mail (optional)
Qualified Certificate Statements (not critical) (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-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) – *it is present if negotiation limits are applicable* qcStatements-5 QcEuPDS (0.4.0.1862.1.5) https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-eseal (0.4.0.1862.1.6.2)
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt

Certificate Policies (not critical) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.4 (automatic signature)User notice: "Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures" NCP+ (0.4.0.2042.1.2) QCP-l-qcsd (0.4.0.194112.1.3) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf Policy: 1.3.76.16.6
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.3 Owner: QCP-n-qscd-T-R - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD for remote signature.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier* *Example 1: registered subject with passport* PASIT-*passport number*

	Example 2: registered subject with tax code TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical) OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.1 (remote signature) Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.4 Owner: QCP-n-qscd-T-A - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD for automatic signature.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier* *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA

Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical) OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.2 (automatic signature)User notice: "Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures" Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.5 Owner: QCP-n-qscd-T-S - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD smartcard.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname

Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier* *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation

Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical) OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.3 (smart card) Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.6 Members of organization: QCP-n-qscd-O-R - Policy for EU qualified certificate issued to a natural person (corporate) where the private key and the related certificate reside on a QSCD for remote signature.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **organization Name (OID 2.5.4.10):** **organizationIdentifier (2.5.4.97)** (ETSI 319 412 -1, ETSI 319 412-2 par.4.2.4): *VAT or NTR||Code country||-||identifier* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT*

	Surname (OID 2.5.4.4): *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-||identifier* *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'3'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role or title conducted by the Subject in the organization (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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-2 QcEuLimitValue (0.4.0.1862.1.2) – *it is present if negotiation limits are applicable* qcStatements-5 QcEuPDS (0.4.0.1862.1.5) https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt

Certificate Policies (not critical) OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.1 (remote signature) Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.7 Members of organization: QCP-n-qscd-O-A - Policy for EU qualified certificate issued to a natural person (corporate) where the private key and the related certificate reside on a QSCD for automatic signature.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **organization Name (OID 2.5.4.10):** **organizationIdentifier (2.5.4.97)** (ETSI 319 412 -1, ETSI 319 412-2 par.4.2.4): *VAT or NTR||Code country||-||identifier* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-||identifier*

	Example 1: registered subject with passport PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'3'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role or title conducted by the Subject in the organization (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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-2 QcEuLimitValue (0.4.0.1862.1.2) – *it is present if negotiation limits are applicable* qcStatements-5 QcEuPDS (0.4.0.1862.1.5) https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.2 (automatic signature) User notice: "Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures"

OID agIDcert	Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.8 Members of organization: QCP-n-qscd-O-A-v - Policy for EU qualified certificate issued to a natural person (corporate) where the private key and the related certificate reside on a QSCD for automatic signature - verified signature.

Version	Versione 3
Serial Number	Numero di Serie del certificato
Signature Algorithm	Sha256, RSA
Issuer	Dname della CA
Validità	3 Anni
Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **organization Name (OID 2.5.4.10):** **organizationIdentifier (2.5.4.97)** (ETSI 319 412 -1, ETSI 319 412-2 par.4.2.4): *VAT or NTR||Code country||-||identifier* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42):** *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4):** *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-||identifier* *Example 1: registered subject with passport*

	PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** '3'||*y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role or title conducted by the Subject in the organization (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algoritmo utilizzato: RSA
Estensioni	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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-2 QcEuLimitValue (0.4.0.1862.1.2) – presente se sono applicabili limiti nelle negoziazioni. qcStatements-5 QcEuPDS (0.4.0.1862.1.5) https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critica)	No 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://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical)	Policy OID 1.3.76.16.3 (verified signature) User notice: "The qualified certification service provider that issued this certificate ensures that the signatures based on this certificate have

	been generated during the period of validity of the certificate./Il certificatore garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme" Policy OID 1.3.76.48.1.2.3.2 (automatic signature) User notice: "Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures."
OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/TSPdoc/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.9 Members of organization: QCP-n-qscd-O-S - Policy for EU qualified certificate issued to a natural person (corporate) where the private key and the related certificate reside on a QSCD smartcard.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **organization Name (OID 2.5.4.10):** **organizationIdentifier (2.5.4.97)** (ETSI 319 412 -1, ETSI 319 412-2 par.4.2.4): *VAT or NTR*||*Code country*||-||*identifier*

	commonName (OID 2.5.4.3): *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-* *||identifier* *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'3'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role or title conducted by the Subject in the organization (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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-2 QcEuLimitValue (0.4.0.1862.1.2) – *it is present if negotiation limits are applicable* qcStatements-5 QcEuPDS (0.4.0.1862.1.5) https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA

