Trust Service Practice Statement

Ver. 1.11

09/03/2020

History

ID	Changes	Rev.	Data	Author	Verifier	Approval
TSPPS	First release	1.0	07/04/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Clause 4.8 updated to include the maximum delay for certificate status publication	1.1	21/05/2017	F.Barcellini	G.Damiano	P.Sironi
TSPPS	General revision of the document. Added Advanced Electronic signature certificates and qualified	1.2	07/07/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Corrected title, general index, some inaccuracies	1.3	02/08/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Correction on tables in paragraph 7	1.4	15/09/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	General revision of the document	1.5	22/11/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Formatting correction. Modification to paragraph 1.3.1; 1.3.4; 3.1.4; 3.2.4; 3.2.5; 4.2; 4.5.3; 6.2.2; 6.2.8; 6.2.9; 6.2.10; 7; 8.6.	1.6	20/12/17	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Modification to paragraph 3.1.4.	1.7	17/01/18	F.Barcellini	G.Damiano	P.Sironi
TSSPS	Modification to paragraphs 3.1.3, 3.2.3, 3.2.6 and 3.2.7.	1.8	13/03/18	F.Barcellini	G.Damiano	P.Sironi
TSSPS	Modification to paragraphs 3.4, 9.3.3 e .94	1.9	20/07/18	F.Barcellini	G.Damiano	P.Sironi

TSPPS	Modification to paragraphs 4.2, 6.1.1.2, 6.1.2	1.10	08/07/2019	F.Barcellini	G.Damiano	P.Sironi
TSPPS	Modification to paragraphs 1.3, 1.3.2, 1.3.6, 1.4, 1.6, 2.2, 3.1.1, 3.1.2, 3.1.3, 3.1.6, 3.1.7, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 4.1.2, 4.3.1, 4.4.1, 4.4.2, 4.9.1, 4.9.2, 5.1,5.2, 5.3, 5.4.1, 5.8, 6.1.5, 6.1.6, 6.2.1, 6.2.2, 6.6, 8. Added paragraphs 1.3.7, 3.2.8, 4.3.1.1, 4.3.2, 7.1.7, 7.1.8, 7.2.1, 7.2.2, 7.2.3, 7.2.4	1.11	09/03/2020	F.Barcellini V. Manaila	G.Damiano	P.Sironi

Index

1 INTRODUCTION

1.1 Overview

This Trust Service Practice Statement (TSPPS) describes the technical, security and organizational requirements implemented by Intesi Group S.p.A. (hereafter referred to also as “Intesi Group”) applicable to all the Trust Services that it provides and the trust service tokens that it issues:

- qualified signature certificates issued to natural persons;
- qualified seal certificates issued to legal persons;
- Time Stamping Unit certificates issuing qualified Timestamp Tokens;
- certificates and the CRLs issued by the above mentioned CAs and the related OCSP services;
- qualified timestamp tokens generation;

The qualified trust services comply with the relevant requirements of the eIDAS regulation (Regulation (EU) N°910/2014) and conforms to the following standards:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

The structure of this TSPPS conforms to the public specification [RFC 3647] and refers to the Certificate Policy whose OIDs are specified in subsection 7.1.3, hereafter referenced as “related TSPPs”. This TSPPS applies to the following certificates issued by Intesi Group:

- The CA root certificate dedicated to issue qualified signature certificates.
- The CA root certificate dedicated to issue certificates for electronic seals.
- The CA root certificate dedicated to issue time stamp certificates.
- Time Stamp Server certificates.
- Time Stamp Tokens.

1.2 Document Name and Identification

Name and version of this document are indicated on the front page of this document.

This document is public and freely downloadable from the Intesi Group web site (http://www.intesigroup.com/en/documents) and published on the AgID website (http://www.agid.gov.it).

1.3 PKI participants

Intesi Group is a Trust Service Provider that issues different types of certificates under this CPS. Intesi Group operates one or more Certification Authorities (CAs) which create and sign end entity digital certificates for electronic signatures, time stamps, electronic seals, according to EU eIDAS Regulation. Intesi Group uses various PKI services and its CAs are hosted in highly secured data centers. All equipment for running PKI services, including but not limited to CAs, OCSPs, RA servers, Server Signing Application (SSA as defined in [CEN/TS 419 241]), HSMs enjoy the same controls described in Section 5 and 6 for physical, personnel, procedural and technical security. The location and construction of the facility housing the CAs and equipment are consistent with facilities used to house high value, sensitive information.

1.3.1 Intesi Group as Time Stamping and Certification Authority

Intesi Group as QTSP acts as time stamping and certification authority and is fully identified as follows:

Company name: Intesi Group S.p.A.

Registered Office: Via Torino, 48 – 20123 Milano (MI) – ITALY

Legal representative: Paolo Sironi (Board of Directors)

VAT Reg. No. and Tax Code: IT02780480964

Telephone: +39 02 6760641

ISO Object Identifier (OID): 1.3.6.1.4.1.48990

Company web site: http://www.intesigroup.com

Company e-mail address: intesi@intesigroup.com

The Intesi Group PKI (Public Key Infrastructure) that issue qualified certificates is based upon a one-level hierarchy. The CA keys currently in use by Intesi Group and covered by this CPS are indicated with the following subjectDistinguishedName:

SubjectDistinguishedName	**Use**
CN=Intesi Group EU Qualified Electronic Signature CA G2, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Used for qualified certificates for electronic signature
CN=Intesi Group EU Qualified Electronic Seal CA G2, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Used for qualified electronic seal certificates
CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964,	Used for qualified certificates for timestamp

SubjectDistinguishedName	Use
O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT	

1.3.2 Local Registration Authority

A Local Registration Authority (RA) is a third party that operates on behalf of Intesi Group, after agreements stipulated with Intesi Group, to carry out:

- Identification and Authentication (I&A) of the subjects requiring qualified certificates.
- transmission to the QTSP of the identified subject information.
- registration of the applicant data and authorization to certificate issuance using tools made available by Intesi Group.
- validation and management of any suspension, unsuspension and revocation request.

Personal identification of Subjects applying for a certificate may take place at Intesi Group premises or at any of the LRAs used for this purpose. Personal identification of Subjects applying for a certificate may also be performed by mobile identification officers operating on behalf of Intesi Group.

LRAs are subject to periodical assessment by Intesi Group to verify the compliance with this CPS and to the agreements taken.

1.3.3 Subscribers or applicants

In this TSPPS subscribers and applicants are:

- Natural person holding the qualified certificate
- Natural person authorized to represent a legal person.
- Legal person.

1.3.4 Subjects

Subjects are:

- natural persons holding qualified electronic signature certificates.
- legal persons holding qualified seal certificates.

1.3.5 Holders

The holders are person using the private keys relating to a qualified signature certificate or qualified seal certificate. For qualified signature certificate is the subject, for qualified seal certificate is the person identified by the RAO and who has in use the credentials.

1.3.6 RAO (Registration Authority Officer)

RAOs are individuals involved in the process of identifying, collecting and recording personal data and responsible for the transmission of the documentation to the CA.

RAOs can be part of the QTSP or LRA staff and can operate after a mandate with the QTSP and only after having attended a training course.

At the end of the training course, operators are given access privileges to web applications made available by Intesi Group to carry out RAO activities. The assignment of the access privileges is under the control of the CA.

1.3.7 TA (Trusted Agent)

Trusted Agents are individuals involved in the process of identity proofing of Subscribers requesting qualified certificates for electronic signature, or qualified electronic seal certificates.

The TA collects and verifies each Subject's identity in support of the Subscriber registration. The TA works closely with RAO or LRA to support Subscribers registrations.

TAs can be part of the QTSP or LRA staff and can operate after a mandate with the QTSP and only after having attended a training course.

At the end of the training course, operators are given access privileges to web applications made available by Intesi Group to carry out TA activities. The assignment of the access privileges is under the control of the CA.

1.3.8 Relying parties or users

The "Relying Parties" are all the subjects that rely on the information contained in the certificates. They are all the subjects that verify electronic signatures and electronic seals through the certificates issued according to this TSPPS.

1.3.9 Other participants

The activities carried out by the Intesi Group as QTSP are under the supervision of AgID (Agenzia per l'Italia Digitale).

1.4 Certificate and Seals usage

The **policy** of qualified certificates for signatures and seals issued under this TSPPS are identified by the **OIDs** specified below.

Intesi OID	ETSI OID	AgID OID	Description
1.3.6.1.4.1.48990.1.1.1.1	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD for Remote Signature.
1.3.6.1.4.1.48990.1.1.1.2	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD for Remote Signature – Short term validity
1.3.6.1.4.1.48990.1.1.1.3	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD for Remote Signature - Customer user notice.

1.3.6.1.4.1.48990.1.1.1.4	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD.
1.3.6.1.4.1.48990.1.1.1.5	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD - Customer user notice.
1.3.6.1.4.1.48990.1.1.2.1	QCP-l-qscd	agIDcert	Qualified Certificates for Legal Seal with QSCD and Remote Signature eIDAS Policy
1.3.6.1.4.1.48990.1.1.2.2	QCP-l-qscd	agIDcert	Qualified Certificates for Legal Seal with QSCD and Remote Signature eIDAS Policy – Short term validity
1.3.6.1.4.1.48990.1.1.5.1	baseline-ts-policy	agIDcert	Qualified TSA

Where:

1. QCP-n-qscd è 0.4.0.194112.1.2 defined into the standard ETSI EN 319 411-2;
2. QCP-l-qscd è 0.4.0.194112.1.3 defined into the standard ETSI EN 319 411-2;
3. baseline-ts-policy è 0.4.0.2023.1.1 Best Practices Policy for Timestamp defined into the EN 319 421 and is included in the time stamps to claim conformance to it;
4. agIDcert 1.3.76.16.6 to indicate the adherence to AgID “Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate” (Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic seals and qualified electronic time stamps);

1.5 Policy Administration

This TSPPS is developed, reviewed and updated by Intesi Group authorized staff and is published only after being approved by the Intesi Group management.

