In.Te.S.A. S.p.A.
Qualified Trust Service Provider
in accordance with Regulation (EU) no. 910/2014 (eIDAS)

CPS - Certification Practice Statement and CP - Certificate Policy for Qualified Certificates for Electronic Signatures and Electronic Seals

English translation of:
CPS - Certification Practice Statement
e CP - Certificate Policy
per i Certificati Qualificati
di Firma Elettronica e di Sigillo Elettronico
Versione: 03 (21/12/2021)

Document code: INTQS-QCSS_CPS_EN
OID: 1.3.76.21.10.100.5.1
Prepared by: Antonio Raia
Approved by: Simone Baldini
(Time stamp and certification services manager)
Issued on: 21/04/2022
Version: 03-EN

This page is intentionally left blank.

Revisions (referred to the Italian version)

Version no.: 03	***Revision Date: 22/11/2021***
Description of changes:	Change of company data and logo Insertion of par *7.1.4 - Certificates issued with electronic identities* Correction of typosi
Reasons:	Certificate profile updates – specific OID for SPID and CIE Organizational changes: ownership, management and coordination of the company
Version no.: 02	***Revision Date: 23/06/2020***
Description of changes:	7.1.1: new root certificate 6.8.8: description update
Reasons:	CA key renewal clarification on the TSS synchronism control
Notes:	qualified electronic signature services
Version no.: 01	***Revision Date: 23/04/2020***
Description of changes:	none
Reasons:	first version
Notes:	it supplements and replaces the document *CPS for Qualified Certificates for Electronic Signatures, ver.01* (document code INTQS-QC_CPS, OID: 1.3.76.21.10.100.4)

Summary

1 Introduction

1.1 General information

This document is the Practice Statement of the Qualified Trust Service Provider (QTSP) In.Te.S.A. S.p.A. and sets out the rules and operating procedures for issuing qualified certificates for electronic signatures and electronic seals, as defined in Regulation (EU) 910/2014 (eIDAS).

The content of this document applies to the QTSP INTESA, and specifically to its logistics and technical infrastructures and its personnel, to the holders of certificates issued by it, to users of the service and to those who use those certificates to verify the authenticity and integrity of the documents to which an electronic signature, electronic seal and/or electronic time stamp has been applied.

The document is issued in compliance with the *RFC 3647* standard and has been laid out as described therein.

NOTE: This document supplements and replaces the document *CPS for Qualified Certificates for Electronic Signatures, ver.01* (document code *INTQS-QC_CPS*, OID: 1.3.76.21.10.100.4).

1.2 Document identifier

This document is the English translation of version no. **03,** issued on **21/12/2021**, of the QTSP INTESA *CPS - Certification Practice Statement and CP - Certificate Policy for qualified certificates for electronic signatures and electronic seals* (hereinafter, also referred to simply as *CPS*).

The content of this document complies with the technical standards contained in the *Italian Prime Ministerial Decree of 22 February 2013* (hereinafter *DPCM*) and *Italian Legislative Decree no. 82 of 7 March 2005, containing the "Digital Administration Code "*as subsequently amended and supplemented (hereinafter the "*DAC*") and complies with *Regulation (EU) 910/2014* (hereinafter, also simply *eIDAS Regulation*).

Document code	*INTQS-QCSS_CPS*
OID	*1.3.76.21.10.100.5*
Reference policies	ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 411-3
Certificate Policies *eIDAS*	0.4.0.194112.1.2 0.4.0.194112.1.3
Certificate Policies *INTESA - qualified certificates*	1.3.76.21.1.3.1.1 1.3.76.21.1.5.1.1 1.3.76.21.10.2.1.1 1.3.76.21.10.2.1.2
Certificate Policy *agIDCert*	1.3.76.16.6
Certificate Policies *pre-eIDAS*	0.4.0.2042.1.2 0.4.0.1456.1.1
In.Te.S.A. S.p.A. OID	1.3.76.21
qualified services eIDAS	1.3.76.21.10
accredited services AgID	*1.3.76.21.1*
this document - original Italian version	*1.3.76.21.10.100.5*
this document -English translation	*1.3.76.21.10.100.5.1*

1.3 PKI Participants

The company ***In.Te.S.A. S.p.A.*** is the QTSP (*Qualified Trust Service Provider*). Its identification details are provided below.

Company name	**In.Te.S.A. S.p.A.**
Registered office	**Strada Pianezza, 289 - 10151 Turin**
Legal Representative	**Managing Director**
Turin Company Register	**Registration no. 1692/87**
VAT no.	**05262890014**
Telephone no. (main switchboard)	**+39.011.19216.111**
HelpDesk - for calls from within Italy	**800.80.50.93**
HelpDesk - for calls from abroad	**+39 02.39.30.90.66**
Website address	***www.intesa.it***
E-mail address	***marketing@intesa.it***
Certificate Directory URL	***ldap://x500.e-trustcom.intesa.it***
ISO Object Identifier (OID)	**1.3.76.21**

Specific entities within the QTSP INTESA organisation are appointed to participate in the processes covered by this CPS.

These entities operate in compliance with the rules and processes established by the QTSP, completing the parts of the tasks assigned to them.

1.3.1 CA - Certification Authority

The QTSP INTESA, operating in accordance with the provisions of the Technical Standards (DPCM), the Digital Administration Code (DAC) and the eIDAS Regulation, performs the role of Qualified Trust Service Provider, involving the *creation, verification and validation of electronic signatures, electronic seals and electronic time stamps* (see eIDAS, Art. 3, paragraphs 16 and 17).

The following personnel are responsible for certification activities, in accordance with Art. 38 of the DPCM:

- Security manager.
- Time stamp and certification service manager.
- Systems technical manager.
- Logistics and technical services manager.
- Inspection and audit manager.

The above-listed persons are all members of the INTESA organisation.

1.3.2 RA - Registration Authority

INTESA has established an RA Department within its organisation, which performs the role of Registration Authority.

More specifically, it performs the following tasks:

- Holder identification.
- Holder registration.
- Initialisation of signature devices.
- Distribution of signature devices.
- Management of signature device inventory.
- Holder support.

In the context of specific agreements, the RA Department is also tasked with training personnel from third-party entities to establish *Local Registration Authorities (LRA)*. The latter operate at a local level, performing all or part of the tasks listed above at INTESA's request.

The QTSP INTESA may also delegate performance of certain RA tasks to third-party entities (see par. 1.3.3.4). The Mandate Agreement, signed by both parties, shall set out the tasks assigned to the third-party LRAs and state the parties' obligations.

The INTESA RA and the LRAs are subject to auditing and supervision by the QTSP, in order to verify compliance with the regulations in force.

1.3.3 Other entities

1.3.3.1 Qualified certificate holder

Natural or legal person to whom the electronic signature or electronic seal is assigned, and who has access to devices for the creation of the electronic signature or electronic seal.

This is the person in whose name the certificate is issued.

1.3.3.2 Interested Third Party

The Interested Third Party is a natural or legal person (enterprise, trade association, organisation, etc.) that requests or authorises issuance of the qualified certificate. It is obliged to request revocation of certificates in the event that the requirements on the basis of which they were issued are no longer satisfied.

1.3.3.3 Relying Party

The Relying Party is the person who uses the certificates (and any time stamps) issued by QTSP INTESA when verifying the electronic document.

1.3.3.4 LRA –Local Registration Authority

For reasons associated with providing the service, and in accordance with Art. 1717 of the Italian Civil Code, the QTSP INTESA makes use of other entities nationwide (hereinafter referred to as third-party LRAs) to carry out part of its own RA Department activities. More specifically, the third party LRAs perform the following tasks:

- positively identifying the holder of the certificate;
- receiving the registration and certification request completed and signed by the Holder;
- delivering the signature device.

The documentation received must be sent to the INTESA RA Department or, if agreed in advance, be kept and stored by the LRA according to the same methods.

Third-party LRAs are established by the QTSP following appropriate training of the personnel specified by the Company or Organisation, with which a valid Mandate Agreement is entered into and signed by both parties. That agreement clearly sets out the obligations of the Company or Organisation appointed by INTESA as an LRA; in particular, these include:

- overseeing the identification activities performed to ensure they are carried out in compliance with the regulations in force;
- preventing employees from continuing to perform identification activities and ensuring that access to all materials is immediately withdrawn from those employees in the event that their relationship with the Company is terminated for any reason, providing prompt written notice to INTESA;
- safeguarding the signature devices until they are delivered to the intended holders, with direct liability in the event they are taken or lost for any reason, with the obligation to notify the INTESA Registration Department of any such events without delay;
- using and processing personal data obtained during the identification process in accordance with the GDPR.
- notifying QTSP INTESA, by way of its RA Department (*uff_ra@intesa.it*) or the relevant INTESA contact people, without delay, of any event or incident relating to the previous points, and of any security breaches or integrity loss that significantly affect the services or personal data.

1.4 Using the qualified certificates

The qualified certificates issued by QTSP INTESA in accordance with this document are used to validate Qualified Electronic Signatures / Digital Signatures and Qualified Electronic Seals.

Except in cases of *intention or negligence* (eIDAS Reg., Art. 13), the QTSP INTESA accepts no liability for consequences arising from use of the certificates in a manner other than that provided for in this CPS, in the relevant Operating Manual and/or from failure to comply with current regulations.

The certificates may contain potential restrictions on their use, specified in the *certificatePolicies* (*OID:2.5.29.32*) certificate extension. That extension specifies whether the certificate is used as part of an automatic signature or seal procedure.

Qualified certificates issued in accordance with the guidelines contain a code, in the *certificatePolicies* (OID 2.5.29.32) field, for a PolicyIdentifier element with an *agIDcert* value (OID 1.3.76.16.6).

Qualified certificates issued by the INTESA CA in accordance with the guidelines only and exclusively contain the *Key Usage* corresponding to "*Type A* "of ETSI 319 412-2i: *keyUsage (OID 2.5.29.15) = nonRepudiation*.

The certificate profiles are described in par. *7* - Certificate profiles and CRL - Certificate Policy.

1.5 Management of the specifications contained in the CPS

The CPS document is managed directly and in full by the QTSP INTESA organisation, with the relevant references provided in par. *1.3*.

The CPS document is drafted in collaboration with the managers involved in the PKI activities (par. *1.3.1*) and ultimately approved by the *Security Manager* (par. *1.3.1*).

The document is then sent to the Supervisory Body for approval: the procedures described in this CPS may only be adopted following formal authorisation by the Agency. This is followed by publication of the document on the QTSP INTESA website and the Agency website.

1.5.1 Revision procedure

Without prejudice to the QTSP's internal approval process, the Agency will be notified of each new version of this CPS.

In fact, an amended version of the document cannot be adopted without the permission of the Supervisory Body.

Once the Agency's approval has been received, the document will be published by the QTSP at the URL specified in par. *1.3*.

The foregoing also applies to any editorial or typographical changes.

1.6 Definitions and References

1.6.1 Definitions and Acronyms

A number of acronyms and specific terms used in this document are set out here below. A full list is included in the eIDAS Regulation (*Art. 3 Definitions*) and in the DAC (*Art. 1 Definitions*, as amended by *Art. 1* of Italian Legislative Decree 179/2016).

AgID	*Agenzia per l'Italia Digitale* (Digital Italy Agency, formerly CNIPA and DigitPA) - *www.agid.gov.it*. Supervisory Body in accordance with Reg. EU 910/2014 (eIDAS). Hereinafter also simply the *Agency*.
QTSP - Qualified Trust Service Provider (previously Accredited Certification Authority)	*Qualified Trust Service Provider*. Natural or *legal* person who provides one or more qualified trust services. Formerly *Accredited Certification Authority*, in accordance with the DAC. In this document, it refers to QTSP In.Te.S.A. S.p.A. In this document, the terms *QTSP*, *Accredited Certification Authority* and *Certification Authority* are used interchangeably.
CAB - Conformity Assessment Body	The body 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.
EUTSL	*EU Trusted List* - A list that includes information on the qualified trust service providers, together with information on the qualified trust services they provide. This list is maintained and published by the individual member state (in Italy, by AgID).
CP	*Certificate Policy* - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