RFC 5280	Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical) OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.48.1.2.3.3 (smart card) Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/*TSPdoc*/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.10 QCP-n-qscd-T-R-PosteID-free - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD for remote signature (identity provided by PosteID) – released free of charge

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier*

	Example 1: registered subject with passport PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical)	Policy OID 1.3.76.48.1.2.3.1 (remote signature) User notice: -L'uso del presente certificato è limitato all'ambito dei servizi del Gruppo Poste Italiane e del fondo negoziale FondoPoste (di cui Poste Italiane è parte istitutiva);

OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	-The use of this certificate is limited to the scope of services of Poste Italiane and of the Negotiating Group FondoPoste (of which Poste Italiane Office is part of the Establishment); Policy OID 1.3.76.16.5 (through SPID) User notice: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity" Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/TSPdoc/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.11 QCP-n-qscd-T-R-PosteID - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD for remote signature (identity provided by PosteID)

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3)

	PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number* **Dn_Qualifier (OID 2.5.4.46):** *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical)	Policy OID 1.3.76.48.1.2.3.1 (remote signature) Policy OID 1.3.76.16.5 (through SPID) User notice: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity"

OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/TSPdoc/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.1.12 QCP-n-qscd-T-R-APV-free - Policy for EU qualified certificate issued to a natural person (retail) where the private key and the related certificate reside on a QSCD for remote signature (verified Poste account) – released free of charge.

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	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)	**countryName (OID: 2.5.4.6):** *countryName contains the ISO 3166 country code of the holder's residence* **commonName (OID 2.5.4.3):** *SURNAME NAME* **givenName (OID 2.5.4.42)**: *EXTENDED NAME OF THE SUBJECT* **Surname (OID 2.5.4.4)**: *EXTENDED SURNAME OF THE SUBJECT* **SerialNumber (OID 2.5.4.5):** (ETSI EN 319412-1 par. 5.1.3) *PAS or IDC or PNO or TIN or "xx":||Code country||-|| identifier* *Example 1: registered subject with passport* PASIT-*passport number* *Example 2: registered subject with tax code* TINIT-*tax code number*

	Dn_Qualifier (OID 2.5.4.46): *'0'||y where y represents the unique identification code of the Subject at the CA* **Title (OID 2.5.4.12):** *Role selected during the registration (it is present only if the role is present)*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extention	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
QC_Statements (not critical) (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://postecert.poste.it/TSPdoc/pi-QUCApds.pdf
KeyUsage (critical)	No Repudiation
Authority Information Access *Regulation (EU) N 910/2014 Annex I (clause h)* *RFC 5280*	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL:http://postecert.poste.it/pi-ocspTSPQUCA Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: http://postecert.poste.it/pi-TSPQUCA/CA.crt
Certificate Policies (not critical)	Policy OID 1.3.76.48.1.2.3.1 (remote signature) User notice: -L'uso del presente certificato è limitato all'ambito dei servizi del Gruppo Poste Italiane e del fondo negoziale FondoPoste (di cui Poste Italiane è parte istitutiva); -The use of this certificate is limited to the scope of services of Poste Italiane and of the Negotiating Group FondoPoste (of which Poste Italiane Office is part of the Establishment);

OID agIDcert (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	Policy OID 1.3.76.16.6 (agIDcert) NCP+ (0.4.0.2042.1.2) QCP-n-qcsd (0.4.0.194112.1.2) Cp: URL: https://postecert.poste.it/TSPdoc/pi-QUCAcps.pdf
crlDistributionPoint (not critical)	http://postecert.poste.it/pi-TSPQUCA/crl.crl

7.2 CRL Profile

The CRLs is compliant with the public specification RFC 5280.

7.3 OCSP Profile

The OCSP is compliant to the public specification RFC 2560. The CA maintains track of the OCSP profile in a separate technical document, made available, on request, at the discretion of Poste Italiane.

8 Compliance Audit and Other Assessment

Poste Italiane is a Trusted Service Provider for the qualified digital signature and electronic seal, accredited by a certification body, accredited by Accredia. The conformity assessment report is sent to the AgID. As a result, Poste Italiane is subject to a compliance assessment ("surveillance") by AgID and is required to carry out periodic internal inspection.

8.1 Frequency and circumstances of assessment

Poste Italiane auditor is responsible for internal audits on Digital Signature and Electronic Seal services, verifying that the processes compliance in according to requirements of legislation and regulations of the corporate procedures. The internal audit is taken at least once a year.

Third party audit performed by a certification body, accredited by Accredia, is carried out with annual periodicity.

8.2 Identity and qualifications of assessors

Internal audit are carried out by Poste Italiane' auditors, qualified as a security auditors in accordance with
the international standard ISO 27001 and ISO 9001.