For further information or explanations about this TSPPS, please write an e-mail to the following address: **tsp@intesigroup.com.**

1.6 Definition and Acronyms

Acronym	Definition
CA	Certification Authority
CAO	Certificate Authority Officer
TSPP	TSP Policy
TSPPS	TSP Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
QTSA	Qualified Time-Stamping Authority
PKI	Public Key Infrastructure
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	Tax Identification Number
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
TLS	Transport Layer Security
TSP	Trust Service Provider
TA	Trusted Agent

2 PUBLICATION AND REPOSITORY

2.1 Repository management

Intesi Group public repositories consist of the following websites:

- **http://www.intesigroup.com**
- **http://www.time4mind.com**

Intesi Group manages the repositories and is responsible for their maintenance and the publication and update of their content.

The repositories are available 24 hours a day, 7 days a week and are designed to guarantee 99.9% service levels (SLAs). In case of system failures or any events that can interrupt the service, Intesi Group will activate all the procedures aimed to restore the service as soon as possible.

2.2 Published information

On the Web repositories are published the following documents:

- the TSP Policy (TSPP), for all the provided trust services.
- the TSP Practice Statement (TSPPS).
- PKI Disclosure Statement (PDS)
- Terms & Conditions of the services.
- All CAs certificates
- CRL – Certificate revocation lists for all the CAs.
- Various forms.

2.3 Time and frequency of publications

The frequency of updating and publication of the documentation is established by Intesi Group's internal processes. The version valid is the latest version available on the certification service website (www.intesigroup.com) or, where applicable, the documentation published on the AgID website (www.agid.gov.it).

In case of inconsistency between the two versions, the version published on the AgID website is the valid one.

For the CRL issuance frequency refer to section 4.

2.4 Access control

Access to documentation and CRLs is free and does not require authentication.

3 IDENTIFICATION AND AUTHENTICATION

The I&A procedures followed by Intesi Group comply with ETSI EN 319411-1 requirement.

3.1 Naming

3.1.1 Types of names

All the qualified certificates issued by Intesi Group comply with EU eIDAS Regulation, the Italian laws and the profile specified in the applicable parts of ETSI EN 319 412, namely part 2 for certificates issued to natural persons, part 3 for legal persons, part 5 for qualified certificates.

All the TSU certificates issued by "Intesi Group Qualified Time-Stamp CA G2" comply with the profile specified in ETSI EN 319 412-3 and the requirements specified in ETSI EN 319 422.

Intesi Group generates and signs only certificates that contain a non-null subject Distinguish Name (DN) complying with the X.500 standard. Certificates may also include other name forms in the subject alternative name forms field.

3.1.2 Need for names to be meaningful

Unless pseudonyms are used, the names used under this TSPPS and the applicable TSPP shall be meaningful as identifying certificate Subjects (physical and legal persons) or TSUs.

Intesi Group will determine the subscriber's DN to make it compliant with common standards, practices and regulations requirements. The name should have commonly understood semantics (full name, company's name, Internet e-mail address) for the relying parties to determine identity

of the person and/or organization. However, the subscriber can choose a pseudonym instead of the real name in the qualified certificate. Intesi Group will issue such pseudonymized certificate.

3.1.3 Subject's anonymity

During a face-to-face identification (cfr.3.2.4, 3.2.5 e 3.2.6), or at the moment of certificate request, the subscriber may request the use of a pseudonym instead of personal data to be inserted in the subjectDistinguishedName's pseudonym field of the qualified certificate. The use of a pseudonym is clearly indicated by the usage of a dedicated field “PSEUDO”.

The use of the pseudonym is accepted only if:

- is unique and not assigned to any other subject identified for Intesi Group Trust Service Provider.
- the certificates are issued to a natural person.

Intesi Group records subject personal information associated with the pseudonym for twenty (20) years from the issuance of the certificate. This information is retained confidential and can never be disclosed to third parties unless foreseen by law.

The use of pseudonym does not apply to TSU and seal certificates.

3.1.4 Professional qualifications, role and organization

The certificate holder, independently or with the permission of a "Third Party", can require the insertion in the certificate of information on its qualifications, such as membership of professional colleges, the qualification of a public official, the possession of professional qualifications, information on powers of representation.

This information is inserted in the "title" attribute of the certificate's Subject field. In this case, the Applicant, in addition to the documentation and the required identification information, must also present documentation to demonstrate the possession of the specific role or professional qualification, also by using a self-certification in accordance with art. 46 del DPR n. 445/2000.

According to the CNIPA Resolution no. 45/2009, when the role is self-certified by the Applicant, no information on the applicant's organization it will be included in the certificate

In this case the QTSP assumes no responsibility for the inclusion of the role in the certificate, except in cases of intentional misconduct or negligence.

Information on the organization will instead be included in the certificate only if that organization has specifically requested or authorized the issue of the certificate, even without the explicit indication of a role. In this case, the QTSP carries out a check on the formal regularity of the documentation submitted by the Applicant.

3.1.5 Rules for interpreting names

Names respect X.500 standard.

3.1.6 Uniqueness of names

The full combination of the Subject Attributes (SubjectDistinguishedName) grants the uniqueness of the names. For certificates issued to a natural person the information granting the uniqueness are:

- the Givenname (OID 2.5.4.44) containing the subject's first name.
- the Surname (OID 2.5.4.44) containing the subject's surname.
- the SerialNumber (OID 2.5.4.44) containing the subject's tax identification number or alternatively a code taken from the identity document used for the identification process.

The same Subject may have different certificates, all bearing the same subject DN, but no two separate subjects may share a common DN and be issued by the same CA. To avoid conflict, Intesi Group add a unique registration number into the DNQualifier field of the subjectDistinguishedName.

When the subject uses a pseudonym the names uniqueness is guaranteed by the uniqueness of the pseudonym.

For certificates issued to a legal person the uniqueness is guaranteed by the combination of the fields:

- OrganizationName (OID 2.5.4.10) containing the full registered name of the subject (legal person).
- Organization Identifier (OID 2.5.4.97) containing an identification of the subject organization different from the organization name. This field is valued according to ETSI EN 319 412-1 [i.4].

For TSU certificates the uniqueness is granted by Intesi Group's internal procedures.

3.1.7 Recognition, authentication, and role of trademarks

The Subscribers must guarantee to operate in the full compliance with national and international intellectual property laws.

Intesi Group does not check the use of trademarks and may refuse to issue or force the revocation of certificates involved in a legal dispute. Intesi Group is not responsible for resolving name claim disputes among subscribers.

3.2 Initial Identity Proofing

Initial Identity proofing is part of the certificate application process described in chapter 4.1. Initial identity proofing procedures for natural or legal subjects are fully detailed in Intesi Group S.p.A. internal documents.

3.2.1 Proving possession of private key

The proof-of-possession of the private key corresponding to the requested certificate is based on the cryptographic verification of the CSR (Certificate Signing Request) sent to the CA. In fact, the applicant must send its own public key to the QTSP in the form of a CSR in PKCS#10 format [RFC2314]. The QTSP shall verify that the digital signature in the CSR is valid.

If Intesi Group generates within its premises the private key belonging to the qualified certificates of the Subject, then the proof of possession is not required.

3.2.2 Authentication of organization identity

The application for qualified certificate issued to a legal person (electronic seal) is done by a natural person representing the legal person and who is identified according to the same procedures used for natural persons (see par. 3.2.3).

The legal person's powers of attorney must be demonstrated providing to QTSP (or to TA or to RAO) appropriate documentation issued by an authoritative body such as, for example, an official certification issued by a chamber of commerce, a competent official register in which the organization is listed (or a comparable document) which proves the existence of the organization.

Governmental or administrative authorities must supply documents which reflect their relationship to the next higher entity (e.g. a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer.

The documentation must include:

- full name and legal status of the associated legal person or other organizational entity,
- relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.

3.2.3 Identification and authentication requirements for an individual

Intesi Group supports all mechanisms for identity verification, as defined by EU eIDAS Regulation, art.24 requiring that the identity and any specific attributes of the natural or legal person to whom the qualified certificate is issued is verified by Intesi Group either directly or by relying on a third party in accordance with national law:

a. by the physical presence of the natural person or of an authorized representative of the legal person; or

b. remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 of eIDAS regulation with regard to the assurance levels 'substantial' or 'high'; or

c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

d. by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

The identity of an individual may be established by in-person proofing before a RAO or TA, or remotely verifying information provided by the individual and confirms that: Full name, Date of Birth (DoB), Place of Birth, address and other personal information in records are consistent with the application and sufficient to identity a unique individual.

The identification process is performed by the RAOs (see 1.3.6), or TA, or LRA or by a public official (in accordance with the provisions governing their activities) which must operate according to EU eIDAS Regulation and to the identification procedures applied by Intesi Group:

- "Face-to-face identification" which happens with the meeting between a RAO or TA and the Subject.
- Identification and registration through the IDentify Web process
- Identification through customers procedures with an LRA mandate.
- Identification by anti-money laundering regulation

Intesi Group guarantees that every identification procedure applied adhere to article 24 of the (EU) regulation No. 910/2014 eIDAS and to corresponding ETSI standards.

In order to proof identity, the subscriber shall present an identification document. For Italian citizens are allowed the following identification documents:

- identity card;
- passport;
- boat license;
- pension booklet;
- license to operate on heating systems;
- gun license;
- Other identification cards provided with a picture and a stamp and issued by an Italian public Administration are allowed.

For subscriber with citizenship of an EU countries the following identification documents:

- passport
- national identity card.

For citizens with non-EU citizenship:

- Passport

For Citizens with residence in the United States are also allowed:

- National Government-issued Picture ID that asserts the holder's identity (e.g. National ID card, Passport, Global Entry Card, PIV card or comparable), two Non-National Government IDs, one of which shall be a photo ID (e.g. Driver's License)[1].

[1] Examples of acceptable identity documents can be found at: https://www.fedidcard.gov/system/files/Acceptable%20Forms%20of%20ID%20Guide%20v1.2%2002262020%20%282%29%20%282%29_0.pdf

Any document presented shall bear an expiration date and must be unexpired

3.2.4 Face-to-face identification and registration

Identification is carried out by the RAO or TA and requires the physical presence of the subscriber which must present a valid, non-expired identification document. .

The identification documents shall contain:

- full name (including surname and given names),
- date of birth and place of birth,
- a serial number or other attributes which may be used to distinguish the person from others with the same name.