CPS	*Certification Practice Statement* - A statement of the practices which a Certification Authority/QTSP employs in issuing and managing certificates.
OM	*Operating Manual* - A document drafted in accordance with Art. 40 of *Italian Prime Ministerial Decree of 22 February 2013* and subject to approval by the Supervisory Body (AgID).
CRL	*Certificate Revocation List* - A list signed by the RA, indicating a set of certificates that are no longer considered valid by the Certification Authority/QTSP that issued them.
OCSP	*Online Certificate Status Protocol* - Service enabling verification of the validity status of the certificate, according to the OCSP protocol.
HSM	*Hardware Security Module* - Devices for creating qualified electronic signatures, if they comply with the requirements referred to in Annex II of Reg. (EU) 910/2014 (eIDAS) and, *mutatis mutandi*, for generating qualified electronic seals. Also referred to as *Remote Signature Devices*.
OID:	*Object Identifier* - Sequence of numbers that identifies a particular object within a hierarchy, registered according to the procedure defined by the ISO / IEC 6523 standard.
PKI	*Public Key Infrastructure* - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke certificates based on public-key cryptography. By extension, it includes the qualified electronic time stamp systems.
CA	*Certification Authority* - PKI entity that issues the signature and/or seal certificates.
RA *Registration Authority*	Registration Authority appointed by the QTSP to register and verify the identities of qualified certificate holders, as required by the QTSP. In any case, the QTSP (INTESA S.p.A.) is responsible for the registration, identification and validation operations.
TSA	*Time-Stamping Authority* - The PKI entity that issues certificates in relation to the time-stamping keys.
TSU	*Time-Stamping Unit*- Set of HW and SW that issues electronic time stamps. Each TSU has its own time-stamping Certificate used for the time stamps issued. In this document, these certificates are also called *TSU Certificates*.
QES - Qualified Electronic Signature *DS - Digital Signature*	Data in electronic form attached to or logically associated with other electronic data and used by the signatory *to sign*. The QES is created by a device used to create qualified electronic signatures and is based on a qualified certificate for electronic signatures. In Italy, the QES corresponds to the *Firma Digitale* [Digital Signature] defined in Art.1, par. 1, point s) of the DAC as: A qualified electronic signature based on a system of cryptographic keys –a public key and a private key, linked to each other –that enables the Holder, using the private key, and the recipient, using the public key, to prove and verify the origin and integrity of an electronic document or set of electronic documents.
QES - Qualified Electronic Seal	Data in electronic form attached to or logically associated with other data in electronic form used *to guarantee the origin and integrity* of the latter. The Qualified Electronic Seal meets the requirements set out in Art. 36 of the eIDAS Reg. and is created by a qualified electronic seal creation device and based on a qualified certificate for electronic seals.
Electronic time stamp	Electronic information containing the date and time that are associated with an electronic document, for the purpose of proving that the document existed at that date and time.
Qualified Certificate for Electronic Signature	Electronic attestation which links electronic signature validation data to a *natural person*. It is issued by a qualified trust service provider and meets the requirements set out in *Annex I* of Reg. EU 910/2014 (eIDAS).
Qualified Certificate for electronic seal	Electronic attestation which links electronic seal validation data to a *legal person*. It is issued by a qualified trust service provider and meets the requirements set out in *Annex III* of Reg. EU 910/2014 (eIDAS).
CRL	*Certificate Revocation List* - A list signed by the RA, indicating a set of certificates that are no longer considered valid by the Certification Authority/QTSP that issued them.
OCSP	*Online Certificate Status Protocol* - Service enabling verification of the validity status of the certificate, according to the OCSP protocol.
HSM	*Hardware Security Module* - Devices for creating qualified electronic signatures, if they

	comply with the requirements referred to in Annex II of Reg. (UE) 910/2014 (eIDAS) and, *mutatis mutandis*, for creating qualified electronic seals. Also referred to as *Remote Signature Devices*.
Holder (of a Qualified Certificate)	Natural or legal person to whom the electronic signature or electronic seal is assigned, and who has access to devices for the creation of the electronic signature. The person in whose name the certificate is issued.
Subscriber or Applicant	For the purposes of this document, this is the (natural or legal) person who contacts the QTSP requesting access to the service.
User	The user of the trust service.
Relying Party	The person who uses the certificate, seal and/or time stamp when verifying the electronic document.
Interested Third Party	Natural or legal person (enterprise, trade association, organisation, etc.) that requests or authorises issuance of the qualified certificate.
Client	Natural or legal person who signs a contract with the QTSP INTESA.
Audit journal	Set of registrations performed, including automatically, by the devices installed at the Certification Authority, stored for the purposes of guaranteeing the authenticity of the entries and making it possible to accurately reconstruct all events that are significant for security purposes (DPCM 22/02/2013, Art. 36).

1.6.2 Regulatory and technical references

Regulation (EU) no. 910/2014 (eIDAS) as subsequently amended and supplemented	Regulation (EU) no. 910/2014 of the European Parliament and Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. In this document, also referred to simply as *eIDAS Reg.* (electronic Identification Authentication and Signature).
DAC - Italian Legislative Decree 82/05 as subsequently amended and supplemented	Italian Legislative Decree no. 82 of 7 March 2005 - "*Digital Administration Code*". Hereinafter also referred to simply as *DAC*.
Italian Prime Ministerial Decree 22/02/2013 New Technical Standards as subsequently amended and supplemented	Italian Prime Ministerial Decree of 22 February 2013 - "*Technical standards for the generation, application and verification of advanced, qualified and digital electronic signatures in accordance with Articles 20, par. 3, 24 par. 4, 28 par. 3, 32 par. 3 point b), 35 par. 2, 36 par. 2, and 71 "(of the DAC, ed.).* Hereinafter also referred to simply as *DPCM [Decreto del Presidente Del Consiglio Dei Ministri]*.
Regulation (EU) no. 2016/679 GDPR - General Data Protection Regulation as subsequently amended and supplemented	Italian Legislative Decree no. 196 of 30 June 2003 - "*Data protection code"* REGULATION (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation). Hereinafter also referred to simply as *GDPR.*
RESOLUTION No. 147/2019 (Guidelines) as subsequently amended and supplemented	Guidelines containing "Technical Standards and Recommendations regarding generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time stamps". In this document, also referred to simply as the *RESOLUTION* or *GUIDELINES.*
DECISION 45, 21/05/2009	CNIPA Decision of 21 May 2009, no. 45 – "*Rules for the identification and verification of electronic documents*"; repealed by Resolution 147/2019. Hereinafter also referred to simply as the *DECISION.*

AgID Communication 0016101 of 07-06-2016	AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016, concerning "*Request for clarification regarding the use of digital signatures in specific closed user contexts*".
ETSI-319.401	ETSI EN 319 401 v2.1.1 - *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.*
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;* *Part 1: General requirements.*
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - *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.*
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 1: Overview and common data structures.*
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 2: Certificate profile for certificates issued to natural persons.*
ETSI-319.412-3	ETSI EN 319 412-2 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 3: Certificate profile for certificates issued to legal persons.*
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 5: QCStatements.*
ETSI-319.421	ETSI EN 319 421 v1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.*
ETSI-319.422	ETSI EN 319 422 v1.1.1 - *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.*
Rec ITU-R	Recommendation ITU-R TF.460-6, *Annex 1 - Time Scales*.
RFC5280	*Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.*
RFC5905	*Network Time Protocol (NTP Protocol).*
RFC3647	*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework.*
ENISA - Art. 19 Incident Reporting (Guidelines)	"*Article 19 Incident Reporting- Incident reporting framework for eIDAS Article 19 - December 2016.* In this document, also referred to simply as *ENISA Guidelines (Art. 19)*.

2 Repository and publication

This CPS and the documentation concerning the qualified services provided by the QTSP INTESA are published at the following address:

- *https://www.intesa.it/e-trustcom/*

The documents are only available to users in read-only format.

The QTSP is responsible for managing publications on its website.

The documents subject to approval by the Supervisory Body are also published and available on the Agency website (*www.agid.gov.it*).

Additional operating information is available in the *Operating Manuals*: the QTSP INTESA is required by Italian law to publish an Operating Manual setting out the procedures and relevant rules applied by the QTSP to issuing qualified certificates, creating and verifying qualified electronic signatures, qualified electronic seals and electronic time stamps.

Like the CPS, the Operating Manuals are also subject to approval and publication by the Agency, which formally authorises the QTSP to act in accordance with the content of those documents.

2.1 Publication of the certificates

The QTSP uses an "LDAP" certificate directory, where it publishes:

- The CA key certificates.
- The time stamp system signing key certificates.
- The Agency signing key certificates.
- The revocation and suspension lists.
- The holders' signature/seal certificates (with their consent)

The QTSP keeps a master copy of the certificate directory that is inaccessible from the outside. This updates the operational copy in real time and is accessible to users via the LDAP protocol at the following address:

- *ldap://x500.e-trustcom.intesa.it*

NB: the certificate is published on the LDAP service at the explicit request of the Holder. Consent to publication does not necessarily result in publication.

The qualified certificate also specifies the location where the CA certificate that signed the relevant certificate is freely available:

- CA Issuers - *URI: https://e-trustcom.intesa.it/CERTS/<<certname>>*.

3 Identification e Authentication (I&A)

The QTSP INTESA issues qualified certificates in accordance with the eIDAS Regulation and the recommendations set out in the AgID Guidelines.

Specifically, the ETSI standards relevant to qualified certificate profiles are:

ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*
ETSI-319.412-3	ETSI EN 319 412-2 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

The *Holder* of a qualified certificate may be a natural person (ref. *ETSI-319.412-2*), in which case we refer to an *electronic signature*, or a legal person (ref. *ETSI-319.412-3*), in which case we refer to an *electronic seal*.

3.1 User identification and registration: Distinguished Name (DN)

The *SubjectDN* field of the certificate contains a minimum set of information that clearly identifies the Holder (natural or legal person), in accordance with the Guidelines and the relevant ETSI.

Other optional attributes can also be included, in order to further restrict use.

3.1.1 SubjectDN Natural Person

Certificates issued to a natural person include at least the following attributes:

ATTRIBUTE	OID:
countryName	2.5.4.6
givenName	2.5.4.42
surname	2.5.4.4
commonName	2.5.4.3
serialNumber	2.5.4.5
dnQualifier	2.5.4.46

The most common optional or alternative attributes, subject to restrictions:

ATTRIBUTE	OID:
organizationName	2.5.4.10
organizationIdentifier	*2.5.4.97*
organizationalUnitName	2.5.4.11
description	2.5.4.13
title	2.5.4.12
pseudonym	2.5.4.65

3.1.2 SubjectDN Legal Person

Certificates issued to a legal person include at least the following attributes:

ATTRIBUTE	OID:
countryName	2.5.4.6
organizationName	2.5.4.10
organizationIdentifier	*2.5.4.97*
commonName	2.5.4.3
dnQualifier	2.5.4.46

3.1.3 Setting attributes

Setting certificate attributes occurs according to the rules described in the relevant ETSI and the recommendations set out in the Guidelines.

A number of specific examples are set out here below.

3.1.3.1 Unique identifier of the Holder

The certificate holder is assigned a code, which is unique in the context of the QTSP, associated with the *dnQualifier* attribute.

The unique nature of the Subject field and the clear attributability of the certificate to the Holder is guaranteed by the following attributes:

- *serialNumber* for natural persons
- organizationIdentifier for legal persons

These attributes contain:

- *serialNumber*: this contains the tax identification number (TIN) of the Holder, identified by the prefix "`TINIT-`" Only if the Holder has not been assigned a tax identification number by the Italian authorities can an equivalent tax identification number issued by another EU authority be used, preceded by the prefix TIN. Alternatively, in such circumstances, ID document information can be provided using the prefixes IDC or PAS, or a national identification number, using the prefix PNO. Such prefixes will be followed by the ISO 3166 code of the country that issued the document. If the laws of the State where the natural person resides do not allow the aforementioned codes to be used, the prefix NS is used to identify the national scheme. In that case, the trust service provider must enter a unique code, potentially derived from one of those listed above.
- *organizationIdentifier*: contains the VAT number of the legal person who holds the certificate. The prefix will be followed by the ISO 3166 code of the country that issued the code.

3.1.3.2 countryName

The *countryName* attribute is filled out as follows:

- *natural persons*: if the *organizationName* attribute is included, this is the ISO 3166 code of the state where the specified organisation is located; otherwise it refers to the state of residence of the Holder
- *legal persons*: this is the ISO 3166 code of the state where the Holder is located

3.1.3.3 organizationName

Optional attribute. It may be used to indicate that the Holder belongs to or is affiliated with the organisation, provided that the trust service provider has been given – and has a record of – proof that the organisation consents to such use, and takes responsibility for requesting revocation of the certificate in the event that the holder of the certificate leaves the organisation.

NB: organizationName is not used if the Holder is simply a client of the organisation (ref. *Guidelines*).

3.1.3.4 title

If the *organizationName* is included, the same restrictions also apply to the potential use of the *title* attribute. If included, the *title* attribute states the role of the Holder in the organisation indicated in the *organizationName* attribute, according to the semantics specified in the *Guidelines*.

3.1.3.5 pseudonym

Under certain circumstances, the Holder may request that a pseudonym appear on the certificate instead of his/her real information. As these procedures relate to qualified certificates, the QTSP will, in any case, keep details of the user's true identity on file for 20 (twenty) years from expiry of the certificate.

The *pseudonym* attribute (OID 2.5.4.65) must be used as an alternative to *givenName + surname.*

Using a pseudonym, the subject DN field will be filled out as follows:

- countryName "c=IT"
- *pseudonym* unique pseudonym used in the context of the QTSP
- commonName "pseudonym"
- serialNumber as specified in the Guidelines
- *dnQualifier* unique identifier used in the context of the QTSP

3.2 Initial positive identification of the certificate applicant

The QTSP positively verifies the identity of each applicant when they first apply for a qualified certificate.

The task of identifying the applicant is performed by:

- The QTSP, via members of its RA Department or its own personnel who have been adequately trained;
- Third-party LRAs: for example, personnel of the Company or the Client Organisation, or third parties specifically appointed by the QTSP and adequately trained.

The person applying for certification is positively identified by the RA operator and a copy of at least one official ID document issued by their State of origin is held on file by the QTSP, INTESA (or the appointed LRA).

If the holder of the certificate is a legal person, the certification application must be submitted by the natural person who represents the legal person, providing appropriate additional documentation to prove that they have the necessary representative powers (e.g. chamber of commerce extract). Generally, the applicant is the Legal Representative or a person formally appointed by the latter.