8.3 Assessor's relationship to assessed entity

There is no relationship between Poste Italiane and the certification body that may in any way influence audit results in favor of Poste Italiane.
Poste Italiane auditors are employees who reports directly to the Management and are independent structure responsible in comparison with Service Responsible.

8.4 Topics covered by assessment

The certification body carries out conformity assessment of Poste Italiane activities, supervised by AgID, that operate in respect of EU Regulation 910/2014, known as "eIDAS-Electronic Identification Authentication and Signature".
Internal audit is mainly aimed at verifying the integrity of the "Journal of Control" (Audit log), and the respect of CA's operating procedures.

8.5 Actions taken as a result of deficiency

In case of compliance deficiencies, Poste Italiane adopt the necessary corrective measures that are tracked until resolution.

8.6 Communication of results

Audit results, carried out by the certificatory auditor, are shared with the interested CA through a conformity assessment report. The internal audit result is communicated to the Management and to the Responsible of the organizational structure in charge for providing the CA service.

9 Other Business and Legal Matters

9.1 Fees

The maximum fees of the service are published on the website: http://postecert.poste.it/ and https://www.poste.it/prodotti/firma-digitale-remota.html .
Different conditions can be negotiated on a custom basis, depending on the required volumes.

9.2 Financial Responsibility

Poste Italiane has signed an appropriate insurance to cover the risks of the activity and any damage deriving from the certification service.

9.3 Protection of confidentiality and processing of personal information

Poste Italiane is the owner of personal information collected in the process of identification and registration of Entities who request certificates.

Therefore the information is treated with the maximum confidence and in accordance with the provisions of the requirements identified in ETSI EN 319 411-1 [2], clause 6.8.4.

In case of the identification and registration activity of users is obtained from a delegated structure (RA), the latter is described as a "processor".

9.3.1 Archives containing personal information

The file containing personal data is the registration database.

The archives listed above are managed by the manager of registration and are adequately protected against unauthorized access and in accordance with the requirements of General Data Protection Regulation (GDPR).

9.4 Intellectual Property Rights

This Document is property of Poste Italiane, which reserves to itself all the rights related to it. The certificate owner maintains all the rights over the own trademark (brand name) and on his domain name. In relation to the properties of other data and information it is applied the law in force.

9.5 Obligations and guarantees

9.5.1 Certification Authority

The CA is committed to:

- Operate in accordance with this document;
- Identify Subscribers as described in this document;
- Issue and manage certificates as described in this document;
- Provide an efficient service of suspension or revocation of certificates;
- Ensure that the owner held, at the time of the certificate issuance, the corresponding private key;

- Promptly report the possible compromise of the private key;
- Provide clear and complete information on the procedures and requirement of the service;
- Provide a copy of this document to anyone who requests;
- Ensure that the provision of digital signature and electronic seal services are accessible for persons with disabilities;
- Ensure the treatment of personal data compliant with current legislation;
- Ensure the availability of the service except in the case of programmed maintenance activity, that is previously notified to the subscribers;
- Provide an efficient and reliable information service on the status of certificates.

9.5.2 Registration Authority

The Registration Authority treats personal data of the subject with the maximum confidence and in accordance with the requirements of General Data Protection Regulation (GDPR).

9.5.3 Subscriber or owner

The Subscriber or owner has the obligation to:

- Read, understand and fully accept this document;
- Request the certificate provided by this document;
- Generate in a safe way the public-private key pair, using a trustworthy system;
- Provide to CA accurate and truthful information in the registration phase;
- Adopt technical and organizational measures designed to prevent the impairment of the private key;
- Ensure the privacy of reserved codes received from the CA;
- Demand immediate suspension of the certificate in case of suspected or confirmed impairment of the private key;
- Immediately request the revocation of the certificate in the event that one or more information contained in the certificate lose validity;
- Following the issue and until the expiration or the revocation of the certificate, promptly notify the CA of any changes to the information provided in the application phase;

9.5.4 End User

The end users, so all the entities (different from the Subscriber or the Owner) that rely on certificates issued under this document, have an obligation to:

- perform a reasonable effort to obtain sufficient information on the functioning of certificates and PKI;
- check the status of certificates issued by Poste Italiane on the basis of this CP;
- rely on a certificate only if it has not expired, suspended or revoked.

9.6 Disclaimers of Warranties

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.7 Limitations of Liability

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.8 Indemnities

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.9 Term and Termination

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.10 Communications

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.11 Dispute Resolution Procedures

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.12 Governing Law

The explanations identified in Disclosure Statement Digital Signature document is applied (https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).

9.13 Compliance with Applicable Law

The explanations identified in Disclosure Statement Digital Signature document is applied

(https://postecert.poste.it/TSPdoc/pi-QUCApds.pdf).