It is also permitted to check the identity of the applicant indirectly using means which provide equivalent assurance to physical presence (for example if the applicant already possesses a qualified certificate, which implies that the applicant has been identified with personal presence).

If the subscriber is requesting:

- a qualified certificate for electronic seal.
- a certificate at the request of a third party.
- the inclusion of professional qualifications, role and organization.

He/she must present documentation to demonstrate the authorization to request the certificate or to use the qualifications required.

RAO checks document validity. If the verification is successfully executed, the Identification officer completes the procedure doing:

- Registration of the subscriber's personal data through the Intesi Group RAO portal. A detailed list of the information entered is shown in section 4.2.1.
- Digitization of a copy of the identification documents presented.

- Printing a copy of the contract with terms and conditions.

The RAO must keep the signed copy which will deliver to Intesi Group and must sent the digital copies to Intesi Group through the RAO portal. Intesi Group will keep digital and paper copies according to the Italian regulation.

The information recorded for the issuance of each certificate is set forth below:

- The identity of the RAO, LRA or TA.
- A signed declaration by the RAO or TA that he or she has verified the identity of the applicant.
- The date and time of the verification.
- A declaration of the identity signed by the applicant using a handwritten signature or appropriate electronic signature.

If the subscriber provides incomplete information, invalid or missing identification documents or does not sign a copy of the contract, the RAO will not be able to approve the issue of the signature or seal certificate.

3.2.5 Identification through LRA process

Intesi Group can accept methods of identification different from those established by its own processes and adopted by customers authorized to perform RA activities after having carefully verified that the procedure is adequate and conforms to the procedure defined by EU eIDAS Regulation, by AgID and from this TSPPS.

3.2.6 Identification and registration through IDentify Web

This identification method is carried out by a RAO operator using a videoconference call, named Identify Web, with the Subscriber. The video conferencing system used is made available by Intesi Group which will provide the Subscriber with all the necessary instructions to access it.

The subscriber shall own a device (PC, Smartphone or Tablet) equipped with a webcam and an audio system.

At a previously pre-established date the Subscriber and the RAO connect to IDentify Web and start the Identification. The RAO will follow a procedure, kept confidential for security reasons, aimed at verifying the actual presence of the subject and aimed at verifying the authenticity of the documents presented.

The RAO verify the identity of the Subscriber through the verification of one or more valid identification documents among those already listed in par. 3.2.4.

The RAO can consider not admissible a document presented by the Subscriber if the document is not valid (expired or issued by an invalid public body) or suspect it is not authentic.

Furthermore, the RAO may not start or interrupt the identification process if the audio and video quality is poor or not adequate to meet the requirements of Article 32 paragraph 3, letter a) of the Italian “Codice Amministrazione Digitale” (Digital Administration Code).

At the starting of the video conference, the user will always be asked to:

1. Accept the privacy policy.

2. Accept the service terms and conditions.

Both documents are downloadable from the Intesi Group website and are sent to the user by email before the video conference session starts.

Without the acceptance, the video conference and the identification process are interrupted by the RAO.

At the end of the videoconference, if the RAO deems the recognition process successful, it will approve the certificate issuance otherwise it will reject the request informing the user.

The recording data, consisting of the audio-video file and metadata structured in electronic format, are stored securely according to the art. 32, paragraph 3, letter j) of the Italian "Codice Amministrazione Digitale" (Digital Administration Code).

3.2.7 Identification and registration through qualified signature verification

A user can be identified by means of a qualified digital signature verification applied on the certificate request form. For this kind of identification, a user must:

1. Fill the request form with its personal data and digitally sign it using its qualified certificate.
2. Send it to Intesi Group using one of the Intesi Group's available encrypted communication channel.

On document reception, Intesi Group verifies the signature validity and verifies that the data contained into the qualified certificate used to sign the document match with the data contained into the certificate request form.

In case of positive verification, the certificate request will be accepted, and the certificate issuance will be approved. Otherwise the certificate request will be reject informing the user with a suitable message.

Intesi Group will safely keep a copy of the request form for twenty years as required by the Italian legislation.

3.2.8 Identification by anti-money laundering regulation

The identification procedure is carried out by credit and financial institutions who are required to correctly and adequately identify their customers according with the anti-money laundering regulation in application of Directive 2005/60/EC.

With specific reference to Italy, data used for recognition are supplied by the Applicant in accordance with Italian Legislative Decree 231/2007 and subsequent amendments, under which

the Applicant must provide, under its own responsibility, all the necessary data to enable the credit and financial institutions to fulfil their obligations to identify their clients.

The information provided can be directly used for the certificate issuance but only after the subject (the Applicant) has:

- accepted the contractual conditions for the certificate issuance.
- confirmed the accuracy if the registered personal data.

The credit or financial institutions acquire the data according to their procedures defined in compliance with the applicable anti-money laundering regulations. For this identifier method, the credit or financial institutions must operate as Local Registration Authority (LRA) and sign an agreement with Intesi Group, comply with this TSPPS and follow the instructions supplied by the Intesi Group as QTSP.

3.2.9 Unverified information

Some information required for the activation and management of the account, such as the e-mail address or the mobile phone number, are not verified by the QTSP which is not responsible when the information provided are wrong. Information that is not verified shall not be included in the certificates.

3.3 Identification and Authentication for Re-Key Requests

Re-key requests are not available for any certificate issued by Intesi Group CA.

3.4 Identification and Authentication for Revocation Requests

The methods for identification and authentication of the certificate suspension or certificate revocation requests are performed by logging in to the portal using the username and password supplied after the first registration.

If the user does not remember or has lost the authentication information, he can submit a revocation request to an enabled authorized RAO or TA, or to the Intesi Group support as described in paragraph 4.9.

The revocation of TSU certificate shall be authorized by the Security Officer according to the procedure described in 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate request

The request for a qualified certificate issued to a natural person can be submitted by the subject (see 1.3.4) by making a request to the QTSP or to an authorized LRA and may also include a "third party", i.e. a subject who allows the insertion of a role in the certificate or an organization that authorizes the issuing of the certificate (see Del. CNIPA No. 45/2009).

The request for a qualified certificate issued to a legal person may be requested by a natural person who is authorized to represent the legal person (see 1.3.3) by submitting the application to the QTSP or to an authorized LRA.

Finally, the certificate for time stamps (TSU) can only be requested by Intesi Group internal staff as part of the key ceremony of the keys.

4.1.2 Enrolment process and responsibilities

The registration process must be carried out after the identification process (see par.3) and includes the following steps:

- registration of personal data;

- acquisition of the signed contract with terms and conditions;
- sending the collected information to the Intesi Group;

The registration process requires the following different steps:

- the Subscriber shall:
  1. read and accept the privacy policy;
  2. provide the required data for registration and present the require documentation for the identity proofing;
  3. sign a copy of the contract with Terms and Conditions;
  4. read and accept this TSPPS;
- the RAO or TA shall:
  1. identify the subscriber or subject;
  2. acquire the acceptance of privacy policy;
  3. register user data;
  4. send a copy of the Identification documents to the QTSP;
  5. approve the issuance of the qualified certificate;
- the QTSP shall:
  1. issues qualified certificates;
  2. stores the identification data and all the information collected during the registration process for the issuance of certificates;
  3. disseminates information on the certificates and seals status;

As indicated in the previous paragraphs the registration functions can also be performed by third parties (LRA) based on agreements with Intesi Group.

4.2 Application processing

The procedure for issuing certificates to natural and legal person takes place through the following steps:

- The RAO performs the identification process described in 3.2;
- The subscriber must:
    1. read and accept the Intesi Group's privacy policy;
    2. read and accept the contract and the Terms and Conditions;
    3. read this TSPPS;
- The RAO, through Intesi Group's RAO portal, register user personal data and send to the QTSP copies of the documentation collected during the Identification. The RAO then can approve or deny the certificate request.
- The QTSP, having received and validated the documentation, communicates to the user (e.g. through and e-mail) the request approval and the procedure to issue the certificate.
- The subscriber, using the credentials provided with the procedure described in par. 4.2.2.1, must authenticate to the Intesi Group Web portal or Mobile App and execute the issuing procedure following the steps proposed (described in section 4.3). The holder, through the features provided by the portal will perform:
    1. The definition of the credential access PIN and the customization of the OTP token (where present).
    2. The generation of the keys on the QSCD device and the issuance of the certificate on the PKI Intesi Group. The communication between QSCD and PKI takes place within the Intesi Group infrastructure or by means of a VPN between the Intesi Group infrastructure and the Intesi Group Customer's infrastructure. The communication is always secured using the TLS protocol and the mutual authentication of the components by means of SSL certificates.

The procedure for issuing TSA certificates is described in the internal procedures of Intesi Group.

4.2.1 Subject information required

To request a qualified certificate the subject or the subscriber must provide the following mandatory information:

- Name and surname;
- Birth date, birth city, birth state and birth country;
- Country of residence;
- mobile phone number;
- email address;
- Tax Identification or equivalent;

If the subscriber represents a legal person must also provide

- organization name;
- organization tax code;
- organization address (country, state, city, address);
- organization email and organization phone number;

4.2.2 Registration and authentication

User data registration is performed at the end of the identification process described in paragraph 3.2 and is responsibility of the RAOs.

Intesi Group provides a web application called pkra that allows RAO to execute the registration process through the following steps:

1. After successful authentication, the RAO must select the certificate profile to be authorized for issuance.
2. Then the web application presents a form that the RAO must fill in with the data provided by the applicant.

3. At the completion, the application requires the acquisition of the digitized images of the identification documents. For this purpose, the operator must use a mobile App developed by Intesi Group (called Identify) and so he must be equipped of a smart device (mobile phone or tablet).
4. The data collected are digitally signed by the RAO and then sent to the CA's servers. The signature is applied by means of a remote signature credential provided to the RAO after having received the RAO mandate and after the stipulation of the contractual agreements.
5. The QTSP server automatically checks the data received and, if they result complete and correct, saves them on the internal repository where they will be stored in accordance with the requirements of the current legislation.
6. The RAO can now complete the registration defining, where applicable, the type of OTP token to be associated with the credential of the applicant. Finally, the RAO can approve the issuance of the certificate.