Positive identification of the Holder may be carried out by way of the following methods:

- *De visu, in person*: identification involves the applicant meeting the RA operator in person
- *De visu, remotely*: identification is carried out using video-conferencing technology that meets quality standards certified by a CAB (conformity assessment body)
- *Based on previous identification*: relying on positive identification carried out previously by a *Financial intermediary* or another *Party Performing Financial Activities* obliged, under anti-money laundering regulations in force at the time, to identify its clients
- *Other methods*, provided that they comply with Art. 24, par. 1 of the eIDAS Regulation.

Further details of Holder identification procedures currently being performed are available in the QTSP Operating Manual, published at the following link:

- *https://www.intesa.it/e-trustcom/*

3.3 Identification for the purposes of reissuing a certificate

Without prejudice to the right to perform a full and detailed verification following a reissue request, *de visu* verification of the Holder is not required if the person in question has already been identified by the QTSP or another appointed body.

3.4 Identification for the purposes of revocation or suspension requests

A request to revoke or suspend a qualified certificate (par. 4.9) can be made by:

- the QTSP INTESA
- the Holder
- the Interested Third Party

A request submitted by the Holder or the Interested Third Party to the QTSP to revoke/suspend certificates must be signed by the applicant and accompanied by a copy of an identity document.

Once the adequacy of the data contained in the request has been verified, the certificate is revoked/suspended by the QTSP Certification Authority.

4 Certificate lifecycle

Qualified certificates issued by the INTESA CA are valid for 24 (twenty-four) months from the date of issue, unless otherwise agreed upon with individual clients.

By the certificate expiry date, the signature device holder will be sent notice of the upcoming expiry, by e-mail where possible, or else by standard post.

If the Holder wishes to renew their certificate, they must promptly notify the RA Department of the Certification Authority or the appointed LRA, to guarantee continuity of the service.

4.1 Certification application

Following successful completion of the identification and registration phase, the signing/seal keys generated by the Certification Authority can be created.

In specific cases, they may be issued prior to completion of the identification phase (par. 7.1.3).

The signing/seal keys are generated using signature devices that meet the requirements set out in *Annex II* of the *eIDAS Reg.* (QSCD –Qualified Signature Creation Device).

4.1.1 Generic applicant - natural person

The applicant, i.e. the *natural person* who will be the *Holder* of the certificate, signs:

- The service contract, setting out the obligations of both parties.
- The *N.P. Qualified Certificate Application Form*, containing the data required to issue the certificate, including:
  - Surname and name.
  - Date and place of birth.
  - Tax identification number (or similar in the case of foreign nationals who do not have an Italian TIN).
  - Mobile phone number.
  - E-mail address.
  - Type, number, issuing body and expiry date of the ID document presented.
- The *Confirmation of having read the INTESA Operating Manual* document, declaring that he/she has read the Operating Manual.
- The *Consent to processing of personal data* document, providing consent to use of his/her personal data in accordance with the GDPR.

The applicant is responsible for providing a valid e-mail address, so that the QTSP (who does not verify the validity of the address) can use that address to communicate with the applicant in the future.

The documentation described above, in relation to holder registration, is stored by the QTSP (or the appointed LRA, if provided for in the mandate agreement) for 20 (twenty) years from expiry of the certificate.

4.1.2 Generic applicant - legal person

The applicant, i.e. the natural person representing the *legal person* who will be the *Holder* of the certificate (par. 3.2), signs:

- The service contract, setting out the obligations of both parties.
- The *L.P. Qualified Certificate Application Form*, containing the data required to issue the certificate, including:
  - Surname and name.
  - Date and place of birth.
  - Tax identification number (or similar in the case of foreign nationals who do not have an Italian TIN).
  - Mobile phone number.
  - E-mail address.
  - Type, number, issuing body and expiry date of the ID document presented.
  - Name of the legal person
  - Registered offices of the legal person
  - VAT or Tax Identification Number (VAT or similar for organisations registered abroad)
- The *Confirmation of having read the INTESA Operating Manual* document, declaring that he/she has read the Operating Manual.
- The *Consent to processing of personal data* document, providing consent to use of his/her personal data in accordance with the GDPR.

The applicant is responsible for providing a valid e-mail address, so that the QTSP (who does not verify the validity of the address) can use that address to communicate with the applicant in the future.

The documentation described above, in relation to holder registration, is stored by the QTSP (or the appointed LRA, if provided for in the mandate agreement) for 20 (twenty) years from expiry of the certificate.

4.1.3 Service contract between INTESA and the Client Organisation/Company

If the client is an Organisation or Company, whose identification details will be set out in a contract, the following rules will apply, without prejudice to the specifications contained in par. *3* concerning the identification and registration of individual holders:

- The persons appointed to identify the members of the Client's personnel that are eligible for INTESA certification shall provide the Certification Authority with lists of the individuals to whom INTESA is authorised to issue qualified certificates. Those lists may also indicate any restrictions on the use of the key pairs, representative powers or professional titles.
- These lists shall be made available to the relevant operators: the RA Department or LRA personnel.
- The authorised persons shall present documentation similar to that specified in the previous paragraph to the LRAs.

The LRA will verify that the person has been authorised for certification, and will proceed as set out in the previous paragraph, with the exception of the first point of that paragraph.

4.1.4 Restrictions on use

In the event of requests to include restrictions on use in the qualified certificate, or limits on value in relation to the stores where the certificate can be used, the applicant must sign appropriate documentation confirming that request. A copy of that documentation is kept on file by the QTSP.

4.1.5 Professional titles or representative powers

In the event of a request to include representative powers on the qualified certificate for electronic signatures (e.g. that the holder belongs to an organisation and their role there, authorisation to act in the name and on behalf of a Client etc.), or to specify professional titles (e.g. membership of a professional association), the applicant must produce suitable documentation to prove that he/she legitimately holds such professional titles. A copy of that documentation is kept on file by the QTSP.

Documentation provided to support requests to include professional titles or qualifications on a qualified certificate must not be dated more than 10 (ten) days prior to submission of the request to issue the certificate.

Inclusion on the qualified certificate of information concerning public offices held, or representative powers in relation to public-law bodies or organisations, will be subject to specific agreements with those bodies. Based on such agreements, the Holder's role within the public body or organisation may be specified.

The documentation produced will be stored by the QTSP or the appointed LRA for 20 (twenty) years.

4.2 Application acceptance process

The application assessment process is performed by the QTSP via its RA, or by the LRA to which the Registration Authority tasks have been delegated.

With regard to that process, the CA, RA/LRA and applicant/holder are bound by the obligations referred to in par. *9.6 - Obligations*.

4.3 Certificate issuance

Following successful completion of the identification and registration phase, the signing/seal keys generated by the Certification Authority can be created.

The signing/seal keys are generated using signature devices that meet the requirements set out in *Annex II* of the *eIDAS Reg.* (QSCD –Qualified Signature Creation Device).

Following creation of the signing/seal key pair, a related certification request can be generated in PKCS#10 format; this provides proof of possession of the private key and verification of the proper functioning of the key pair.

The CA will immediately process the request received, verifying the authenticity of the request and that the Holder is actually in possession of the private key (and as such verifying proper functioning of the key pair).

The QTSP issues the certificate using a system that complies with Art. 33 of the DPCM 22/02/2013 and the eIDAS Reg.

With the consent of the Holder, the certificate generated as referred to above is published in the certificate directory.

Certificate generation is recorded in the audit journal.

4.3.1 Generation of keys and the relevant certificate on a signature device

In general terms, issuing a certificate using a signature device involves the following operations:

- The RA operator logs on to the application, selects the Applicant's registration data and launches the certificate request procedure.
- The application accesses the signature device using the default PIN and generates the key pair.
- Following generation of the keys, the application launched by the RA operator generates the certificate request.
- The request is forwarded directly to the CA; it is electronically signed by the operator and sent via a secure channel.
- The certificate issued is received by the application and included on the signature device following the necessary verifications.
- In the case of an Individual Signature Device, the application locks the signature device access PIN. The Holder will receive a separate envelope containing the PUK for the device, to activate the same.
- In the case of remote signatures, the log-in details will be sent to the Holder.

4.4 Accepting the certificate

Holders must verify that the information contained in the certificate provided to them is correct, and immediately report any errors to the Certification Authority. In the latter case, the Holder must sign a request to revoke the certificate that contains erroneous data (par. *4.9.2*).

The QTSP will inform the client in advance of the terms and conditions for using the qualified certificate for electronic signatures.

The applicant signs the document to confirm that they have read the applicable *Operating Manual*, which sets out the obligations of the Holder and other entities involved in the relevant services (par. *9.6 - Obligations*).

The Operating Manual is available on the QTSP website at the following URL: *https://www.intesa.it/e-trustcom/*

4.5 Using the certificate and the keys

4.5.1 Using the private key and the certificate - obligations of the Holder

The Holder is obliged to store the information required to use the private signing key in an appropriate manner and to take all appropriate organisational and technical measures to prevent damage to others.

In particular, the utmost care and diligence must be taken in storing the information that enables the private key to be used, whether it is on an individual signature device (smartcard, token) or a remote signature device (HSM). The same diligence must be taken with strong authentication devices (e.g. OTP keys, smartphones or mobile phones).

The private key associated with the certificate cannot be used by third parties.

Among its other obligations, the Holder of the key must (par. *9.6.2*):

- provide all information requested by the QTSP, guaranteeing its accuracy under his/her own responsibility;
- notify the QTSP, including via the LRAs, of any changes to the information provided at the time of registering: personal details, address, phone numbers, e-mail addresses, etc.;
- store the information that enables the private key to be used with the utmost care and diligence;
- immediately revoke the digital certificate in the event of loss or theft of the codes used to access his/her signing keys;
- send any requests for revocation or suspension of the qualified certificate in accordance with the instructions provided in this CPS or the relevant Operating Manual.

4.5.2 Using the public key and the certificate - obligations of the Relying Party

The Relying Party is any person who receives a digitally signed document and, for the purposes of verifying its validity, avails of the qualified certificate used by the Holder to sign that document.

Verification of the digital signature and subsequent extraction of the objects signed may be performed using any software capable of processing signed files in accordance with the eIDAS Regulation.

Persons who avail of a qualified certificate to verify the validity of a digitally signed document are required to:

- verify the validity of the certificate containing the public key of the Holder who signed the message, in accordance with the standards in force at the time of its issue;
- verify the certificate validity status using the OCSP protocol or by accessing the Revocation Lists;
- verify the validity of the certification path, based on the public list of QTSPs;
- verify whether or not there are any restrictions on the use of the certificate used by the Holder, in accordance with the Operating Manual of the QTSP that issued the certificate of the holder who signed the electronic document.

The obligations set out above are automatically performed by Verification Software that complies with the regulations in forces (Art. 14 of DPCM).

4.6 Certificate renewal

Qualified certificate renewal – understood to refer to extending the validity period – is not provided for. In the period leading up to its expiry and at the request of the Holder, a new key pair will be generated and a new certificate will be issued.

4.7 Renewal of the keys

The Holder's signing/seal keys will remain valid for at least as long as the relevant certificate is valid.

Digital certificates issued by the INTESA CA are valid as standard for 24 (twenty-four) months from the date of issue, unless otherwise agreed upon with individual clients.

By the certificate expiry date, the signature device holder will be sent notice of the upcoming expiry, by e-mail where possible, or else by standard post.

If the Holder wishes to renew their certificate, they must promptly notify the RA Department of the Certification Authority, to guarantee continuity of the service.

The procedure to obtain a new certificate differs from that involved in issuing a certificate for the first time insofar as the Holder identification and data registration tasks are not repeated.

As such, new certificates can be issued according to the methods described in par. *4.3*.

4.8 Amending the certificate

The information included on the certificate cannot be amended. Any corrections or changes can only be made by issuing a new certificate.

4.9 Revocation or suspension of the certificate

If the revocation or suspension takes place at the request of the QTSP INTESA or the Interested Third Party (Articles 23, 25, 27 and 29 of the DPCM), the QTSP INTESA will notify the Holder of the request and of when the requested event will come into effect.

At the request stage, the date and time when the certificate will be revoked will be specified (Art. 24, par. 1, DPCM).

Revocation/suspension will come into effect within a maximum of 24h from receipt of the request.

A certificate will be revoked in the following cases, each of which corresponds to a *CRLReason* code:

- *CRLReason* ***Superceded***: replacement of the certificate without the private key being compromised;
- *CRLReason* ***Key Compromise***: private key compromised (loss of security and uniqueness);
- *CRLReason* ***Affiliation Changed***: the certificate data are obsolete or wrong;
- *CRLReason* ***Cessation of Operation***: planned or unexpected cessation of performance by the Holder of the tasks for which the certificates were issued, in the context of a dispute or otherwise ();
- *CRLReason* ***Privilege Withdrawn***: failure by the Holder to comply with the obligations set out in the CPS or the Operating Manual, to the extent that the Interested Third Party or the CA deems immediate revocation necessary.

At the request stage, the date and time at which the certificate must be revoked or suspended must be specified, as well as the suspension period, in the latter case.

4.9.1 Revocation at the Certification Authority's request

The QTSP INTESA may revoke the holder's certificates in the cases specified in the previous paragraph.

In any case, it will notify the affected holders of the revocation performed by e-mail, or by standard post.

4.9.2 Revocation at the Holder's request

The Holder may request revocation of his/her certificate by way of three different methods:

- If the Holder has a signature device, he/she should send an e-mail to *uff_ra@intesa.it* containing the revocation request document, filled out and signed using his/her private key, as an attachment: the *Digital Certificate Revocation Request* form is available at *https://www.intesa.it/e-trustcom/*. As well as the revocation request document, the message must contain details of the certificate to be revoked (or information that enables the certificate to be revoked to be uniquely identified - see below) and the reason for the request.
- Alternatively, if the Holder does not have his/her own signature device, he/she can send a request with the details referred to in the previous point and including a copy of his/her ID document:
    a. by fax, to the number provided at the following URL, during the service hours specified there: *https://www.hda.intesa.it*
    b. by standard post, to the address of the QTSP (par. *1.3*).

