In.Te.S.A. S.p.A.
Qualified Trust Service Provider

Operations Manual
for remote digital signing procedures
in the context of the services provided by FinecoBank S.p.A.

English version of:
Manuale Operativo
per la procedura di firma digitale remota
nell'ambito dei Servizi forniti da FinecoBank S.p.A.
ver.05 (13/03/2020)

Document code: MO_FNC_ENG

OID: 1.3.76.21.1.3.1.161

Prepared by: Antonio Raia

Approved by: Franco Tafini

Issued on: 07/05/2020

Version: 05-E

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A.

Revisions

Version no.: 05-E	***Revision Date: 7 May 2020***
Description of changes:	English translation of the document *Manuale Operativo per la procedura di firma digitale remota nell'ambito dei Servizi forniti da FinecoBank S.p.A. ver.05 (13/03/2020)*
Reasons:	English version
Version no.: 05	***Revision Date: 13 March 2020***
Description of changes:	Updates to FinecoBank S.p.A. company name and logo F.3: new paragraph F.4: new paragraph Updates to relevant laws and definitions Updates to QTSP layout and logo
Reasons:	Change to company articles of association Description of "Mobile Code" authentication methods added Description of "Voice Password" authentication methods added Regulatory updates New QTSP In.Te.S.A. S.p.A. logo
Version no.: 04	***Revision Date: 13 June 2017***
Description of changes:	A.1: Share capital updated C.5: restriction on identification methods added
Reasons:	Change to FinecoBank S.p.A. Share Capital Specification of identification methods
Version no.: 03	***Revision Date: 09 February 2017***
Description of changes:	Change in procedure for certificate issuance Change to applicable regulation – verification of conformity
Reasons:	Updates to services Regulatory updates: Reg. (EU) 910/2014 (eIDAS) - Italian Legislative Decree no. 179 of 26/8/2016
Version no.: 02	***Revision Date: 17 March 2014***
Description of changes:	Updates to External Registration Authority Obligations Updates to references to the Decree of the President of the Council of Ministers, February 22, 2013 Addition of references to Applications for mobile devices Updates to the Document Code (MO-FNC)
Reasons:	Update
Version no.: 01	***Revision Date: 07 November 2012***
Description of changes:	None
Reasons:	First issue

Summary

Applicable laws

Consolidated Law Italian Presidential Decree 445/00 and subsequent amendments and supplements	Italian Presidential Decree no. 445 of 28 December 2000. "Consolidated legislative and regulatory provisions concerning administrative documentation". *Hereinafter also referred to simply as TU [Testo Unico]*.
Privacy Regulations	These include Regulation (EU) 2016/679 concerning the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"); the personal data protection Code, containing provisions to harmonise national regulations with the GDPR (Italian Legislative Decree 196/2003), orders, guidelines and opinions of the Italian Data Protection Authority, the European Data Protection Board (formerly the Article 29 Working Party) and any other competent authority; the Parties act in their capacities as independent data controllers in relation to the personal data collected by each for the purposes of performing their official functions and fulfilling their contractual obligations. Hereinafter they shall be referred to simply as *Privacy Regulations*
Italian Digital Administration Code - Italian Legislative Decree 82/05 and subsequent amendments and supplements	Italian Legislative Decree no. 82 of 7 March 2005. "Digital Administration Code". *Hereinafter also referred to simply as* CAD [Codice dell'Amministrazione Digitale].
Decree of the President of the Council of Ministers 22/02/2013 New Technical Standards and subsequent amendments and supplements	Decree of the President of the Council of Ministers of 22 February 2013 "Technical standards for the generation, application and verification of advanced, qualified and digital electronic signatures in accordance with articles 20, par. 3, 24 par. 4, 28 par. 3, 32 par. 3 point b), 35 par. 2, 36 par. 2, and 71" (of the CAD, ed.). Hereinafter also referred to simply as *DPCM [Decreto del Presidente Del Consiglio Dei Ministri]*.
Regulation (EU) no. 910/2014 (eIDAS) and subsequent amendments and supplements.	Regulation (EU) no. 910/2014 of the European Parliament and Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Hereinafter also referred to simply as *eIDAS Regulation* (electronic IDentification, Authentication and trust Services).
COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 and subsequent amendments and supplements.	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance). Hereinafter also simply referred to as *DECISION (EU) 2015/1506*.
RESOLUTION NO. 147/2019 and subsequent amendments and supplements	Guidelines containing "Technical standards and recommendations regarding generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time stamps". Hereinafter also referred to simply as the *RESOLUTION* or the *AgID Recommendations*.

Definitions and Acronyms

AgID Agency for Digital Italy	*Agenzia per l'Italia Digitale* (formerly CNIPA and DigitPA) - *www.agid.gov.it*. Supervisory Body in accordance with Reg. EU 910/2014 (eIDAS). Hereinafter also simply the *Agency*.
QTSP Qualified Trust Service Provider.	*Qualified Trust Service Provider*. Natural or legal person who provides one or more qualified trust services. Formerly *Accredited Certification Authority*, in accordance with the CAD.