For LRAs that have their own identification processes approved by Intesi Group, the steps described above can be performed automatically using specific WebServices exposed by the Intesi Group Time4mind portal.

The completion of the registration is confirmed to the applicant by sending an email containing:

- A unique code called "security code" that will be required to start the procedure for issuing the qualified certificates for signature or seal.
- A link that automatically starts the issuance of the certificate.

After the email reception, the user can execute the certificate issue procedure.

4.2.2.1 Subject authentication credentials

To issue a certificate, the holder must authenticate to the Intesi Group's user portal (reachable at the URL https://user.time4mind.com) using basic credentials.

The basic credential can be provided directly by the RAO during the identification or it can be generated directly by the requestor by filling out the "Registration" tab of the authentication form of the time4mind portal.

The registration request to the Time4Mind portal is notified to the user through an e-mail containing a link that the user must click to confirm the registration request.

The basic credentials are not enough to start the certificate issuance process because for this it is necessary that the user also insert the security code received at the end of the registration.

4.2.2.2 RAO authentication credentials

Every RAO must have basic credentials enabled to access the PkRA portal and must be provided with remote signing credentials to perform the registration procedure.

The generation of RAOs credentials is carried out by allowed Intesi Group staff and is executed following procedures defined by Intesi Group.

4.2.2.3 LRA authentication credentials

Intesi Group's customers authorized to do LRA Identification by means of their processes can do the registration using webservices exposed by the Time4Mind portal.

Communication between LRA client and Intesi Group server is protected by a secure TLS channel and requires:

- a certificate authentication to get access to services.
- a remote signature credential to sign the documentation sent.

Authentication and signature certificates are generated and distributed by Intesi Group staff following the procedures for the assignment of LRAs defined by Intesi Group.

4.3 Certificate Issuance

4.3.1 Qualified certificate issuance for remote signature

Users requesting remote signature must verify to have the required tools to generate OTP tokens. In particular:

- Users who use SMS tokens must ensure to have the mobile device associated with the phone number provided during the identification.
- Users who use physical OTP tokens must be sure to have the OTP provided by the RAO upon registration.
- Users who use OTP tokens generated by the Mobile Valid App, before starting the certificate issuance procedure must be sure that the App is installed on their mobile device. The App is freely downloadable from the Google Play Store for Android devices and from the Apple App Store for iOS devices.

The certificate issuance procedure can be performed through the Intesi Group Time4Mind portal or directly from the Valid mobile app.

To start the certificate issuance procedure through the user portal of Time4Mind the user must log in to the portal using its basic credentials and select the menu item "Enroll Certificate".

Then, the user must select the credential to be issued and enter the "security code" received via e-mail to complete the authentication phase.

Alternatively, the user can skip these steps by clicking on the link received with the confirmation email. In both cases, if the authentication completes successfully, the procedure to generate the signing credential can be started. At this point, depending on the type of certificate to be issued and the type of token associated, the procedure will continue in different ways.

For automatic signature certificates it is necessary to define a PIN that, combined with the alias automatically generated and displayed to the user, will constitute the authentication credential.

For remote signature certificates using OTP SMS, in addition to the PIN is required to enter the OTP that the procedure automatically send to the phone number provided during the identification. In this case the combination of alias, PIN and OTP SMS will be the credentials to unlock the signing credential.

For remote signature certificates using physical OTP, in addition to the PIN is required to enter the OTP generated by the device provided by the RAO. In this case the combination of alias, PIN and OTP are the credentials to unlock the signing credential.

Finally, for remote signature certificates coupled with OTP tokens generated by App Valid for which the procedure, once started, will continue within the App. The App will require only the definition of a PIN and then autonomously and in safety mode will start the certificate issuance procedure by communicating with the Time4Mind portal.

Upon receipt of the information, the Time4Mind server starts the key pair generation process on the QSCD device and receive a certificate request in PKCS#10 format in response. This request is then sent to the internal certificate generation system (PKI) which will validate the request and will issue an X.509 certificate.

The certificate generated will be returned to the caller who will save it on the QSCD device coupled with the private key completing the signing credential.

The certificate issuance process completes by sending a confirmation message to the holder containing a revocation code that can be used to send a request for revocation or suspension to Intesi Group customer care.

A copy of the confirmation email can be sent to the third party if it is present.

Intesi Group verifies the accuracy and validity of all necessary data for the issuance of a qualified certificate, according to EU eIDAS Regulation and corresponding ETSI standards. Intesi Group will either issue the subscriber’s certificate upon successful completion of the process above, or will inform the subscriber about any problems or inconsistencies.

4.3.1.1 Shot-term certificates

For short-term cloud-based certificates, the identification process, the credential issuance and the document signature take place at the same time. The credential is issued, and a document is signed only after the user inserts an OTP code received via SMS or email on the telephone number provided during identification. Upon signature completion, the private key and the qualified certificate are deleted.

In some cases, the issuing and signing process can be carried out again for a period not exceeding 30 days after the identification date and only if the following conditions are met:

1. The user has not changed the telephone number provided during identification.
2. The certificates issued will always have the same subjectDistinguishedName.

4.3.2 Qualified certificate issuance on QSCD device

For qualified certificates issued on QSCD, Intesi Group will supply directly or through selected suppliers, only devices that are approved and published on the Compilation of Member States SSCDs and QSCDs list, available here: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

The QSCD customization process is carried out using software developed by Intesi Group includes a check on the serial code to verify its presence in QSCD certified devices list. If the device is not included in these lists, the personalization process is interrupted.

Users requesting qualified certificate on a QSCD device (smartcard or USB token) must first install on their PC the required software to handle the device and issue the qualified certificate. Information on where to download the software package and the installation instructions will be provided by the QTSP or RAO or TA at the end of the identification process. The procedure for customizing the signature token and issuing the certificate is done through the following steps:

1. The user must insert the QSCD device into the smartcard reader or in the USB port of its PC and then start the software to manage the QSCD device.

2. The user must then start the personalization procedure of his / her signature token by selecting the appropriate menu. At the beginning of the procedure the user will be asked to enter the authentication credentials and the "security code" that he / she has received after the identification procedure.
3. The user authentication starts the key pair generation, inside the QSCD device, and the PkCS#10 certificate request generation. The PkCS#10 certificate request and the authentication credentials are sent to the QTSP through a secure channel protected by the TLS (Transport Layer Security) protocol.
4. Upon receipt of the request, Intesi Group will verify the accuracy and validity of all the necessary data for the issuance of a qualified certificate according to the (EU) eIDAS Regulation and the corresponding ETSI standards.
5. If the verification process successfully completes, Intesi Group will issue the certificate that will return to the caller. In case of unsuccessfully verification Intesi Group will return an error message containing problems or inconsistencies that have caused the rejection.
6. Upon receipt of the certificate, the client software will install the certificate into the signature token completing the customization procedure.

The certificate issuing process is completed sending to the subscriber a confirmation message containing a revocation code that he / she can uses for a certificate revocation or suspension request.

4.3.3 TSA certificate issuance

The certificate request is manually executed by two TSP operators as follows:

- The first TSP operator using the timestamping software feature used by Intesi Group, generates the key pair on the HSM partition dedicated to the time stamp keys and generates the certificate request in PKCS # 10 format. The request is saved on a physical device (e.g. a Pen Drive) that is passed to a second TSP operator.
- The second TSP operator, after having received the physical support, proceeds with the issuance of the certificate by operating on the Intesi Group PKI administration

panel. The generated certificate is saved on the same physical device that returns to the first TSP operator.

- The first TSP operator, operating on the timestamping software, will proceed with the installation of the certificate on the HSM and with the activation of the time stamp service

The process is performed under the supervision of the TSA Officer.

4.4 Certificate Acceptance

4.4.1 Certificate acceptance

4.4.1.1 Subscriber Certificate acceptance

On receiving a certificate, the subscriber is committed to check its contents. If the certificate has any faults that cannot be accepted by the subscriber, the subscriber must inform Intesi Group without any delay. Intesi Group will then revoke the certificate and take the appropriate measures to reissue a new certificate.

If a certificate is not rejected within 7 day of the reception of the certificate, the certificate is considered accepted.

4.4.1.2 TSA Certificate acceptance

In case of erroneous certificates, the TSA Officer will request the security officer authorization to revoke the certificate according to the described procedure in 4.8.

4.4.2 Publication of the certificate by the QTSP

Qualified certificates are made available for retrieval from Intesi Group's certificate repository by third parties only if the subscriber has declared his /her consent. Without the subscriber consent the certificate is stored into the QTSP internal database and is not public available.

4.4.3 Notification of Certificate issuance by the QTSP to other entities

An e-mail containing a confirmation message is sent to the holder and, if requested, to the interested third party. No notification is sent for TSA certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

4.5.1.1 Keys and certificates of digital signature and seal

The holder must:

- be the sole user of the private key.
- maintain exclusively the knowledge of the authentication data (PIN, PUK and/or OTP), keeping them with the maximum diligence.
- keep the OTP device with the maximum diligence.
- use credentials respecting any user notice contained in the certificate.
- refrain from using improper or fraudulent keys and certificates in its possession.
- inform Intesi Group of any changes to the data not included in the certificate but communicated during the registration process.
- request the revocation of the certificate if there is reason to believe that the authentication data (e.g. PIN code) have been compromised.
- ask for the revocation of the certificate if the data contained in it are changed or incorrect.

4.5.1.2 Keys and certificates for TSU

TSU keys and certificates are generated and issued internally by authorized personnel and following Intesi Group's internal procedures. The keys and certificates are used only for generating time stamps (see rfc3161). Each private key is used for a maximum of 3 months after which it is destroyed in the presence of a TSA officer.

4.5.2 Relying Party public key and Certificate usage

Who rely on the information contained in the certificates (see 1.3.7) must verify that the certificate has not been expired, suspended or revoked. The validity can be verified using the CRLs or the OCSP service referenced in the CRLDistributionPoints and AuthorityInformationAccess extensions of the certificate.

The verification must consider the certificate status at the relevant date and time based on the context. The current date and time, if there is no way of knowing when the signature was generated, or the date and time when the signature was generated if is demonstrable by a time stamp included in the signed document.