- Under exceptional circumstances, if the revocation request is submitted on the grounds of *Key Compromise*, the Holder can call the number provided by the QTSP at the time of issuance of the original qualified certificate to him/her. He/she must provide the details of the certificate and the *Emergency Code* (DPCM, Art. 21). In this case, the certificate specified will be temporarily suspended pending a written request from the Holder.

A request submitted using any of the methods described above will serve as justification documentation as provided for under Art. 24, par. 1, of the DPCM.

Outside of the support hours specified at *https://www.hda.intesa.it*, the applicant will only be able to make contact using the freephone number.

With regard to the affected Holder, the request must clearly specify:

- his/her general details (e.g. surname, name, e-mail address, phone number, relevant organisation)
- the reason for the request
- when the measure should come into effect.

Other additional information may be useful for the purposes of uniquely identifying the certificate to be revoked. This information may be obtained by the Holder from the documentation provided at the time of issue, if still available (e.g. type of device and serial number, relevant organisation, certificate serial number, date of issue etc.).

Having determined that the request is valid, the QTSP will notify the Holder of the revocation by e-mail, or in certain cases by standard post, and will include the certificate on the revocation list (CRL).

4.9.3 Revocation at the Interested Third Party's request

The Interested Third Party may request revocation of the Holder's certificate.

QTSP INTESA offers three different methods for the Interest Third Party to submit a revocation request:

- If the Interested Third Party has a signature device, he/she should send an e-mail to *uff_ra@intesa.it* containing the revocation request document, filled out and signed using his/her private key, as an attachment (the *Digital Certificate Revocation Request* form is available at *https://www.intesa.it/e-trustcom/*.) As well as the revocation request document, the message must contain the details of the certificate to be revoked (or information that enables the certificate to be revoked to be uniquely identified) and the reason for the request.
- Alternatively, if the Interested Third Party does not have his/her own signature device, he/she can send a request with the details referred to in the previous point:
    a. by fax, to the number provided at the following URL, during the service hours specified there: *https//www.hda.intesa.it/*;
    b. by standard post, to the address of the QTSP (par. *1.3*).

A request submitted using any of the methods described above will serve as justification documentation as provided for under Art. 25, par. 1, of the DPCM.

Outside of the support hours specified at *https//www.hda.intesa.it*, the applicant will only be able to make contact using the freephone number.

The request must clearly specify:

- with regard to the Interested Third Party:
    - the Company to which they belong
    - their general details
    - reference to the document that authorises them to request the issuance, revocation or suspension of the certificate of the affected Holder
    - contact details: telephone number and e-mail address
- with regard to the affected Holder:
    - their general details
    - details of the certificate for which revocation or suspension is requested
    - type (revocation or suspension) and reason for the request (CRLReason).
    - when the measure should come into effect.

Having determined that the request is valid, the QTSP will notify the affected holders of the revocation by e-mail, or in certain cases by standard post, and will include the certificate on the revocation list, which will be issued immediately.

4.9.4 Suspension of certificates

Certificates will be suspended in the event that further investigation is required to determine whether or not a certificate should be revoked (e.g. in the event of suspected private key compromise or the loss/theft of the signature device, or while awaiting further information to positively determine that the Holder has ceased to perform the activities for which the certificate was issued, etc.).

In the case of suspension, the CRLReason code is *certificateHold*.

A suspension request can be submitted by any of the entities provided for in Articles 27, 28 and 29 of the DPCM (Certification Authority, Holder, Interested Third Party).

As regards methods of suspension and providing notice of the same, the information set out in relation to the revocation request applies.

4.9.4.1 Duration of suspension period

The applicant is responsible for contacting the INTESA RA Department to request reactivation or revocation of a previously suspended certificate. This should be done using the same methods used to request suspension.

If no such contact is made, the certificate will be automatically revoked at the end of the suspension period – a maximum of 90 (ninety) days – specified by the Holder in the request, with the *CRLReason* specified at the time of submitting the request.

In the event of revocation of a suspended certificate, the revocation date will coincide with the suspension date.

4.10 Certificate status information

In accordance with the eIDAS Regulation, information on the certificate status is available via the OCSP protocol at the URL specified on the certificate.

Revocation and suspension of certificates can be formalised by their inclusion on the CRL list (Art. 22 of the DPCM). The CRL profile complies with the RFC 3280 standard. This list, signed by the Certification Authority issuing the certificate, is updated at pre-established intervals in accordance with current regulations.

The web address of the CRL list is specified on the certificate in the *CDP - CRL Distribution Point* field.

The CRL list is also available in the certificate directory.

All of the publication services described above are available 24 hours a day.

4.11 Contract duration

Unless otherwise agreed upon with the client, the contract between the Holder and the QTSP will cease to have effect upon expiry of the certificate.

4.12 Key Escrow & Key Recovery

Not applicable to private keys associated with qualified certificates issued by the QTSP INTESA.

5 Physical security and procedural controls

This section describes the non-technical security controls (i.e. physical, procedural and personnel controls) put in place by the QTSP to securely perform the tasks of generating the keys, managing the lifecycle of the qualified certificate (identification, issuance, revocation, etc.) and perform auditing and archiving tasks.

The QTSP, in accordance with Art. 35 of the DPCM, prepares and updates a *Security Plan*, an encrypted copy of which is sent to the Agency. The document is classified as *INTESA Confidential.*

5.1 Physical security

The INTESA PKI system and its HW and SW components are managed at secure sites (so-called *Data Centres* or *Server Farms*), protected against unauthorised access by access-control and surveillance systems, which provide records for verification audit purposes.

Only authorised personnel have access to the specific areas, under strict policies and procedures that are subject to periodic audits.

5.1.1 Physical location and structure of the building

Each building of significance to the PKI structure is equipped with security measures that comply with the legal regulations in force.

Each building is subject to surveillance and monitoring by electronic systems and trained personnel.

Electrical and security systems are certified in accordance with the law.

The INTESA PKI systems are hosted in buildings located in non-seismic zones, equipped with appropriate water disposal systems and not in the vicinity of waterways.

There are no plants in the vicinity that present the risk of harmful emissions.

5.1.2 Physical access

The INTESA PKI systems (CA, RA, Directory, Time Stamp Server) are hosted in closed, electronically-controlled areas. Anti-intrusion systems are in place.

Access to the PKI areas is restricted to authorised personnel and limited to specific routes within the sites. If required, an escorting service may be provided by the server farm personnel. Specific regulations govern the number and type of professionals required for each significant operation involving systems hosted at the facilities.

Occasional visitors are only granted access if accompanied by authorised personnel (the number of which will depend on the specific area). Access is only granted to unauthorised persons (e.g. service personnel) in the presence of the minimum required number of authorised personnel.

All access is tracked.

Personnel authorised to access restricted areas must comply with specific INTESA procedures.

5.1.3 Energy and Air-Conditioning

The Server Farms are air-conditioned. The air-conditioning systems are duly monitored to prevent the spread of harmful substances. The ducts do not bypass the control systems installed between the security areas.

Additional stand-alone electric power generators are installed outside of the building and are subject to periodic testing.

5.1.4 Risk of flooding

The Data Centres used are equipped with systems to detect any flooding.

5.1.5 Fire prevention and protection

The fire prevention and protection measures put in place comply with current regulations.

5.1.6 Data storage devices

The devices used to store data are located in secure areas. Procedures are in place to cover their entire lifecycle, from purchase to disposal.

5.1.7 Waste disposal

Waste is disposed of according to the regulations in force.

The disposal of storage devices involves deletion or destruction to prevent disclosure of data.

5.1.8 Off-site Backup

Backups are stored at sites separate to the original site.

5.2 Procedural controls

This section describes the requirements relevant to the trust service roles assigned, together with the responsibilities associated with each role.

5.2.1 Roles of PKI personnel

The following personnel are responsible for certification activities, in accordance with Art. 38, par. 1 of the DPCM:

a) *Security manager.*
b) *Time stamp and certification manager*.
c) *Systems technical manager.*
d) *Logistics and technical services manager*.
e) *Inspection and audit manager*.

No individual is assigned more than one of the roles listed above (DPCM, Art. 38, par. 2).

The personnel referred to above have at least five-years' experience in information technology and telecommunications (DPCM, art 38, par. 1).

The figures listed above belong to the INTESA organisation. All of the tasks associated with certification are formally assigned, by way of a signed appointment letter, to INTESA S.p.A. employees.

When it is determined that the employment relationship with a member of the certification system will be terminated, either immediately or in the medium-short term (so-called *Notice period*), they will immediately cease to work with the system, they will no longer have access to the relevant tasks, and they must promptly return all devices and ID documents that enable them to access the reserved areas and documents and continue to perform the duties involved in the trust service.

They shall also be reminded of their obligation not to disclose confidential information that they have had access to, even after termination of the employment relationship.

None of the figures referred to above will be described in detail herein, with the exception of the *Time stamp and certification service manager*, which is the only role with operational responsibilities.

Without prejudice to the responsibilities of the QTSP, some of the responsibilities set out below may be assigned to other organisations. In this case, the security manager, or another specifically appointed employee, will handle dealings with the relevant professionals (DPCM, Art. 38, par. 3).

5.2.1.1 Time stamp and certification service manager.

This person is responsible for generating certificates: he/she is tasked with supervising the certificate issuance and management process, and is responsible for the QTSP's signature devices (HSM).

He/she is therefore responsible for the various aspects involving encryption, and for the appropriateness of and compliance with procedures put in place for:

- safely storing all signature devices: those intended for use by the holders and those kept by the QTSP;
- activation of the signature devices associated with the certificate issuance system (CA), the time stamping system (TSA) and the holders
- generating certificate issuance system keys (CA) and time stamp system keys (TSA); replacing them in emergency situations and as part of normal changeover processes;
- replacing holder keys;
- proper issuance of time stamps and their storage;
- issuing, suspending, revoking and replacing certificates;
- publishing information on certificate status (OCSP / CRL);
- producing and managing backup copies;
- managing tasks associated with the above, including in emergency and disaster situations.

He/she collaborates with the Heads of Security and Auditing to establish, draft and implement security measures concerning the areas within his/her field of competence.

5.2.1.2 CA Operator

CA Operators are responsible for installing, managing and updating the certificate issuance system, including the QTSP signature devices.

The CA Operator role is performed by multiple operators, including the *Time stamp and certification service manager*.

Certain tasks within the remit of the CAO are performed in dual-control mode.

5.2.1.3 RA / LRA Operator

Registration Authority operators are tasked with interfacing with certificate applicants and holders during the registration, certification, revocation and suspension stages.

Their operational responsibilities may also extend to installing, managing and updating RA products.

5.2.1.4 Network and System Administrators

The CA network infrastructure and system managers are appointed by Company Management.

- *System Administrators* are responsible for managing the systems associated with the PKI (certificate and time stamp generation system). If necessary, they may access the rooms where the aforementioned systems are located, provided that they are accompanied by at least one authorised person: access to and time spent at those locations by such persons are recorded in the Audit Journal. The operations they perform on a specific system are recorded in the logs for that system.
- *Network Administrators* are responsible for the local network containing the various central systems of the PKI. If necessary, they may access the rooms where the aforementioned systems are located, provided that they are accompanied by at least one authorised person: access to and time spent at those locations by such persons are recorded in the Audit Journal. The operations they perform are recorded in the logs.

5.3 Checks on appointed personnel

5.3.1 Qualifications and experience

All personnel assigned to the roles referred to in the previous paragraph are INTESA employees and have multiple years' experience in the analysis, development, planning or management of IT systems. This does not apply to LRA operators, who may simply be trained for the specific role.

The Agency is sent an organisational chart of the persons responsible for the trust service (DPCM, Art. 38, par. 1), including detailed, up-to-date CVs, at the outset. An updated version of the chart must be sent with each organisational change.

5.3.2 Verification that appointed personnel satisfy the criteria

INTESA personnel CVs are held in a repository.

Likewise, a declaration of adequate training is required in the case of third-party suppliers, potentially accompanied by a short-form CV.

Before being hired, candidates must submit a self-declaration stating that they have no criminal convictions or pending charges. Within 180 days of being hired, employees must produce the relevant certificate, issued by the public prosecutor's office.

Company guidelines are developed to minimise any conflicts of interest that may arise in relation to work or family contexts.

5.3.3 Training

The appointed personnel have received adequate training and are constantly up-to-date with the technological solutions adopted as part of the INTESA PKI system, with the procedures, security and data privacy policies, and with any organisational changes. Specific training is required for each update made to the certification system.

5.3.4 Disciplinary sanctions

None of the appointed personnel have previously been subject to disciplinary sanctions for breaching security measures, nor do they currently hold positions that are incompatible with their certification service roles.

5.3.5 Checks on third-party personnel

The QTSP INTESA prepares periodic audit plans for strategic service suppliers, and for organisations appointed to perform the LRA role.

5.4 Audit logging

The audit journal (DPCM, Art. 36) consists of a set of recordings made, including automatically, by devices installed at the QTSP premises. Recording can be performed independently, including on separate media of different kinds.

5.4.1 Type of events recorded

All INTESA systems keep track of significant operations: the log files produced are kept and managed in such a way as to prevent tampering of any kind.