Users can avoid the above checks only in the case of a "verified signature" certificate, according to the AgID Determination n. 63/2014; this kind of certificates can be detected analyzing the OID contained into CertificatePolicies extension. For more details on users' obligations, please refer to par 8.

4.5.3 User notice

Qualified certificates for server-side signature contains the user limit set by the Italian Conformity Assessment Body – Agid - as additional Certificate Policy:

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

Conforming to the Italian regulation, the Subscriber can also request to the Certification Authority the inclusion into the certificate of one of the following user notices:

I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato.	The certificate holder must use the certificate only for the purposes for which it is issued.
L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto).	The certificate may be used only for relations with the (declare the subject).

Furthermore, the Subscriber can also request the inclusion of custom user notice which must be evaluated by the CA.

The subscriber can also request limitation on the value of transaction for which a certificate can be used and is responsible to verify the compliance with the limits of use inserted into the certificate. The QTSP is not responsible for damage caused using a certificate that does not comply with the user notice contained into the certificate itself.

4.6 Certificate Renewal

A certificate renew can be executed by the subscriber only if the certificate is not yet expired and only within the ninety days before the certificate expiration and always includes a new key pair generation.

The TSA certificate renewal procedure is executed every three months by a TSP Operator under TSP Officer supervision following TSP internal procedure.

4.6.1 Procedure to process renewal request

The Holder can start the procedure from its Valid Mobile App or from the Intesi Group portal and only after having:

1. done a successfully login using basic authentication credentials.
2. Signed, with the expiring certificate, the contract with terms and conditions.
3. defined a pin to use as certificate access PIN.

After obtaining this information, the QTSP generates a new key pair and a new certificate using the same procedure used for the first generation (see 4.3).

The TSU certificate renewal procedure is executed by two TSP operators who can generate a new key pair and issue a new certificate. The renewal of TSU keys is carried out following a specific

internal procedure and is recorded on a KeyCeremony document which must be approved by the TSP Officer and which is kept for a period of 20 years.

4.6.2 Notification to the subscriber

The notifications sent to the holder are:

- Ninety days before the expiration, the server sends to the subject an e-mail containing a reminder about the certificate expiration and the instructions on how to proceed with the certificate renewal.
- After the certificate renewal process is completed, a confirmation message containing a revocation code that will be required to revoke or suspend the certificate. When present a copy of the message is sent to the third party.
- If the user left expires its certificates, it will receive an email informing about the certificate expiration and the instruction on how to apply for a new certificate.

4.6.3 Certificate acceptance

Refer to section 4.4.1.

4.6.4 Publication of the certificate by the CA

Refer to section 4.4.2.

4.6.5 Notification of Certificate issuance by the QTSP to other entities

Refer to section 4.4.3.

4.7 Certificate Re-key

Certificate re-key is not allowed by Intesi Group qualified CA.

4.8 Certificate Modification

The certificate modification is not allowed by Intesi Group qualified CA. To modify a certificate a user must revoke the certificate to be modified and issue a new certificate following the procedure described in section 4.9 and 4.3.

4.9 Certificate Revocation and suspension

4.9.1 Circumstances for revocation

The circumstances to request a certificate revocation are those provided by the regulations and by the TSPP. A certificate shall be revoked when the binding between the Subject (holder) and the Subject's Public Key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Subject can be shown to have violated the stipulation of its respective Subscriber Agreement, or the stipulations of this CPS.
- Subscriber or another authorized agent asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL. Revoked certificates are published on all new publications of the certificate status information.

If a private key used to approve requests for one or more certificates may have been compromised, all certificates authorized since the date of actual or suspected compromise and directly or indirectly chaining back to that private key will be either revoked or be verified to be appropriately issued.

4.9.2 Who can request revocation

The certificate may be revoked on request of:

1. The certificate holder.
2. Third party, when present
3. The “certification authority”.

For certificates that bind an organizational affiliation, Intesi Group accepts revocation requests from the designated organization’s Contact Point. The organization shall inform Intesi Group of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a subject (holder), Intesi Group will revoke any certificate issued to that subject containing the organization affiliation.

For TSU certificates, revocation can be required by TSP Operators after having informed and obtained approval from the TSP Security Officer.

4.9.3 Procedure for revocation request

The form and/or procedure to be used for applying for the suspension, un-suspension or revocation of a certificate can be obtained by the subject:

- from the Time4Mind user portal;
- making a request to a RAO;
- making a request to Intesi Group's customer care;

Applications and reports relating to a revocation are processed on receipt, are authenticated and are confirmed through the following process:

4.9.3.1 Revocation with Time4Mind portal

To revoke its certificates through the time4mind portal (https://user.time4mind.com) the holder must:

1. Successfully login to the Time4Mind user portal;

2. search for the certificate to be revoked from those listed by the application using the "Credential" menu;
3. invoke the “revocation” function and confirm the request.

The request is immediately taken in charge and executed as soon as possible. The result of the operation is shown on the user screen and confirmed with an email sent to the holder and, when applicable, to the third party.

4.9.3.2 Revocation by means of Intesi Group RAO

The Revocation of a certificate can be made by any RAO operator using the PkRA RAO in response to a request from:

- Certificate holder;
- Third party, when applicable;
- CA;

The holders and third parties who wish to request a certificate revocation to a RAO, must present the revocation form, downloadable from the Time4Mind portal, filled in all its parts and a copy of the identification document.

Using the supplied information, the RAO, by means of the PkRA web portal, can:

1. search the user;
2. Compare the data provided with those recorded in the portal to authenticate the applicant. if the RAO consider that the information is wrong or incomplete, it will proceed with the certificate suspension waiting for the applicant providing clarification or additional information.;
3. request the certificate revocation or the certificate suspension.

The request is immediately taken in charge and executed as soon as possible. The result of the operation is shown on the RAO screen and confirmed with an email sent to the holder and, when applicable, to the third party.

4.9.3.3 Customer care revocation

Only in case of unavailability of the Intesi Group revocation services users and RAOs can ask a revocation at the Intesi Group's customer care sending an email at the address

certificate@intesigroup.com

When the sender is a RAO, the email must be sent within eight hours of receipt of the revocation request of the subject.

Any email must contain a compiled copy of the revocation module including the revocation code or a digitized copy of the identification document. If the user cannot supply one of this last two, the certificate will be only suspended. The user then has ten days to proceed with the revocation or the un-suspension of the certificate. At the end of this period, if the user hasn't done any operation, the certificate will be automatically un-suspended.

Note, for security reason the sender email address must be the same of the email address supplied during the registration at the Time4Mind portal. Any email received from an unknown sender will be rejected.

Intesi Group operator verifies the correctness of the information supplied and proceeds with the suspension or revocation of the certificate.

A confirmation email of the certificate revocation or suspension is always sent to the holder and to the third party when defined.

4.9.3.4 TSA certificate revocation

According to clause 4.8 of the QTSP policy, the certificate revocation is executed by TSP Operator with the approval of the Security Officer following TSP Internal Procedure.

After the certificate revocation, the TSP operator will proceed with the deletion of the related private keys from the HSM.

4.9.4 Revocation request grace period

Intesi Group performs revocation on a best effort basis, to ensure that the time needed to process the revocation request and to publish the revocation status (updated CRL) is be as reduced as possible.

4.9.5 Time within which QTSP must process the revocation request

When the QTSP receives a revocation request, it tries to immediately executes the operation. Intesi Group shall process revocation requests within 24 hours of the receipt of the request. If the operation is successfully executed, the revoked certificate is inserted in the CRL within 6 hours of the revocation and in any case not later than 24 hours after the operation. If the revocation fails the status of the certificate is not changed and the holder, and the third party when applicable, are informed by an email.

4.9.6 Revocation checking requirement for Relying Parties

Refer to section 4.5.2.

4.9.7 CRL issuance frequency / OCSP response validity period

4.9.7.1 CRLs

The CRL is re-generated and re-published every 6 hours, even in the absence of new revocations. In some circumstances, the QTSP can force a new CRL issuance before of the 6h.

4.9.7.2 OCSP

OCSP service is available for certificate status validation. The fields “this update” and “next update” reflect the validity period of an OCSP (see section 7 of the TSPPS).

4.9.8 Maximum latency for CRLs

The time between the request for revocation or suspension and the confirmation with the issuance of a new CRL is at maximum six hours.

4.9.9 On-line revocation status checking availability

The QTSP makes available Certificate status checking services including CRLs and OCSP. See section 4.10 of this document.

4.9.10 Other forms of revocation advertisements available

Not available.

4.9.11 Special requirements regarding key compromise

Not available.

4.9.12 Circumstances for suspension

The certificate suspension can be executed under these circumstances:

1. the QTSP receive a revocation request without necessary information to authenticate the requester.
2. the owner, the subscriber or the certification authority acquire elements of doubt about the validity of the certificate;
3. there are doubts about the safety of the key storage device or the authentication system;
4. is required an interruption of the validity of the certificate.

The suspension for the TSU certificate is not available.

4.9.13 Who can request suspension

Who can request a certificate suspension is listed in paragraph 4.9.2 of this TSPPS.

4.9.14 Procedure for suspension and un-suspension requests

Tools and procedures available are the same used to invoke the revocation of certificates (see paragraph 4.9.3).

4.9.15 Limits on suspension period

The suspension has a period of ten days after that the certificate can be automatically revoked or un-suspended depending on the customer configuration.

4.10 Certificate Status Service

The status of the qualified certificates is made available through the publication of CRLs, in conformance to RFC 5280, via HTTP protocol [RFC7230] on the server **crl.time4mind.com**.

The status of the certificate is also available through a status checking service based on OCSP (On-line Certificate Status Protocol) in compliance with the specification [RFC2560].

The revocation services addresses are inserted into the certificates, the CRL address is inserted in the CRLDistributionPoints extension and the OCSP server address is inserted in the AuthorityInformationAccess extension.

The Certificate status services are public.

4.10.1 Service Availability

Access to the CRL and OCSP service is continuously available (24 x 7).

4.11 End of Subscription

The contract between the QTSP and the holder ends when the certificate expires or is revoked, unless there are different conditions that may be stipulated in contracts signed with customers.

4.12 Key Escrow and Recovery

The key recovery is available for CA and TSU keys in the case of unintentional cancellation or HSM fault. To allow key recovery, the QTSP keeps a backup of CA and TSU key pair and recovery is performed according to the HSM procedures and under dual operator control.

5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, operational, procedural, personnel and physical (non-technical security) controls that are used by Intesi Group S.p.A. with regards to its qualified service is compliant with the technical standards EN 319 411-1 for non-qualified certificate issuing, EN 319 411-2 for qualified certificate issuing EN 319 421 for timestamp issuing and Intesi Group ISO/IEC 27001 certified Information Security Management System.

Intesi Group information security policy as well as documentation on security controls and operating procedures are available in the security plan (Piano della Sicurezza) and other reserved documents that are available only to authorized Intesi Group personnel, to auditors and to the Italian Supervisory Body.

5.1 Physical security

Several layers of physical security controls restrict access to sensitive hardware and software systems used for performing critical CAs operations, which take place within a physically secure facility. These systems are physically separated from the organization's other systems so that only authorized employees can access them.

Physical access to the QTSP systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes access cards in combination with passwords for access. An audit log is maintained, listing all physical entries to restricted areas.

Private keys used for issuing certificates or signing certificate status responses are not vulnerable to physical penetration. These keys are stored in tamper-resistant secure signature creation devices which are confirmed to fulfill the requirements of the EU eIDAS Regulation and corresponding ETSI standards. The devices are protected from unauthorized access while installed and activated. Physical access controls are implemented to reduce the risk of device tampering even when is not installed and activated. Regular security checks are made to ensure that all these controls function properly. Access to any physical area where information or equipment sensitive to QTSP operations is located is restricted and monitored by the integrated alarm system.

All computer systems used for the provision of the qualified trust services herein described are housed in the Intesi Group data centers that guarantee:

- a **physical access control** system, so that access to the building is only possible to authorized personnel;
- access to the TSP services is only possible for authorized personnel holding a personal badge and the corresponding PIN;
- a video surveillance
- a **fire protection system** including **smoke detection** (VEWASD) **and** dedicated extinguishing system;
- a **power supply system** fully redundant at all levels (transformers, power centers, generators, UPS's, distribution panels, etc.)
- an **air conditioning** system (HVAC) which guarantees optimal working conditions;
- redundant **Internet connectivity**, with a capacity of at least twice the minimum necessary.

5.2 Procedural controls

Intesi Group S.p.A. carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the

full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is part of the reserved documentation. Appropriate systems, infrastructures and measures for quality and information security management are implemented and maintained always. Any changes that would impact on the level of security provided must be approved by the Security Officer.

Development and testing facilities are physically separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective actions are executed. Users of QTSP systems are required to note and report observed or suspected security weaknesses and threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are always available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

Operational procedures are documented under the company's Quality Management System, certified in accordance with the ISO 9001 standard and into the QTSP operative procedures.

5.3 Personnel security controls

All members of the personnel staff that involved for the provision of the trust services are either employees of Intesi Group S.p.A. or authorized and qualified personnel. All members are subject to

personnel and management practices that Intesi Group follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and time stamping related technologies.

Personnel involved in the service development and management time stamp service have been adequately trained on the procedures and tools to be used during the various operational phases.

All personnel must have proper knowledge and experience related to QTSP operations and must have demonstrated security consciousness and awareness regarding its duties at Intesi Group. Periodic reviews occur to verify the continued trustworthiness of all personnel.

No unauthorized users have access to systems storing sensitive data. All systems storing such data are located inside a protected area. In addition, access to rooms inside the protected area is controlled by an access control system; access to systems is permitted to authorized persons only.

Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. All employees of the organization and, where relevant, third-party users receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. Intesi Group's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

The trusted roles assigned to personnel are defined in accordance with the ETSI EN 319 401 and are:

1. Security and RA Officer: responsible for the information security and the compliance with the company's security policy
2. TSP Operation Officer: responsible for the certification and validation service.

3. System Administrator: administers the systems of the TSP service.
4. System Operation Officer: responsible for technical and logistic services.
5. System Operator: reporting to the System Operation Officer manages the operation of the TSP systems.
6. System Auditor: verifies the compliance of the TSP services with regulatory requirements and standards. .
7. Registration Officer - individual authorized to request or approve certificates or certificate revocations. These individuals do not hold any other roles.

All staff has received a mandate through a letter of engagement.

5.4 Audit logging procedures

5.4.1 Type of events recorded

The main events relevant to the certification service operations are registered in electronic form. The events logged are:

- All events relating to the life-cycle of CA keys;
- All events relating to the identification operation.
- Logging systems events related to certificate life cycle operations including but not limited to:
  - Subject key generation;
  - Certificate issuance;
  - Certificate revocation;
  - Certificate suspension;
  - Publishing of a CRL;
- All other certification services are equipped with event logging systems that record events related to any operation performed.

- Physical access to the data center.
- Physical access to the QTSP server area.
- Logical access to the all TSP systems.
- Events related to the certificate life cycle.
- Events related to clock synchronization.
- Events related to the release and updating of software.

For each event, information about the type, date and time of occurrence is also logged. The time source used is the system clock that is kept aligned by a NTP service.

No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted. These provisions are implemented using the features of a secure B1 operating system requiring the simultaneous login of two persons.

5.4.2 Frequency of processing log

Audit logs are processed continuously and/or following any alarm or anomalous event. Audit logs are archived daily.

5.4.3 Retention period for audit log

Log files are kept for 20 years.

5.4.4 Protection of audit log

The archive system has a daemon that checks the consistency and the immutability of the stored log files. In case of inconsistencies fires an alarm to the monitoring system.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.4.5 Audit log backup procedures

Log files are backed up according to internal procedures.

5.4.6 Audit collection system (internal vs. external)

Audit systems are an integral part of the CA.

5.4.7 Notification to event-causing subject

If required, Intesi Group notifies the originator of the audit event.

5.4.8 Vulnerability assessment

Vulnerability assessment related to the audit log systems is part of the risk analysis carried out by Intesi Group S.p.A. and available as a separate internal and confidential document.

5.5 Record Archival

5.5.1 Type of records archived

The TSP keeps the following information related to the certificate issuing and management processes:

- Event logging;
- All the logging files of the systems involved in the QTSP service;
- Identifications data, digital copy of identification document and contract approval.

The archive system has a daemon that checks the consistency and the immutability of the stored log files. In case of inconsistencies fires an alarm to the monitoring system.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.5.2 Retention period for audit log

Archived records are kept for 20 years.

5.5.3 Protection of archive

The archive system has a daemon that checks the consistency and the immutability of the stored information. In case of inconsistencies fires an alarm to the monitoring system so that a "System Administrator" is immediately informed and can treat the problem according with Intesi Group internal procedures.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.5.4 Archive backup procedures

Ref. Paragraph 5.5.3.

5.5.5 Requirements for time-stamping of records

Intesi Group ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 is recorded obtained through NTP synchronization of all systems. NTP service grants the time accuracy within a few milliseconds of Coordinated Universal Time.

5.5.6 Procedure to obtain and verify archive information

Archives are only accessible to the Intesi Group's authorized personnel as described in internal documents. Records are retained only in electronic format.

The Certificate holder and third party, may access to records and other information related to the certificates by contacting Intesi Group writing an e-mail to the e-mail address defined in the paragraph 1.5.

5.6 Renewal of CA Key

The Key ceremony procedure in force shall be applied.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The applicable and appropriate incident and/or compromise reporting and handling procedures, disaster recovery procedures and Business Continuity Plan have been established and are available as a separate internal document.

All such procedures are compliant against ISO/IEC 27001 standard. All incident and/or compromise events are documented, and any associated records are archived as described in section 5.5 of the TSPPS.

5.7.2 Computing resources, software, and/or data are corrupted

Intesi Group S.p.A. establishes the necessary measures to ensure full and highly automated recovery of the certification services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27001 procedure.

Disaster recovery resources are established at sufficient distance from the original resources to avoid that a disaster would corrupt resources at both sites. Sufficiently fast communications are established between original and remote sites to ensure the alignment and data integrity. Secured communications infrastructures are established from both sites to the RAs, the Internet, the certificate revocation status and repository services.

Disaster recovery infrastructure and procedures are fully tested at least once a year with witnessing of at least one member of Intesi Group.

5.7.3 Entity private key compromise procedures

Compromise of the CA private key(s) implies immediate revocation of the certificate of the key(s) compromised. The QTSP will additionally take the following measures:

- stop the affected qualified services.
- revoke all certificates that became unreliable because of the event;
- immediately publish the CRL with revocation information;
- Notifies customers and end users of the key compromise.
- Informs the Conformity Assessment Body.

Only after having assessed the reasons of the problem and put in place all the necessary measures for the resolution, Intesi Group will generate a new key pair and new CA certificate that will send to AgID which will insert it into the TSL. After the TSL publication Intesi Group will proceed with the reactivation of the qualified service.

5.7.4 Business continuity capabilities after disaster

Intesi Group S.p.A. establishes the necessary measures to ensure full and highly automated recovery of the time Certification Authority in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27001 standard. A Contingency Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.8 CA termination

In case of termination the TSP will take any measure necessary to minimize disruption to the certificate holders and relying parties; the TSP shall:

- at least 60 days before termination inform all customers and certificate holders;
- publish a notice on its website;
- terminate all contracts with any subcontractor;
- before the effective date of termination, transfer to another TSP the registration information, the certificate status information and all the relevant logs; If it is not possible to identify a TSP, all the data will be sent to AgID

- at the date of termination, destroy its private CA and TSU keys unless the service is taken over by another TSP; any issued certificates that have not expired will be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the latest CRL has been issued, the private signing key(s) of the CA will be destroyed.

6 TECHNICAL SECURITY CONTROLS

The security measures taken by Intesi Group S.p.A. with regards to its CAs to protect CAs cryptographic key and activation data, the constraints on repositories, subject CAs, and other PKI Participants, to protect their Private Keys, activation data for their Private Keys, and critical security parameters, ensuring secure key management, and other technical security controls used by Intesi Group S.p.A. to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, archiving, and other technical security controls on PKI Participants are compliant with the following technical standards:

- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI EN 319 421

These controls are further described and ruled by the following sub-sections.