Among other events, the Audit Journal records:

- Access to the PKI systems
- Physical access to the data centres
- Events related to the certificate (issuance and lifecycle)
- Customisation of the signature device

Events are classified based on level of significance: the lowest level relates to events of an informational nature, including normal activities (e.g. requesting a certificate, issuing a new CRL), the maximum level relates to critical events, such as errors attributable to an operator (e.g. attempts to perform an unauthorised operation) or HW or SW malfunctions.

5.4.2 LOG Frequency

Events are collected in real time by dedicated SW. The data is monitored and verified daily to guarantee a full audit.

5.4.3 LOG Storage

All log data are stored for at least 20 (twenty) years.

5.4.4 Log Protection

The progressive numbering of events, specification of when they occurred and use of the digital signature essentially eliminate the possibility of changes being made to the file. The log collection and management SW features a control system that makes it impossible to modify the logs collected.

The *Audit Manager* is responsible for inspecting the logs; he/she must be accompanied by at least one authorised person when accessing them.

5.4.5 Log backup procedures

Logs are stored in triplicate on three dedicated servers, physically located at the primary site and the DR site. When there is no more physical space on the servers, the data will be logged to the NAS system.

5.4.6 Log accumulation system

Log accumulation takes place within the specific systems involved, by way of an application dedicated to the so-called Audit Journal.

5.4.7 Notifying the persons who caused the events

The *Security Manager* notifies the persons who caused the events, and their manager, in writing.

5.4.8 Vulnerability verification

Log vulnerability verifications are performed together with the general INTESA Risk Assessment process.

5.5 Document archive

5.5.1 Type of documents and archived events

As required by DPCM 22/02/2013, the following documentation and events are subject to archiving.

5.5.1.1 Hard copy archive

This includes all documentation signed by the Holder when submitting the registration request, and all other documents submitted (e.g. documentation proving any representative powers or restrictions on use).

The documentation produced includes a copy of the identity document.

The aforementioned hard copy documentation can later be subject to optical storage, to facilitate consultation by authorised INTESA personnel.

5.5.1.2 Electronic documentation

This includes the data recorded in the Audit Journal and the time stamp system events.

In particular, all time stamps issued by the validation system are stored in a dedicated non-modifiable digital archive, for a period of at least 20 (twenty) years, or longer at the request of the subject.

5.5.1.3 Documentation that may be electronic or hard copy

All documentation relating to suspension or revocation requests submitted by the Certification Authority, the Holder or the Interested Third Party.

If the aforementioned documentation is submitted in hard copy, it can later be subject to optical storage, to facilitate consultation by authorised INTESA personnel.

5.5.1.4 Additional documents

Reports, including those relating to the generation of CA and TSA keys, potentially in digital format and digitally signed by the appointed personnel.

5.5.2 Storage period

All elements referred to in the above par. *5.5.1* are stored for 20 (twenty) years.

5.5.3 Archive protection

In accordance with specific procedures, the integrity of archived data is guaranteed by the digital signature.

Data classified as confidential is protected against unauthorised disclosure.

5.5.4 Archive backup procedures

5.5.4.1 Hard copy archive

The information contained in hard copy documents is securely stored at the QTSP premises or at the premises of the appointed LRAs, subject to agreement.

5.5.4.2 Electronic archive

Data is backed up on a daily basis. The archives are consolidated and backed up on a weekly basis. A monthly back-up is performed on the last Saturday of each month.

5.5.5 Requirements in relation to time reference for records

Records must include a time reference, as described in this document.

5.5.6 Integrity verification

The integrity of the CA INTESA archive is verified:

- periodically, at the time of scheduled security Audits;
- whenever a full security audit is requested.

5.5.7 Procedures for obtaining and verifying the archived information

In accordance with Reg. (EU) 2016/679 (GDPR), access to personal data and related information can be requested at any time.

Information relating to controlled-access systems can only be examined by the appointed personnel and the assigned Auditors.

5.6 QTSP key renewal

This paragraph covers the planned replacement of the QTSP keys, and relates to both the certification system keys (CA and TSA) and the time stamp system keys.

5.6.1 Renewal of CA keys

Within the period of time required by current regulations, and prior to the expiry of the certificate associated with the CA Key pairs (CA and TSA) used by the systems to issue signature/seal certificates and TSA certificates, the QTSP will perform the steps provided for in Art. 30 of the DPCM.

The operation is performed in dual-control mode, in the presence of the *Certification Service Manager*.

The activity is planned so as to ensure continuity of services, taking into account the fact that the validity period of the qualified certificate must expire at least two years prior to the expiry of the validity period for the certification keys used to verify its authenticity, as required by the DPCM (Art. 18, par. 3).

A record will be kept of the activities performed, and the report will be stored by the QTSP for 20 (twenty) years from the date of expiry of the certificate.

5.6.2 Renewal of time stamp keys

In accordance with the provisions of Art. 49, par. 2 of the DPCM, in order to limit the number of time stamps generated with the same time-stamp key pair, the latter are replaced within 90 (ninety) days of their issue. A certificate is also issued for the new key pair at that time, without revoking the certificate for the replaced key pair.

5.7 Compromise and disaster recovery

5.7.1 Managing security incidents

In accordance with Art. 19(2) of the eIDAS Regulation, the QTSP is required to notify the supervisory body (AgID) and, where applicable, other interested bodies – such as the competent national information security organisation, or the data protection authority – of any security breaches or integrity losses that may have a significant impact on the trust services provided and the personal data held.

If it seems probable that the security breach or integrity loss has negatively impacted a natural or legal person to whom the trust service has been provided, the trust service provider shall also promptly notify that natural or legal person of the security breach or integrity loss.

The severity levels set out in the *ENISA ART.19 Incident Reporting Guidelines* are specified here below:

1. No impact
2. Insignificant impact: provider assets were affected but no impact on core services
3. Significant impact: part of the customers/services is affected
4. Severe impact: large part of the customers/services is affected
5. Disastrous: the entire organisation, all services, all certificates are affected

With regard to each severity level, and by way of example, the ENISA document sets out a series of events classified as security incidents. For further information, see the document, available on the ENISA website (*https://www.enisa.europa.eu/publications/article19-incident-reporting-framework*).

5.7.2 CA INTESA signature device failure

In the event of failure of the device containing the certification keys, and depending on the type of failure, it may be necessary to either re-initialise the device or to initialise a new one, in order to recreate the original keys.

Everything will be recorded, signed and stored for 20 (twenty) years.

The supervisory body will be notified of such events as security incidents.

5.7.3 Certification key compromise

In the event that the certification keys are compromised, the root certificate revocation procedure will be activated. The QTSP INTESA will generate a new key pair, as set out in par. 5.6.1.

If the time stamping keys are compromised, the relevant certificate will be revoked and the keys will be recreated, as described in 5.6.2.

If the two aforementioned events occur simultaneously, the certificates issued and timestamped using the affected keys will be revoked at the request of the Certification Authority (DPCM, Art. 23). The steps set out above will be followed, and the certificates will be re-issued according to normal procedures. Note: this possibility has been evaluated and planned for merely in the interests of completeness, as it is reasonable to assume that it will never arise.

The security incident is reported to the supervisory body and, where applicable, to the other interested organisations.

5.7.4 Managing catastrophic events

The systems are configured in dual-site mode with replicas distributed across multiple sites, making it possible, in the event of a service interruption at one of the sites, to access the services if at least one of the data centre sites is operational.

The QTSP INTESA has a Catastrophic Events Management Plan, involving the following steps:

- Emergency period management: activation of the disaster recovery solutions
- *Transition period management*: active service and restoration of additional *disaster recovery* solutions;
- *Return to standard operating mode*: at the original site or at an alternative permanent site.

For the purposes of managing the emergency, off-site replication of the data is performed. Within 24 hours, trained personnel will activate DR site functionality.

5.8 Termination of CA or RA activities

In the event of termination of one or more of the QTSP services, disruption to those who signed contracts for use of the discontinued services, and associated third parties, must be kept to a minimum. In particular, continuity of the information required to verify proper performance of the trust services must be ensured.

Termination of the Services may be planned, if the QTSP INTESA deliberately chooses to no longer provide the services for which it acts as QTSP from a certain date, or may be due to reasons outside of the control of the QTSP.

In accordance with the eiDAS Regulation, the QTSP INTESA prepares a *Termination Plan*, an up-to-date copy of which is sent to the supervisory body. The aim of this document is to describe, in general terms, the procedures put in place by the QTSP INTESA for the eventuality of termination of the trust service provided.

At least six months prior to the planned termination date, the QTSP will provide notice of the decision and associated consequences to the affected persons.

Preferably and if possible, communication will take place by Certified E-mail or, alternatively by e-mail and/or standard post (or registered post in specific circumstances).

Notice will be sent to the following recipients:

- • The competent supervisory and monitoring authorities
- • Those subscribed to the services
- • Certificate holders, if separate to those subscribed to the service
- • The Interested Third Party
- • Third parties involved in the processes, including
  - Third-party Local RAs (par. 1.3.3.4)
  - service providers /product suppliers
  - logistics service providers (server farm)
- • Any other QTSPs with whom there is collaboration

A similar announcement will be made on the QTSP INTESA website - www.intesa.it.

Certificate holders will also be notified of the planned revocation of the signature/seal certificate.

5.8.1 Cancellation of contracts

Termination of the service will result in cancellation of the contracts entered into with:

- • Third-party Local RAs, with revocation of the mandate to operate on behalf of the QTSP
- • The Client or client Company/Organisation

All relevant financial considerations will be assessed and handled by General Management.

5.8.2 Revocation of the certificates and destruction of the keys

Termination of the service will result in the revocation of the certificates associated with the certification and time stamp keys.

Subsequently, the certification keys will be deleted from the devices.

The aforementioned operations will be performed in the presence of the QTSP service managers (par. *1.3*): the operation will be subject to a report, which will be signed at least by the *Time stamp and certification service manager* and the *Inspection and audit manager*.

The CA will notify the Agency and the holders of the revocation within 24 hours.

Before proceeding to revoke the certificates associated with the certification keys, a procedure will be carried out to revoke all signature/seal certificates signed by the CA.

Once the certificates have been revoked, the keys associated with the remote signature certificates located on the remote signature devices held by the Certification Authority will be deleted. In the case of any devices held by third parties on behalf of the Certification Authority (DPCM, Art. 3, par. 4), an audit will be carried out at the sites where the device is held, to ensure proper deletion of the signature/seal keys.

The operation will be subject to a report, which will be signed at least by the *Time stamp and certification service manager* and the *Inspection and audit manager*.

As regards the individual signature devices distributed (smartcard/USB token), specific notice will be sent to holders, recommending that they destroy the device following revocation of the certificate associated with the signature/seal keys contained therein.

6 Technical Security Controls

6.1 Generating and installing the keys

6.1.1 Generating certification key pair (CA and TSA)

Certification keys are generated in the signature devices stored at the QTSP premises and in the presence of the *Time stamp and certification service manager*, as provided for by the DPCM, Art. 7, par. 1, following prior initialisation of the signature devices.

The entire process takes place, furthermore, in the presence of a sufficient number of company managers to prevent illegal transactions.

Initialisation of the signature device requires the creation of multiple devices (USB token) that enable management of the HSM; these are created according to an *m of n* logic: the n devices are stored in separate physical locations, as are the passwords to the authorisation devices.

A record will be kept of the activities referred to in the previous points, and the report will be stored by the Certification Authority for 20 (twenty) years from the date of expiry of the certificates.

Following generation of the certification keys, the public key certificates are then generated, signed with the relevant private keys and registered in the certificate directory according to the methods established.

Certification key certificates are sent to the Agency.

The length of certification keys complies with the regulations in force on each occasion.

6.1.2 Generation of the time stamping unit key pair (TSU)

Generation of the time stamping unit keys takes place in accordance with Art. 49 of the DPCM.

The operation is performed in the presence of the *Time stamp and certification service manager* or a person appointed by the latter.

A public key certificate is generated, and is valid for 10 (ten) years, signed with the private key generated for that purpose by the Certification Authority.

A record will be kept of the activities referred to in the previous points, and the report will be stored by the Certification Authority for 20 (twenty) years from the date of expiry of the certificates.

In order to replace the keys and the TSU certificate as provided for in Art. 49, par. 2 of the DPCM, the operation is scheduled to take place at maximum intervals of 3 months.

The length of the certification keys complies with the regulations in force on each occasion.

6.1.3 Generating the signature/seal key pair

The signature/seal keys can be generated by the Holder or by the Certification Authority.

For remote signatures, it is possible to securely export the private keys and securely replicate the keys contained on the HSM, for the purposes of achieving a highly reliable configuration of the secure device.

6.1.4 Length of the keys and signature algorithms

The system uses an RSA encryption algorithm, and a SHA-256 signature algorithm.

The length of the certification keys complies with the regulations in force on each occasion.

6.1.5 Key usage (keyUsage)

In accordance with the Guidelines and the eIDAS Regulation, the keyUsage field of the certificates is set as follows:

- CA - TSA
  (root certificate)
  keyUsage: keyCertSign + cRLSign
- TSU
  (time stamping unit certificate)
  :keyUsagedigitalSignature
  extKeyUsage: timeStamping
- Electronic signature
  Electronic seal
  (qualified certificate)
  keyUsage: nonRepudiation

6.2 Private key protection

All key pairs are generated within the encryption device.