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

6.1.1.1 Root CA

The CA generation procedure is executed by two Intesi Group operators following the Intesi Group's Key Ceremony procedure. Execution of the key generation procedure (or “key ceremony”) is recorded by Intesi Groups’ internal auditor and is kept for 20 years.

The key pair used by the Root CA is generated inside a high quality HSMs (Hardware Security Module) located into the Intesi Group data center in a controlled access area. The HSMs used are certified in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.1.2 Subject Certificate

The subject's key pair is generated:

- on a QSCD certified device located into the Intesi Group data center or located in the Intesi Group's customers data center and is recorded by the internal auditing system.
- on a QSCD certified device (SmartCard or USB device) owned by the subject.

6.1.1.3 TSU Certificate

Generation of the TSU key pair takes place in a physically secured environment, according to the Time-Stamp internal procedures.

Execution of the key generation procedure is recorded by Intesi Groups’ internal auditor.

The key pair used by the time-stamp to sign the TimeStampToken is generated inside a high quality HSM (Hardware Security Module) located into the Intesi Group data center in a controlled access area. The HSMs used are certified in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.2 Private key delivery to holder

Private keys are securely generated and stored into a QSCD device located into the Intesi Groups' server room or in the Intesi Group's customers server room. Access to the private key takes place only by means of the interfaces provided by the QSCD device and only after having executed a successful authentication.

6.1.3 Public key delivery to certificate issuer

The public keys are sent to the certification service in form of a PKCS#10 request over an HTTP channel protected by a TLS v 1.2 protocol. Every RA must authenticate to the QTSP service by means of a client certificate.

6.1.4 CA public key delivery to Relying Parties

The Root CA public keys are distributed by means of the publication on the QTSP web portal (www.intesigroup.com) and distributed through the Trust-service Status List (TSL) issued and maintained by AgID.

6.1.5 Key sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

The Root CA keys are generated with RSA algorithm and are 4096 bits length.

The Subject and TSU keys are generated with RSA algorithm and are 2048 bits length.

No certificates, CRLs or OCSP responses will be signed using RSA 2048 bit that extend beyond 12/31/2030. Also, all certificates issued for 2048 bit RSA keys will expire by 12/31/2030, otherwise will be revoked.

6.1.6 Public key parameters generation and quality checking

The algorithms and parameters used by Intesi Group for key pairs generation for qualified certificates and seals comply with eIDAS Regulation and Italian Regulations.

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

6.1.7.1 Root CA

The root certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- keyCertSign (sign certificates)
- cRLSign (sign CRLs)

For further details see chapter 7.

6.1.7.2 Qualified and Seal certificates

The qualified certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- Non-repudiation

For further details see chapter 7.

6.1.7.3 TSU

The TSU certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- Digital Signature

The TSU certificate also contains the extended key usage extensions:

- Timestamping.

For further details see chapter 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Intesi Group ensures the secure management of the CA private keys used for issuing qualified certificates and the private keys used for signing revocation status information (CRL, OCSP) and prevents the private keys disclosure, copy, deletion, modification and unauthorized usage. The CA private keys are stored at a physically secure location, in a secure Hardware Security Modules (HSM).

The private keys used by the Root CA is kept inside a high quality HSM (Hardware Security Module) with security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

The private keys used by the qualified certificates, seals are generated and kept inside a QSCD (Qualified Electronic Signature Creation Device) certified device.

6.2.2 Private key (n out of m) multi-person control

Access to devices containing CA and TSU private keys is available with two operators authenticated simultaneously. No single person has all the activation data needed for accessing any of the private CA keys.

Access to the private keys related to certificates qualified for digital signature and for seal can be executed only by the holder using the authentication credential that he defined during the certificate issuance and only through the interfaces of the QSCD device.

6.2.3 Private key escrow

Key escrow is never allowed.

6.2.4 Private key backup

For guaranteeing continuity of service, the QTSP keeps an encrypted backup copy of CA and TSU keys on removable media. The backup copy is kept in a safe place in a different location of the operational copy (inside the HSM). Backup and restore procedures require the joint intervention of at least two people (“dual control”).

Subscriber’s key back-up and key recovery are not allowed except for the purpose of disaster recovery as stated by this TSPPS and the applicable TSPP.

6.2.5 Private key archival

Not applicable.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

The private keys are generated and stored in a hardened and tamper-resistant protected area of the cryptographic module managed by the Certification Authority.

6.2.8 Method of activating private key

CA's private keys and TSU's private keys are activated using the procedures established by the HSM supplier and are consistent with the security certification. Activation always occur under the dual control of two TSP operators.

The private keys related to the signature certificate and the private keys relating to the seal certificate can only be activated by the holder using the authentication credentials defined during the certificate issuance (see section 4.2) and in accordance with the procedure provided by the provider of the QSCD device.

6.2.9 Method of deactivating private key

CA's private keys and TSU's private keys are deactivated using the procedures established by the HSM supplier and are consistent with the security certification. Deactivation always occur under the dual control of two TSP operators.

The private keys related to the signature certificate and the private keys relating to the seal certificate can only be deactivated by the holder closing the working session opened with the authentication, according with the procedures established by the QSCD.

6.2.10 Method of destroying private key

The CA and TSU keys are destroyed through secure deletion from the primary and backup media removing permanently any keys were stored on. The CA key destruction is performed following and internal procedure and is executed under dual control of two authorized operators.

Signature's private keys and seal's private keys, at the end of the validity period of the related certificate, are automatically deleted form the security modules through a process that ensures the impossibility of recovering them and re-using them again.

6.2.11 Cryptographic module rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

KeyPair usage period corresponds with the validity period indicated into the corresponding certificate.

TSU Certificates has ten years validity and three months usage period.

6.4 Activation data

Intesi Group S.p.A. ensures that activation data associated to operation executed with Intesi Group. CAs and TSUs private keys are securely generated, managed, stored and archived as described in the sub-section of sections 6.1 and 6.2.

The private keys activation data relating to qualified certificates (signature and seal) are defined by the holder during the certificate issuance phase. Holders are responsible for managing and securely protecting private activation data. For details see section 4.1.2 of this document and the related TSPP.

The Intesi Group's registration and issuing process ensures the confidentiality of the certificate activation data by protecting all communications between the components of the infrastructure through a secure TSL/SSL channel and saving all the information in encrypted form.

6.5 Computer Security Controls

Intesi Group ensures that computer security controls are implemented in compliance with the technical standard ETSI EN 319 411-1 and with ETSI EN 319 411-2.

Intesi Group internal procedures are ISO/IEC 27001 certified.

Detailed descriptions of implemented computer security controls are available as internal document(s).

6.6 Life cycle technical controls

The software development supporting the trust services of Intesi Group is executed conforming with the quality management system in compliance with UNI EN ISO 9001:2015

Intesi Group internal procedures are ISO/IEC 27001 certified.

Detailed descriptions of implemented life cycle technical controls are available as internal document(s).

Intesi Group only uses applications and devices that:

- are commercial off-the-shelf hardware and software, designed and developed by a documented design methodology, or;
- custom hardware and software developed by a reliable party in a controlled environment using structured development methods, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and validation.

New components are first tested within the testing environment before being used in production environment. Production and development environments are totally uncoupled.

Hardware is procured and shipped in a manner to reduce the likelihood of tampering. The hardware is dedicated to QTSP and QTSP related operations.

6.7 Network security controls

Network security controls including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc. are implemented in compliance with the requirements contained into the standard ETSI EN 319 411-1 and with ETSI EN 319 411-2.

Detailed descriptions of implemented network security controls are available as internal document(s)

6.8 CA and Time-stamping

All the computer systems used by the CA and Time-stamping service are synchronized with a Network Time Protocol (NTP) synchronized using “Stratum 1” time source. NTP service grants the time accuracy within few milliseconds of Coordinated Universal Time.

7 CERTIFICATE AND CRL PROFILE

The certificates conform to the ISO/IEC 9594-8:2005 [X.509] standard and to the [RFC 5280] public specification.

As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the QTSP conforms to: ETSI TS 119 312.

7.1 Certificate profile

7.1.1 CA for Time-stamp certificate

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Validity	<20 years>

Field	Value
SubjectDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.2 CA for Qualified Electronic Signature

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>

Field	Value
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.3 CA for Qualified Electronic Seal

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN = Intesi Group EU Qualified Electronic Seal CA G2, OU = Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Validity	<20 years>
SubjectDistinguishedName	CN = Intesi Group EU Qualified Electronic Seal CA G2, OU = Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>

Field	Value
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.4 Certificate for TSU

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT
Validity	<10 years>
SubjectDistinguishedName	CN=Time-Stamping Authority TSU<n>, OrganizationIdentifier=VATIT-02780480964, O=Intesi S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
Extended Key Usage (EKU)	Critical: Time Stamping
CertificatePolicies	PolicyOID = 1.3.6.1.4.1.48990.1.1.5.1 TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	http://crl.time4mind.com/Intesi/qualifiedtimestampCA.crl
QCStatement	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)

Field	Value
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.5 End User Certificate for Qualified Electronic Signature

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	serialNumber=<see id-etsi-qcs-SemanticsId-Natural>, G=<Subject name>, SN=<Subject surname>, dnQualifier=<CA Internal identifier> CN=<Name Surname>, O=<Optional: subject organization>, OrganizationIdentifier=<Optional: subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>

Field	Value
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.2 (QCP-n-qscd) • PolicyOID = 1.3.6.1.4.1.48990.1.1.1.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsignatureCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsignatureCA.crt
QCStatement	PKIX QCSyntax-v2 qcStatement-2 (0.4.0.194121.1.1) id-etsi-qcs-semanticsId-Natural
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS esi4-qcStatement-5 (0.4.0.1862.1.5) url:http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-esign
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.6 Certificate for Qualified Electronic Seal

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	dnQualifier=<CA Internal identifier> CN=<Commonly used organization name>, O=<subject organization>, OrganizationIdentifier=<subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.3 (QCP-l-qscd) • PolicyOID = 1.3.6.1.4.1.48990.1.1.2.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsealCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsealCA .crt
QCStatement	PKIX QCSyntax-v2 qcStatement-2 (0.4.0.194121.1.2) id-etsi-qcs-semanticsId-Legal
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3)

Field	Value
	QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS esi4-qcStatement-5 (0.4.0.1862.1.5) url:http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-eseal
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.7 OCSP Certificate for Qualified Electronic Signature

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 2048 bits>

Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.8 OCSP Certificate for Qualified Electronic Seal

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>

SubjectDistinguishedName	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.2 CRL profile

The CRLs are compliant with the with the ISO/IEC 9594-8:2005 [X.509] International Standard and public specification [RFC 5280].