6.2.1 Standard for encryption modules

The Certification Authority uses HSM-type (Hardware Security Module) encryption modules as signature devices for its systems (to issue certificates and generate time stamps). These are connected to the system via the TCP/IP protocol using an Ethernet-type connection.

It is declared that these conform to CC EAL 4+ (Common Criteria Assurance Level 4+)

The remote signature devices conform to the criteria set out in Annex II of the eIDAS Regulation (QSCD).

6.2.2 Multi-person control of the private key

The encryption devices can only be activated and managed in the presence of an adequate number of authorised persons (at least two).

6.2.3 Depositing the private key with third parties

The private keys are not deposited with third parties.

6.2.4 Private key backup

The private certification keys are not subject to backup.

The time stamp keys are not subject to backup.

6.2.5 Private key archiving

An encrypted backup of private keys is archived off-site.

6.2.6 Introduction of the private key in encryption module

The QTSP INTESA only generates the key pair within the encryption device.

Certification key backup is restored in dual-control mode, and always in the presence of the *Time stamp and certification service manager*.

6.2.7 Private key storage

The private keys are generated within the device and stored there and protected using the device's own security mechanisms.

6.2.8 Private key activation

The CA, TSU and remote signature encryption devices can only be activated in dual-control mode, and always in the presence of the *Time stamp and certification service manager.*

6.2.9 Private key deactivation

The CA, TSU and remote signature encryption devices can only be activated in dual-control mode, and always in the presence of the *Time stamp and certification service manager.*

6.2.10 Private key destruction

Tamperproof HSM devices are used across all of the CA (Primary and Disaster Recovery), time stamping and remote signature systems, dedicated to generation and storage of the keys (CA/TSA, TSU, signature/seal). If that device is tampered with or removed (and therefore disconnected from the power source), it is automatically deactivated. To switch the device out of that mode, it must be reactivated using specific security devices.

If the private key is compromised, as a result of the device being locked as described above, the device must be initialised, in dual-control mode and in the presence of the *Time stamp and certification service manager*, in order to delete its contents, and its backups will be re-initialised or destroyed.

A report on the process will be drafted by the *Audit Manager*, and stored for 20 (twenty) years.

6.3 Additional considerations regarding management of the keys

6.3.1 Public key archiving

The public certification keys are archived by INTESA in the certificate directory.

6.3.2 Period of validity of the keys

The period of validity of the certificates associated with the CA keys is at least 15 (fifteen) years.

The period of validity of the certificates associated with the TSU keys is at least 10 (ten) years. The TSU keys are in any case replaced, without revocation of the relevant certificate, within a maximum of 90 (ninety) days, in order to limit the number of time stamps issued per key pair.

The standard period of validity of the signature/seal certificates is 24 months, unless otherwise agreed upon with the client.

6.4 Activation codes

CA operators are provided with "m of n" activation codes to activate and manage CA/TSA and TSU encryption devices.

Each person who is assigned an encryption device must undertake the necessary due diligence in storing the activation codes.

6.5 Security controls on the machines

6.5.1 Specific security requirements

As well as separation of roles (par.1.3), all activities performed are recorded in logs (system and application).

6.5.2 Security classification

The CA components of INTESA meet the verification requirements in accordance with the security criteria established by the regulations in force.

6.6 Security control management

INTESA has rules, procedures and processes in place for managing and updating security controls.

6.7 Network security controls

The INTESA network is protected by a Firewall and IDS (Intrusion Detection System).

The INTESA PKI network is a dedicated network, protected by a specific Firewall, within the INTESA network.

The machines dedicated to the PKI are subject to hardening and only allow the necessary tasks to be performed.

Communication among the machines at the INTESA PKI sites and the LRAs is protected, and occurs by way of specifically authorised communication ports.

Penetration Testing and *Vulnerability Assessments* are carried out periodically in accordance with current regulations.

6.8 Synchronisation with the standard time

All machines included in the QTSP INTESA PKI system are synchronized with the I.N.RI.M. – *Istituto Nazionale di Ricerca Metrologica* (National Institute of Metrological Research) in Turin, formerly *Istituto Elettrotecnico Nazionale* (National Electrotechnical Institute) *Galileo Ferraris*. This function is performed by specific software installed on each server, which connects to the configured remote server via the NTP (Network Time Protocol). I.N.RI.M. provides a synchronization service for computer systems connected to the Internet, based on two primary NTP servers installed in the Time and Frequency Standard Laboratory. They are synchronized via a time and date code generator by caesium beam atomic clocks, also used to generate the Italian national time scale UTC (IT). The time gap between I.N.RI.M NTP servers and the Italian national time scale is monitored and is usually less than a few milliseconds. The synchronization accuracy that can be obtained depends on the network type and the distance placed between the NTP server and the computer to be synchronized; the typical deviation values are less than a millisecond for systems belonging to the same network and can reach a few hundred milliseconds for remote networks.

The time references applied by the applications are strings in date format (DD/MM/YYYY HH:MM:SS) and are precise to the nearest second. They represent the local time according to the machine configuration. Such references comply with Art. 51 of the DPCM.

All records made in the Audit Journal contain time references that, having been generated as described above, are binding on third parties (Art. 41 of the DPCM).

6.8.1 Monitoring synchronisation with the standard time

The servers dedicated to time stamping services also have software control between the machine time and a large number of NTP servers distributed worldwide: the control utility, installed on each of the servers used by the INTESA QTSP as part of the time validation, periodically checks the alignment of the system clock these reference NTP Servers If the time alignment does not comply with the technical specifications of reference time by time in force, the time stamping service provided by the specific server that is misaligned is stopped. At the date, the time validation system will be blocked if a tolerance threshold set at 1 (one) minute second (in absolute value) is exceeded.

The appointed personnel will be notified in the event that the system is blocked, to enable them to verify the reasons and intervene appropriately.

7 Certificate profiles and CRL - Certificate Policy

The certificate profiles and CRLs issued by the QTSP INTESA comply with the specifications set out in the RFC5280 (Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile) and the reference ETSI EN standards under the eIDAS Regulation and the Guidelines.

7.1 Certificate profiles

The QTSP INTESA CA root certificate profiles, and the certificates issued by them, are set out here below.

All root certificates are included in the EUTSL - EU Trusted List of Trust Service Providers.

7.1.1 CA - Certification Authority - Qualified Electronic Signature

This paragraph describes the certificates associated with the *qualified electronic signature service*.

A. Root certificate

The QTSP INTESA root certificates dedicated to the qualified trust service to generate *qualified certificates for electronic signature* have the following OIDs:

- 1.3.76.21.1.3.1
- 1.3.76.21.1.5.1

The root certificates and related content are structured as set out in the *Decision* (for certificates issued while it is in force) and the *Guidelines* and in accordance with the *eIDAS Regulation*.

- ***OID 1.3.76.21.1.3.1 - CA root (30.03.2010 - renewed 16.06.2020))***
  https://e-trustcom.intesa.it/CERTS/CAINTESA2.cer

Summary table:

field	value
Version	v3
Serial Number	4b b1 eb 5b
Signature	sha1WithRSAEncryption
Hash	Sha1
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Validity (20 yrs)	Wednesday 30 March 2010 13:45:24 Sunday 30 March 2025 14:15:24
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	1d 75 8b d9 cf 85 83 82 f3 26 b7 56 77 8a ce 50 db 2c cb 3d
Authority KeyIdentifier	1d 75 8b d9 cf 85 83 82 f3 26 b7 56 77 8a ce 50 db 2c cb 3d
Certificate Policies	Policy: 1.3.76.21.1.3.1 CPS: *http://e-trustcom.intesa.it*
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/INTESA_CA.crl*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Certificate signature, Offline CRL signature, CRL Signature (06)

- ***OID 1.3.76.21.1.3.1 - CA root (renewed 16.06.2020)***
  https://e-trustcom.intesa.it/CERTS/CAINTESA2R.cer

Summary table:

:field	value
Version	v3
Serial Number	4c 39 3a d0
Signature	sha256WithRSAEncryption
Hash	Sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Validity (20 yrs)	martedì 16 giugno 2020 15:16:05 sabato 16 giugno 2035 15:46:05

Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Public Key	rsaEncryption (4096)
Subject KeyIdentifier	F7:29:FB:D8:B4:D8:40:7D:EC:28:BB:5F:F3:7E:50:3D:A1:59:4C:C4
Authority KeyIdentifier	F7:29:FB:D8:B4:D8:40:7D:EC:28:BB:5F:F3:7E:50:3D:A1:59:4C:C4
Certificate Policies	Policy: 1.3.76.21.1.3.1 CPS: *http://e-trustcom.intesa.it*
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/INTESA_CA1.crl*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)

- ***OID 1.3.76.21.1.5.1 - CA root (09.01.2015)***
  https://e-trustcom.intesa.it/CERTS/CAINTESA3.cer

Summary table:

field	**value**
Version	v3
Serial Number	27 7d 09 de 55 2f 88 07
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. CA - Certification Authority**
Validity (20 yrs)	Friday 9 January 2015 14:48:32 Wednesday 9 January 2030 14:48:32
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. CA - Certification Authority**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	b0 e0 26 b6 2b 34 1c 74 78 71 ca 05 90 96 c1 d0 2c 05 8c 44
Authority KeyIdentifier	b0 e0 26 b6 2b 34 1c 74 78 71 ca 05 90 96 c1 d0 2c 05 8c 44
Certificate Policies	Policy: 1.3.76.21.1.5.1 CPS: *http://e-trustcom.intesa.it*
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/INTESA_eCA.crl*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Certificate signature, Offline CRL signature, CRL Signature (06)

B. Qualified Certificate for Electronic Signature

The qualified certificate for electronic signature and related content are structured as set out in the *Decision* (for certificates issued while it is in force) and the *Guidelines* and in accordance with the *eIDAS Regulation*.

The qualified certificates issued by the CA referred to in the previous par. have the following Policy OID:

- 0.4.0.194112.1.2

With reference to the CA root that issued them, the *certificatePolicies* extension also contains the following OIDs:

- 1.3.76.21.1.3.1.1
- 1.3.76.21.1.5.1.1

Qualified certificates issued in accordance with the guidelines contain a code, in the *certificatePolicies* (OID 2.5.29.32) field, for a PolicyIdentifier element with an *agIDcert* value:

- OID 1.3.76.16.6

Summary table:

field	value
Version	v3
Serial Number	Defined by the CA and unique in the context of that CA
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=<<ca emittente>>**
Validity	Contractually defined
Subject DN	*PROFILE CONFORMS TO:* *ETSI-319.412-2* *Guidelines*
Public Key	rsaEncryption (2048) or higher
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	AKI of the issuing CA
Authority Information Access	CA Issuers - URI: *https://e-trustcom.intesa.it/CERTS/<<nomeCAcert>>.cer* OCSP - URI: *https://e-trustcom.intesa.it/<<nomeOCSP>>*
qcStatements	**qcStatement:** REF ETSI 319 412-5 points 4.2 - 4.3 (4.2.1) 1. This is a Qualified Certificate that conforms to Annex I, III or IV of Regulation (EU) No. 910/2014 (4.2.2) 2. The certified public key is contained in a Secure Signature Creation Device (QSCD) (4.2.3) 3. Certificate type: id-etsi-qct-esign (4.3.3) 4. This certificate has a "retention" period of 20 years with regard to the CA. (4.3.4) 5. Certificate of conformity: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.2 Policy: 1.3.76.21.1.3.1.1 or 1.3.76.21.1.5.1.1 CPS: *https://www.intesa.it/e-trustcom/* - and any restrictions on use Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specific to the certificate

7.1.2 CA - Certification Authority - Qualified Electronic Seal and Signature

This paragraph describes the certificates associated with the CA dedicated to *qualified services for electronic seal and electronic signature*.

A. Root certificate (OID 1.3.76.21.10.2.1)

The QTSP INTESA root certificate dedicated to the qualified trust service for generating *qualified certificates for electronic seal and electronic signature* has the following OID:

- 1.3.76.21.10.2.1

The root certificate and related content are structured as provided for in the Guidelines and comply with the *eIDAS Regulation.*

- ***OID 1.3.76.21.10.2.1 - CA root (18.03.2020)***
  https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer

Summary table:

field	value
Version	v3
Serial Number	59CB 51E D 07 46 5 CC3
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Validity (20 yrs)	Wednesday 18 March 2020 17:52:05 Sunday 18 March 2040 17:52:05
Subject DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Public Key	rsaEncryption (4096)
Subject KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Certificate Policies	Policy: X509v3 Any Policy CPS: *https://intesa.it/e-trustcom/*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Certificate signature, Offline CRL signature, CRL Signature (06)

B. *Qualified certificate for electronic seal (OID 1.3.76.21.10.2.1.1)*

The qualified certificate for electronic seal and related content are structured as provided for in the Guidelines and comply with the *eIDAS Regulation.*

The qualified certificates for electronic seal issued by the CA referred to in the previous par. have the following Policy OID:

- 0.4.0.194112.1.3

With reference to the CA root that issued them, the *certificatePolicies* extension also contains the following OID:

- 1.3.76.21.10.2.1.1

Qualified certificates issued in accordance with the guidelines contain a code, in the *certificatePolicies* (OID 2.5.29.32) field, for a PolicyIdentifier element with an *agIDcert* value:

- OID 1.3.76.16.6

Summary table:

field	value
Version	v3
Serial Number	Defined by the CA and unique in the context of that CA
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Validity	Contractually defined

Subject DN	*PROFILE CONFORMS TO:* *ETSI-319.412-3* *GUIDELINES*
Public Key	rsaEncryption (2048) or higher
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority Information Access	CA Issuers - URI:*https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer* OCSP - URI:*https://e-trustcom.intesa.it/ocsp*
qcStatements	**qcStatement:** REF ETSI 319 412-5 points 4.2 - 4.3 (4.2.1) 1. This is a Qualified Certificate that conforms to Annex I, III or IV of Regulation (EU) No. 910/2014 (4.2.2) 2. The certified public key is contained in a Secure Signature Creation Device (QSCD) (4.2.3) 3. Certificate type: *id-etsi-qct-eseal* (4.3.3) 4. This certificate has a "retention" period of 20 years with regard to the CA. (4.3.4) 5. Certificate of conformity: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.3 Policy: 1.3.76.21.1.10.2.1.1 CPS: *https://www.intesa.it/e-trustcom/* - and any restrictions on use Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specific to the certificate

C. *Qualified certificate for electronic signature (OID 1.3.76.21.10.2.1.2)*

The qualified certificate for electronic signature and related content are structured as provided for in the Guidelines and comply with the *eIDAS Regulation.*

The qualified certificates for electronic signature issued by the CA referred to in the previous par. have the following Policy OID:

- 0.4.0.194112.1.2

With reference to the CA root that issued them, the *certificatePolicies* extension also contains the following OID:

- 1.3.76.21.10.2.1.2

Qualified certificates issued in accordance with the guidelines contain a code, in the *certificatePolicies* (OID 2.5.29.32) field, for a PolicyIdentifier element with an *agIDcert* value:

- OID 1.3.76.16.6

Summary table:

field	value
Version	v3
Serial Number	Defined by the CA and unique in the context of that CA
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**

Validity	Contractually defined
Subject DN	*PROFILE CONFORMS TO:* *ETSI-319.412-2* *GUIDELINES*
Public Key	rsaEncryption (2048) or higher
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority Information Access	CA Issuers - URI: *https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer* OCSP - URI: *https://e-trustcom.intesa.it/ocspsl*
qcStatements	**qcStatement:** REF ETSI 319 412-5 points 4.2 - 4.3 (4.2.1) 1. This is a Qualified Certificate that conforms to Annex I, III or IV of Regulation (EU) No. 910/2014 (4.2.2) 2. The certified public key is contained in a Secure Signature Creation Device (QSCD) (4.2.3) 3. Certificate type: *id-etsi-qct-esign* (4.3.3) 4. This certificate has a "retention" period of 20 years with regard to the CA. (4.3.4) 5. Certificate of conformity: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.2 Policy: 1.3.76.21.1.3.1.1 or 1.3.76.21.1.5.1.1 CPS: *https://www.intesa.it/e-trustcom/* - and any restrictions on use Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specific to the certificate

7.1.3 Digital signature certificate in specific closed user contexts

Prior to completion of the holder identification process, a certificate can be issued that is valid for a limited period of time (30/60 minutes). This option only applies in specific circumstances associated with limited use of the digital signature in closed user contexts, in which the digital signatures generated have no legal effect if the certificate holder identity verification process is not successfully completed.

This option was confirmed by the Agency in its notice to the CAs on 7 June 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", concerning "*Request for clarification regarding the use of digital signatures in specific closed user contexts*".

The communication referred to above sets out the following restrictions:

1) The process is only available for remote signature systems;
2) The digital signature must be used in closed user contexts;
3) The Holder's qualified certificate must include strict restrictions on use associated with the specific relationship (e.g. client and financial institution) between the Holder and co-interested party and co-signatory;
4) With a view to clearly distinguishing between these certificates and those issued in accordance with more traditional procedures, the Holder's qualified certificate must contain a specific OID, which can be found in the operating manual, that describes this particular process and the relevant closed context;
5) Strict application restrictions must be established: the remote signature application must limit the objects that can be signed to the documents presented by the co-interested party and co-signatory. The documents that can be signed must be legally imperfect, i.e. have no legal effect until they are signed by the co-interested party and co-signatory. For example, contracts to sign up for a service;

6) If verification of the Holder's identity takes place by way of an in-person meeting between the Holder and a person appointed to perform identity verification, the latter must be an employee of the Certification Authority or appointed by the latter, but shall not be an employee or appointee of the co-interested party and co-signatory, if separate from the Certification Authority;
7) The co-interested party and co-signatory can perform the identity verification in lieu of the Certification Authority via audio-video sessions (under the well-known standard conditions) or in accordance with regulations concerning identity verification referred to in Italian Legislative Decree 231/2007, where applicable. If a bank transfer is used as part of the verification process in accordance with the aforementioned Italian Legislative Decree, it must be verified that the transfer originates from a bank account in the sole name of the certificate holder;
8) The time stamp must not be applied when the Holder signs; it is, instead, mandatory that it is applied when the co-interested party and co-signatory sign, making the document legally perfect;
9) Until such time as the signature and stamp referred to in point 8 above are applied, the object signed by the Holder alone must not be presented to anyone and, if the Holder verification process is unsuccessful, it must be destroyed, with the events being recorded in specific logs.

For the purposes of complying with point 4), a certificate issued under these conditions must be distinguishable from the others: to that end, the QTSP INTESA has identified the following three OIDs to preserve the reference to the root CA that issued the certificate:

- *1.3.76.21.1.3.1.1.1*
- *1.3.76.21.1.5.1.1.1*
- *1.3.76.21.10.2.1.2.1*

A description of the procedure involving issuance, signing and application restrictions will be included in the relevant operating manuals.

7.1.4 Certificates issued with electronic identities

In accordance with art. 24, point 1, b) of the eIDAS Regulation, the QTSP INTESA can proceed to the verification of the identity of the qualified certificate applicant through a SPID authentication procedure with level 2 or 3 credentials.

7.1.4.1 SPID

The qualified Certificate issued through a SPID digital identity shall include in addition the ***OID 1.3.76.16.5***, registered by the Agency with the following description: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*".

Any further qualified certificate issued following a request signed by an electronic signature based on this type of qualified certificate must, in turn, contain the above mentioned OID.

7.1.4.2 CIE (Carta di Identità Elettronica – Electronic Identity Card)

In accordance with art. 24, point 1, b) of the eIDAS Regulation, the QTSP INTESA can proceed to the verification of the identity of the qualified certificate applicant through a CIE authentication procedure with, at least, a *significative* level.

The QTSP INTESA has decided to include a specific additional OID, in order to identify the qualified certificates issued following this type of identification.

to maintain the reference to the root CA that issued the certificate, the OIDs will be:

- *1.3.76.21.1.3.1.1.2*
- *1.3.76.21.1.5.1.1.2*
- *1.3.76.21.10.2.1.2.2*

7.2 CRL - Certificate Revocation List Profile

The CRL format complies with RFC 2459.

The following fields are included:

- Version
- Certification Authority

- Effective date
- Next update
- Signature algorithm
- Authority key Identifier
- CRL Number

7.2.1 Entry extensions

- Certificate serial number
- Revocation date
- Revocation reason (*reasonCode*)

7.3 OCSP Profile

The eIDAS Regulation makes it mandatory to provide information on the certificate status via the OCSP protocol.

The response format complies with RFC 6960.

7.4 Time stamping profile

The format of the Time Stamp meets the requirements set out in the eIDAS Regulation and, specifically, *ETSI-319.422*. The OID specified in the policy field of the TSTs is 0.4.0.2023.1.1.

The time stamp contains the information required by the relevant regulations (RFC 3161, point 2.4.2), without prejudice to the requirements set out in *ETSI-319.422*:

- Version
- Policy
- messageImprint
- serialNumber
- genTime
- accuracy
- TSA

8 Conformity audits

The QTSP INTESA is subject to periodic audits for the purposes of issuing and maintaining certification in relation to its trust services in accordance with the eIDAS Regulation.

That same regulation requires verification of the conformity of the organisation and its services by a *CAB (Conformity Assessment Body*) accredited by the national *Accreditation Body* (for Italy: Accredia - *https://www.accredia.it*).

The QTSP sends the conformity reports to the Supervisory Body within three days of receiving them.

8.1 Frequency of audits

Qualified trust service providers are subject to an audit by a conformity assessment body every 24 months.

Furthermore, the supervisory body (AgID) may request to perform an audit at any time, or request that a conformity assessment body carries out a conformity assessment.

Finally, audits are carried out of service providers, including organisations tasked with performing the Local Registration Authority tasks. Such audits are performed by persons included on the QTSP organizational chart.

8.2 Identity and qualifications of the auditors

Audits are performed under the responsibility of an accredited conformity assessment body, which in turn uses qualified and accredited professionals.

8.3 Relationship between the QTSP and the Auditor

The auditors appointed by the *conformity assessment body* have no relationship with the QTSP INTESA.

The *Inspection and audit manager* (par. 1.3) and the *Time Stamp and Certification Service Manager* belong to different company departments.

8.4 Subject-matter of the audits

The audits conducted by the conformity assessment body focus on procedural and organisational aspects of the QTSP's performance of the trust service activities. They therefore involve a thorough examination of the requirements set out in the eIDAS Regulation and reference ETSI standards.

Audits of service providers or LRAs focus on specific aspects of the service provision or the tasks performed.

8.5 Identifying non-conformities

In the event that a non-conformity is identified, an *Action Plan* is developed that sets out the actions required to resolve the reported non-conformity.

The timescale for handling and resolving the issue is linked to the degree of severity of the non-conformity.

8.6 Notification of results

The QTSP sends the conformity reports to the Supervisory Body within three days of them being received from the conformity assessment body.

The results of audits conducted by the QTSP are shared with the managers referred to in par. 1.3 and with company management.

9 General conditions

9.1 Fees

The fees for the certification and time stamp service are published on the QTSP website.

For specific projects, fees are agreed upon at a contractual level with the individual client.

Access to information on the certificate status (CRL and OCSP) is freely available and free of charge.

The QTSP provides free access to verification software (https://www.intesa.it/e-trustcom/).

9.2 Financial liability - insurance cover

As well as satisfying the minimum company capital requirements, INTESA has insurance policies in place to cover risks associated with the activities and damage to third parties, the content of which satisfies the requirements for performing the professional activities in question.

AgID has been provided with a specific declaration regarding the existence of such a policy.

9.3 Protection of confidential information

All of the confidential information that QTSP INTESA obtains while managing the services covered by this CPS is stored and processed in accordance with the data privacy regulations in force (Italian Legislative Decree 196/03 and Reg. (EU) 2016/279 as subsequently amended and supplemented).

All personal or company information that does not appear on the qualified certificate is considered *Confidential*.

9.4 Personal Data Protection

With regard to the QTSP trust service activities covered by this CPS, INTESA acts as *Personal Data Controller*, in accordance with the data privacy regulations in force (Italian Legislative Decree 196/03 and Reg. (EU) 2016/279 as subsequently amended and supplemented).

Specifically, the personal data processed are collected during the Holder identification and registration phase.

9.5 Intellectual Property

This document is the exclusive property of In.Te.S.A. S.p.A., which is the Holder of all related intellectual property rights: all aspects related to the performance of INTESA's activities set out herein are subject to intellectual property rights.

All material provided by INTESA to the Subscribers and their operators to enable them to use the Public Key Infrastructure (PKI) functions managed by INTESA is covered by intellectual property rights.

9.6 Obligations

The obligations of PKI participants are set out here below (par. *1.3*)

9.6.1 Obligations of the QTSP INTESA

In performing its activities, INTESA operates in accordance with the provisions of:

- Italian Legislative Decree no. 82 of 7 March 2005 and subsequent amendments (DAC)
- Italian Prime Ministerial Decree of 22 February 2013 (DPCM)
- Regulation (EU) 2016/679 (GDPR)
- Regulation (EU) 910/2014 (eIDAS)

In particular, the QTSP INTESA:

- implements all appropriate organizational and technical measures to prevent damage to others;
- complies with the technical rules specified in the DPCM;
- guarantees that its Quality System complies with ISO 9001 standards;
- ensures that the signature generation device (HSM) satisfies the security requirements provided for in Art. 29 of the eIDAS Regulation;
- issues the qualified certificate and publishes it, unless otherwise specified by the Holder, in accordance with Art. 32 of DAC;
- provides applicants with clear and explicit information on the certification process, technical requirements to access it, characteristics of signatures issued on the basis of the certification service and restrictions of their use;
- complies with security measures concerning personal data processing (GDPR);
- is not a data repository for generation of the Holder's signature;
- revokes or suspends the electronic certificate if requested by the Holder or the Interested Third Party;
- guarantees precise specification of the date and time of issue, revocation and suspension of electronic certificates;
- keeps a record, including electronically, of all information relating to the qualified certificate for 20 (twenty) years, particularly for the purpose of providing proof of certification in the event of legal proceedings;
- ensures that the identification code (exclusive to INTESA) assigned to each Holder is unique among its users;
- provides all information that may be useful to persons applying to use the certification service in a durable medium. This information includes: the precise terms and conditions for using the certificate, including any restrictions on its use, the existence of an optional accreditation scheme and the complaint and dispute-resolution procedures. Such information, which may be sent electronically, must be written in clear language and be provided prior to the agreement being entered into between the service applicant and the QTSP;
- uses reliable systems to manage the certificate directory in a way that ensures that only authorized persons can make entries and changes, that the authenticity of the information is verifiable, that certificates are only available for public consultation if permitted by the holder of the certificate, and that the operator can identify any events that may compromise the security requirements;
- records the issuance of qualified certificates in the audit journal, specifying the date and time of generation.
- provides or recommends at least one system that enables verification of digital signatures.