Besides the mandatory information, the CRLs also contain:

- *nextUpdate* (date for next issue of CRL)
- *CRLNumber* (sequential number of CRL)

Moreover, in correspondence with each item of the CRL there is a *reasonCode* extension to indicate the reasons for suspension or revocation.

The CRLs are signed using the hashing algorithm sha256WithRSAEncryption (1.2.840.113549.1.1.11).

7.2.1 CRL issuing parameter

Field	Value
CRL Issuance Period	6 hours
CRL Duration	24 hours
CRL Grace Period	600 seconds

7.2.2 CRL for the Qualified Timestamp certificate

Field	Value
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
thisUpdate	<included>
nextUpdate	<included>
Extentsions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>

Field	Value
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.3 CRL for the Qualified Electronic Qualified certificate

Field	Value
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
thisUpdate	<included>
nextUpdate	<included>
Extentsions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.4 CRL for the Qualified Electronic Seal certificate

Field	Value
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
thisUpdate	<included>
nextUpdate	<included>
Extensions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

8 COMPLIANCE AUDIT

The technological infrastructure, physical and logical security controls, the operating procedures, and the personnel employed in providing the TSP services described in this TSPPS conforms to the EU eIDAS Regulation, implementing acts and corresponding ETSI standards for trust services eIDAS Regulation, implementing acts and corresponding ETSI standards for trust services.

Intesi Group is subject to external audits. Audits are conducted every year with compliance review in between according to eIDAS Regulation. These include audits pursuant to EU eIDAS Regulation, ETSI EN 319 401 and other relevant ETSI standards for the services provided. All these audits

require demonstration of a maximum level of security and conformity to documented policies and practices.

The auditor shall be an accredited Conformity Assessment Body (CAB), according to EU eIDAS Regulation and ETSI standards. The list of the accredited CABs is published and maintained updated by the European Commission.

In addition, Intesi Group performs internal self-audits. Topics covered by these audits include checks of proper implementation of Intesi Group's certificate policies and extensive checks on key management policies, security controls, operations policy and comprehensive checks on certificate profiles.

Intesi Group reserves the right to perform periodic inspections and audits of any LRA facilities to validate that the LRA is operating in accordance with the security practices and procedures laid out in the present CPS and in internal documents. Intesi Group is a Qualified Trust Service Provider (QTSP) according to European legislation; as such, Intesi Group is supervised by AgID

8.1 Frequency or circumstances of assessment

Intesi Group commits to do what is necessary so that a compliance audit be done at least every 12 months engaging a Conformity Assessment Body accredited according to the eIDAS Regulation.

The internal audits are carried out in accordance with a schedule which provides different periods (from monthly to annual) for the various technical-operational aspects of the QTSP service.

8.2 Identity and qualification of assessor

The internal audits are carried out by Intesi Groups' internal auditor, who is suitably qualified for the task. External audits, are performed by a Conformity Assessment Body accredited according to the eIDAS Regulation.

8.3 Assessor's relationship to assessed entity

No relationship shall exist between the QTSP and any external auditors that can influence the outcome of the audits in favor of Intesi Groups.

Intesi Group internal auditor does not belong to the organizational unit in charge of TSP operations.

8.4 Topics covered by assessment

Audits performed by external assessors (other than AgID) are aimed at verifying compliance of Intesi Group and the qualified services it provides according to the applicable requirements of the eIDAS Regulation.

The main objective of the internal audit is to verify the respect of Intesi Group internal operating procedures and their compliance with this TSPPS.

8.5 Actions taken as result of deficiency

In the case of non-compliances, AgID will require the QTSP to adopt the necessary corrective measures within a certain period, under penalty of fines and revocation of the accreditation.

Non-compliances found by CABs are brought to the attention of Intesi Group management who decides how to handle them on a case-by-case basis.

8.6 Communication of results

The results of internal audits are presented directly to Intesi Group top management, and shared with the other internal stakeholders, via an audit report.

When relevant and according to the eIDAS Regulation security incidents will be notified to the interested parties.

9 OTHER BUSINESS AND LEGAL MATTERS

The general Terms & Conditions of the QTSP service herein described are provided to customers as a separate document to be accepted at application time. The Terms & Conditions document is published on the QTSP web site.

In the case of a discrepancy between this TSPPS and the separate “Terms & Conditions” document, “Terms & Conditions” will take precedence.

9.1 Service fees

The fees are published on the TSP web site www.intesigroup.com and are subject to change without prior notification.

Different conditions may be negotiated case by case, according to the volumes requested.

9.2 Financial responsibility

Intesi Group maintains the following insurance related to its performance and obligations under this TSPPS:

- Commercial General Liability insurance
- Professional Liability/Errors and Omissions insurance.

Such insurance is with a company rated no less than A- as to Policy Holder’s Rating in the current edition of Best’s Insurance Guide.

9.3 Confidentiality of Business information

9.3.1 Confidential information

The following information are considered confidential:

- data provided by Certificate Applicants except for information that must be included in the certificates or that for other reasons are considered non-confidential (see paragraph 9.3.2 e 9.3);
- certificates issuance requests;
- certificates suspension or certificates revocation requests;
- communications exchanged between PKI participants (see section 1.3);
- reserved codes provided to the certificate holder (e.g. login credentials, private keys activation data etc.) if are generated by the QTSP or are managed by the QTSP systems;
- private keys;
- system logs;
- contracts with external RAs.

9.3.2 Non-confidential information

All information that must be public in compliance with the law or the certification services technical standards (e.g. RFC 5280) or for the explicit request of the certificate holder are not considered confidential.

The following information are not considered confidential:

- certificates and the information contained therein;
- lists of suspended or revoked certificates (CRL);
- information on the status of certificates issued on-line (e.g. via OCSP).

9.3.3 Responsibility for the protection of confidential information

The QTSP ensures that confidential information is physically and/or logically protected from unauthorized access (even if read only) and from the risk of loss due to disasters.

All confidential information is processed by the QTSP in compliance with applicable data protection and privacy laws.

9.4 Privacy of personal information

The Intesi Group privacy policy is published at the URL:

https://www.intesigroup.com/en/privacy-policy/

9.5 Intellectual property rights

Within the service regulated by this TSPPS, the QTSP does not collect and does not process sensitive data nor judicial data (with reference to article 4 of the aforesaid Decree [DLGS196]). This TSPPS is the property of Intesi Group who reserves all rights associated with the same. The subscriber of the service keeps all the rights on its own commercial marks (brand names) and its own domain names. With regards to the property rights of other data and information, the applicable law shall be applied.

9.6 Representation and warranties

9.6.1 Certification Authority

The QTSP shall:

- operate in compliance with this TSPPS;
- identify the subscriber as described in this TSPPS;

- issue and manage the certificates as described in this TSPPS;
- provide an efficient suspension and revocation service for the certificates;
- guarantee that the subscriber, at the time when the certificate is issued, did possess the corresponding private key;
- timely inform about any eventual compromise of its own private key;
- provide clear information about the procedures and requirements of the service;
- provide a copy of this TSPPS to anyone requesting it;
- guarantee processing of personal data in compliance with applicable law;
- provide an efficient and reliable information service about the status of the certificates.

9.6.2 Registration Authority

The RA activities are performed by RAO and LRA under a contractual obligation to comply scrupulously with the TSPPS, with the relevant section of the applicable TSPP, and with the RA relevant Intesi Group internal procedures.

The registration authority service is not applicable for Time Stamp service.

9.6.3 Subscribers

Refers to “Terms and Conditions” document at chapter 5.

9.6.4 Relying parties

Refers to “Terms and Conditions” document at chapter 7.

9.7 Disclaimer of warranties

Except as expressly provided elsewhere in the TSPPS, the applicable TSPP and in the applicable legislation, Intesi Group S.p.A. acting as TSP disclaims all warranties and obligations of any type,

including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorized source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. Intesi Group S.p.A. does not warrant “non repudiation” of any Certificate or message. Intesi Group S.p.A. does not warrant any software.

9.8 Limitations of Liability

Refers to “Terms and Conditions” document at chapter 8

9.9 Indemnities

Refers to “Terms and Conditions” document at chapter 8.

9.10 Term and Termination

This TSPPS is effective from the time it is published on the QTSP website (see Chapter 2) and on the AgID website and will remain in force until it is replaced with a new version.

9.11 Amendments

Intesi Groups reserves the right to modify this TSPPS at any time whatsoever without prior notification.

9.12 Dispute Resolution Provisions

The Subscribers can submit their claim or complaint on the following email:

tsp@intesigroup.com.

Complaints received by Intesi Group will be treated by Intesi Group internal services to resolve any dispute promptly and efficiently.

Any controversy that cannot be solved by Intesi Group internal services shall be submitted to the exclusive jurisdiction of the Milan Court, except for the conditions that apply in case the Subscriber can be qualified as Consumer according to Italian Legislative Decree 206/2005.

9.13 Governing Law

This TSPPS is subject to Italian and European Law and as such shall be interpreted and carried out. For that not expressly prescribed in this TSPPS, the applicable law shall prevail.

9.14 Compliance with Applicable Law

Mandatory applicable laws shall prevail on the provisions of this TSPPS.

9.15 Miscellaneous Provisions

Intesi Group incorporates by reference the following information in all Certificates it issues:

- Terms and conditions described in the applicable CP;
- Any other applicable Certificate Policy as may be stated in an issued Certificate;
- The mandatory elements and any non-mandatory but customized elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a Certificate.

To incorporate information by reference Intesi group through its CAs uses computer-based and text-based pointers that include URLs, OIDs, etc.