Furthermore, the QTSP INTESA:

- generates a qualified certificate for each of the advanced electronic signature keys used by AgID to sign the public list of certification authorities, and publishes it in its own certificate directory in accordance with Art. 42 of the DPCM;
- recommends an electronic signature verification system, as referred to in Art. 14 of the DPCM;
- keeps a copy of the list, signed by AGID, of certificates associated with the certification keys referred to in Art. 43 of the DPCM, publishing it electronically in accordance with Art. 42, par. 3, of the DPCM.

The QTSP INTESA periodically performs audits at the LRA premises to verify compliance with the regulations and this CPS, the relevant Operating Manual, and the provisions of the mandate agreement, in accordance with a sampling plan shared with the LRA.

9.6.2 Obligations of the Holder

Holders who have been assigned a qualified certificate for the trust services provided by the QTSP INTESA covered by this CPS and described in the relevant Operating Manual (OM) are obliged to store the information required to use their private signing key in an appropriate manner, and to take all necessary organisational and technical measures to prevent damage to others (DAC, Art. 32, par. 1).

The key Holder must also:

- provide all information requested by the QTSP, guaranteeing its accuracy under his/her own responsibility;
- send the certification application using the methods specified in this CPS and the relevant Operating Manual;
- notify the QTSP INTESA, including via the LRAs, of any changes to the information provided at the time of registering: personal details, address, phone numbers, e-mail addresses, etc.;
- store the information that enables the private key to be used with the utmost care and diligence;
- send any requests for revocation or suspension of the qualified certificate in accordance with the instructions provided in this CPS;
- not use the signing key for tasks other than those permitted for the specific type of key (Art. 5, par. 5 of the DPCM);
- immediately revoke the digital certificate in the event of loss or theft of the codes used to access his/her signing keys;
- revoke or suspend the digital certificate in accordance with the provisions of this CPS and the relevant Operating Manual.

9.6.3 Obligations of certificate users

The Relying Party is any person who receives a digitally signed document and, for the purposes of verifying its validity, avails of the qualified certificate used by the Holder to sign that document.

Verification of the digital signature and subsequent extraction of the objects signed may be performed using any software capable of processing signed files in accordance with the eIDAS Regulation.

Persons who avail of a qualified certificate to verify the validity of a digitally signed document are required to:

- verify the validity of the certificate containing the public key of the Holder who signed the message, in accordance with the standards in force at the time of its issue;
- verify the certificate validity status using the OCSP protocol or by accessing the Revocation Lists;
- verify the validity of the certification path, based on the public list of the QTSPs;
- verify whether there are any restrictions on the use of the certificate used by the Holder.

9.6.4 Obligations of the Interested Third Party

In the context of the services covered by this CPS, the Interested Third Party is usually the organisation (client) that enters into a contract for the supply of trust services with the QTSP.

The Interested Third Party:

- formally authorises the QTSP to use the *organizationName* field of the certificate (par. 3.1.3.3)
- verifies that the Holder meets all of the necessary requirements and authorises the latter to request issuance of a qualified certificate for electronic signature

- informs the QTSP INTESA of any additional restrictions on use of the qualified certificate
- informs the QTSP INTESA of any titles or representative powers applicable to the Holder

The Interested Third Party undertakes to request revocation of the certificate in the event that the certificate holder leaves the organisation or no longer satisfies the requirements on the basis of which the certificate was issued (e.g. in the event of a change or termination of representative powers).

Requests by the Interested Third Party to revoke or suspend a certificate must be forwarded immediately to the CA when the Holder ceases to meet the requirements on the basis of which the qualified certificate for electronic signature was issued.

The interested third party must also report any changes to the identification details of the company (e.g. company name, registered offices, etc.), termination of the activities by the organisation, and any other information that is relevant or that affects the use of the certificate.

9.6.5 Obligations of the LRAs

For reasons related to providing the service, INTESA relies on additional parties across the country (hereinafter LRAs – Local Registration Authorities) to perform some of the Registration Department's tasks.

Typically, an LRA is required to perform the following activities:

- positive identification of the person applying for certification (the certificate Holder);
- applicant/ Holder registration;
- delivery to the Holder of codes that enable access to their own signing key in accordance with Articles 8 and 10, par. 2, of the DPCM;
- sending documentation signed by the INTESA RA Department, unless otherwise agreed in the mandate agreement.

The Mandate Agreement explicitly establishes the obligations binding upon the LRA, which INTESA is obliged to monitor.

More specifically, the LRA is required to:

- ensure that the identification activities are carried out in accordance with the regulations in force (DAC, DPCM, eIDAS Regulation and anti-money laundering regulations);
- use and process personal data obtained during the identification process in accordance with the GDPR;
- make the material collected during the identification and registration process available to INTESA;
- securely store the documentation collected during the identification and registration process, and send it to the RA Department of the QTSP INTESA at the request of the QTSP;
- grant access to its premises to QTSP personnel, or third parties appointed by the latter, to comply with audit obligations; such access must also be granted to auditors appointed by the Supervisory Body (AgID);
- notify the QTSP INTESA, by way of its RA Department (*uff_ra@intesa.it*) or the relevant INTESA contact people, without delay, of any event or incident relating to the points set out above, and of any security breaches or integrity loss that significantly affect the services covered by this CPS and the relevant Operating Manual or holders' personal data.

9.7 Exclusion of guarantees

No additional obligations are provided for other than those contained in par. *9.6.1*.

9.8 Limitations of liability

Except in *cases of intention or negligence* (eIDAS Regulation, Art. 13), the QTSP INTESA accepts no liability for consequences arising from use of the certificates in a manner other than that provided for in Art. 5 of the DPCM, and in particular from failure by the Holder and the Interested Third Party to comply with the provisions of this CPS, the Operating Manual and/or non-compliance by those parties with the regulations in force.

Likewise, INTESA shall not be held liable for consequences arising from circumstances not attributable to it, including, but not limited to: natural disasters, disruptions to service and/or technical and logistical failures beyond its control, interventions by Authorities, riots or acts of war that also or only affect entities of whose services INTESA avails for the purposes of providing its certification services.

INTESA shall not be held liable for damage resulting from improper use of the qualified certificate in relation to a restriction on use specified on that certificate.

The Holder, having read this CPS and the relevant Operating Manual, must undertake all appropriate special due diligence measures to prevent damage to third parties associated with improper use of the material provided by the QTSP.

Unless otherwise specified, the limitation of liability is contained in the *INTESA General Contract Conditions* (*www.intesa.it*).

9.9 Compensation

Unless otherwise specified, the compensation terms and conditions are contained in the *INTESA General Contract Conditions* (*www.intesa.it*).

9.10 Duration and termination of the contract

Unless otherwise specified, the Contract will come into effect and be valid from the date on which it is signed. The contractual Duration is specified in each individual Contract.

Unless otherwise specified, the termination clauses are contained in the *INTESA General Contract Conditions* (*www.intesa.it*).

9.11 Communication

Requests for information can be submitted to the QTSP contact people, par.*1.3*.

9.12 Managing changes

See par. *1.5.1 - Revision procedure*.

9.13 Dispute resolution procedure

The Court of Turin shall have exclusive jurisdiction in the event of any disputes.

9.14 Applicable law

The laws of Italy and the European Community shall apply.

9.15 Compliance with applicable regulations

In performing its activities, INTESA operates in accordance with the regulations in force and, in particular, with:

- Italian Legislative Decree no. 82 of 7 March 2005 and subsequent amendments (DAC)
- Italian Prime Ministerial Decree (DPCM) of 22 February 2013 as subsequently amended and supplemented
- Regulation (EU) 2016/679 (GDPR) as subsequently amended and supplemented
- Regulation (EU) 910/2014 (eIDAS) as subsequently amended and supplemented

A more comprehensive list of the reference regulations is provided in par. *1.6.2*.

10 Appendix: Verification of signatures and time stamps

10.1 Signature and verification software

10.1.1 Verification software – DigitalSign Reader

As provided for in Art. 14, par. 1 of the DPCM, the QTSP INTESA provides the ***DigitalSign Reader*** application for the purposes of verifying digital signatures and time stamps.

The software and associated documentation are available to download from:

- https://www.intesa.it/e-trustcom/

The software is free to use.

The application makes it possible to verify any electronic archive that has been signed and time stamped, and to view its content, provided that the work station is equipped with suitable software to process that type of archive. For example, the application can view documents with a '.pdf' extension, provided that the Acrobat Reader application is already installed.

Access to a signature device is not required to use the application.

The procedure for verifying a digital signature placed on an electronic document involves the following checks:

- verifying the structure of the cryptographic envelope;
- verifying that the signatory's certificate is not expired;
- verifying that the signatory's certificate has not been revoked or suspended;
- verifying that the signatory's certificate has been issued by a Certification Authority included on the public list of accredited certification authorities;
- verifying the information contained in the qualified certificate, and the mandatory extensions (DPCM, Art. 14, par. 2b);
- enabling electronic updating of the information published on the public list of accredited certification authorities (DPCM, Art. 14, par. 2c);
- verifying the time stamp;
- verifying the validity of the certification certificate (CA and TSA).

For further details on the application, see the user manual included in that application.

10.1.2 DeSigner proprietary platform

The QTSP INTESA offers its clients a solution to provide prompt and/or batch Remote Digital Signature and Time Stamp services, minimising adoption costs for service users.

The ***DeSigner*** INTESA platform allows users to:

- promptly place Qualified Digital Signatures (complete with time stamps) on documents covered by the service and subject to Strong Authentication
- place multiple qualified signatures (including time stamps) on individual documents or on all documents within a specified area
- place a time stamp on a specific document or all documents contained in a specified area
- verify the signature and/or time stamp placed on a specific document or all documents contained in a specified area.

The basic elements that make up the INTESA DeSigner Remote Signature solution are:

- The DeSigner signature server (the signature application component capable of interfacing with signature encryption devices), which will be installed at the INTESA server farm.
- The DeSigner Client component, provided via a SOAP and REST type web services interface, to be integrated into the Client application.
- Signature encryption devices (HSM) of an appropriate size to meet the relevant needs (number of users, and the chosen HA, DR configuration), located at the INTESA Server Farm.
- Integration with Timestamp Servers that provide time stamps to link a document, or the signature placed on that document, to a specific time.
- Integration with the DeAuth authentication solution for Strong Authentication operations related to the signature: generation, sending and verification of the authentication token.
- Integration with the DeVerify Signature and Time Stamp verification solution.
- INTESA Certification Authority.

The proposed solution enables users to interface with the Time Stamp services both directly via the Client applications, in compliance with the RFC 3161 standard, and via the DeSigner component.

Indeed, DeSigner can interface directly with the Time Stamp service, providing it with all of the information required and obtained by the Client web services component and, as such, requesting placement of time stamps on individual documents or a batch of documents.

The DeSigner solution can also interface directly with the Signature and Time Stamp verification services provided by the ***DeVerify*** component.

DeVerify is the Signature and Time Stamp verification service offered by INTESA to perform the following functions:

- Verification of a Digital Signature, with or without a Time Stamp, on a single document or batch of documents for all standard Signature profiles: CADES (P7M), PADES (PDF), XADES (XML)
- Verification of a Time Stamp on a single document or batch of documents
- Verification of multiple Signatures/Time Stamps within the same document
- 3-level Verification of Signatures/Time Stamps: integrity check, compliance with regulatory requirements, date verification with CRL download
- Generation of summary or detailed reports following the verification process

The functions referred to above will also be handled directly by DeSigner, as part of integration with the DeVerify solution, with the support of information provided by the Client web services.

10.1.3 Signature and verification software – DigitalSign

DigitalSign (*CompEd Software Design Srl.*) is the application distributed by the QTSP INTESA for generating and verifying digital signatures and applying time stamps.

The signature device must be configured when activating the solution for the first time, and the list of CA certificates must be updated together with the relevant CRLs. This information is obtained from the list of certification certificates held by AgID.

When using the Signature function, users are asked to select the document to be signed, and to enter the signature device (smartcard or USB token) if not already entered. The selected document is displayed on the application, and the user is asked to enter the signature device PIN code. Finally, the user is asked to save the signed (CADES or PADES) and/or time stamped document, if requested.

The process of generating a digital signature involves the following operations:

- Verifying that the signature/seal certificate specified by the user has not expired.
- Verifying that the private key on the signature device matches the Holder certificate.

The *DigitalSign* application also allows multiple signatures to be placed on a single document.

The signature may also be associated with a time stamp generated by the QTSP INTESA time stamp service.

As well signature generation, the product also offers the following functions:

- Signature verification: this is similar to the function described in par. *10.1.1*.
- Encryption: this function allows a document to be encrypted, providing a certificate that can be used to encrypt the data.
- Decryption: this function allows for the decryption of previously encrypted data.

For further details on the *DigitalSign* application, see the user manual provided with the product.

10.1.4 Signature and verification software – firma4ng

The QTSP INTESA also distributes ***firma4ng*** *(Bit4id)* signature and verification software. This professional digital signature application is compatible with Windows, Linux and Mac OS X operating systems. It provides the option to sign and verify any type of electronic document.

For further details on the *firma4ng* application, see the user manual provided with the product.

10.2 Document format

The applications provided by the QTSP INTESA make it possible to place a digital signature and time stamp on all electronic document formats.

It is, however, important to note that certain types of electronic document will not, in any case, produce the effects described in Art. 21 of the DAC, because they may contain macro-instructions or executable codes that could activate functionality that modifies the documents or data represented therein.

End of document