Accredited Certification Authority	In this document, it refers to QTSP In.Te.S.A. S.p.A.
Qualified Trust Service	An electronic service provided by a QTSP consisting of the elements referred to in Art. 3, points 16) and 17) of Reg. EU 910/2014 (eIDAS). In this document, it refers to QTSP In.Te.S.A. S.p.A. who provides qualified electronic signature services and electronic time stamp services and other related services.
Qualified Certificate for electronic signature (digital signature)	Electronic attestation, which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. It is issued by a qualified trust service provider and meets the requirements laid down in Annex I of Reg. (EU) 910/2014 (eIDAS).
Private Key	The key in the asymmetric pair used by the Holder to digitally sign electronic documents.
Public Key	The key in the asymmetric pair intended to be made public, used to verify the digital signature applied to the electronic document.
CRL	Certificate Revocation List, a list of all revoked or suspended certificates, no longer regarded as valid by the QTSP / Certification Authority that issued them.
OCSP	Online Certificate Status Protocol: Certificate validity status verification service, in accordance with the OCSP.
Electronic document	Electronic document containing the representation of acts, facts or legally relevant data
QES *Qualified Electronic Signature* *DS - Digital Signature*	Electronic signature created by a device used to create qualified electronic signatures and based on a qualified certificate for electronic signatures. In Italy, it is equivalent to the *Firma Digitale [Digital Signature]* defined in art.1, par. 1, point s) of the CAD as: A qualified electronic signature based on a system of cryptographic keys – a public key and a private key, linked to each other – that enables the Holder, using the private key, and the recipient, using the public key, to prove and verify the origin and integrity of an electronic document or set of electronic documents.
Remote Signature	A specific qualified electronic signature or digital signature procedure, generated on a HSM supervised and managed under the responsibility of the QTSP / Certification Authority, ensuring exclusive control of the private keys by the holders of the same.
HSM - Hardware Security Module	Devices for creating qualified electronic signatures, if they comply with the requirements referred to in Annex II of Reg. (EU) 910/2014. Also referred to as Signature Devices.
Qualified Electronic Time Stamp	*Qualified Electronic Time Stamp* Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. It meets the requirements of art. 42 of the eIDAS Reg.
CA - Certification Authority	Authority that issues the electronic signature certificates.
RA - Registration Authority	*Registration Authority*: entity, appointed by the QTSP, responsible for recording and verifying the information (particularly the Holder's identity) required by the QTSP for the purposes of issuing the Qualified Certificate.
Certificate Directory	The combination of one or more electronic files, held by the QTSP / Certification Authority, containing all of the Certificates issued.
Applicant	The Natural Person who requests the Certificate.
Holder	The Natural Person to whom the Qualified Certificate is issued and who is authorised to use it for the purposes of applying his/her qualified electronic or digital signature.
Client *Prospect*	Is the Client (or potential Client, referred to as a Prospect) of the Bank.
Interested Third Party:	A natural or legal person whose consent is required for the Qualified Certificate to be issued to the Holder. He/she has the right/duty to request the revocation or suspension of the certificate in the event that changes occur to the criteria on the basis of which it was issued
Time Reference	Information containing the date and time, associated with one or more electronic documents.
TSA - Time Stamping Authority	Authority that issues electronic time stamps.
RACI (Table)	RACI - Responsible, Accountable, Consulted, Informed Responsibility assignment matrix (in relation to a process)

A. Introduction

This document is the *Operations Manual for the remote digital signing procedure in the context of the services provided by FinecoBank S.p.A.* (hereinafter also simply *Fineco* or *Bank*), with registered offices at Piazza Durante 11, 20131 Milan - Head Office at via Rivoluzione d'Ottobre, 16, 42123 Reggio Emilia, a Bank registered on the Banking Register and Parent Company of the FinecoBank Banking Group – Register of Banking Groups code 3015 - VAT no. 12962340159 - Tax Code and Milan-Monza-Brianza-Lodi register of companies number 01392970404 - Economic and Administrative Index no. 1598155 - Member of the *Fondo Nazionale di Garanzia* [Italian National Guarantee Fund] and the *Fondo Interbancario di Tutela dei depositi* [Interbank Deposit Protection Fund].

A.1. Intellectual Property

This Operations Manual is the exclusive property of In.Te.S.A. S.p.A., who holds all relevant intellectual property rights.

The information described in this document concerning performance of QTSP activities is subject to intellectual property rights.

A.2. The Operations Manual

The Operations Manual describes the procedures and relevant rules applied by the *Qualified Trust Services Provider In.Te.S.A. S.p.A.* (hereinafter also simply referred to as *INTESA* or *QTSP INTESA*) for the issuance of Qualified Certificates and the generation and verification of qualified electronic signatures as part of the services offered by FinecoBank S.p.A.

The content of this Operations Manual complies with the requirements of the technical regulations contained in the *Decree of the President of the Council of Ministers of February 22, 2013* (hereinafter also simply referred to as the "*DPCM*") and in the Legislative Decree of 7 March 2005, no. 82, containing the "*Digital Administration Code*", as subsequently amended and supplemented (hereinafter also simply referred to as to as "*CAD*") and complies with *Regulation (EU) 910/2014* (hereinafter "*eIDAS Reg.*").

Regarding anything not expressly mentioned in this Operations Manual, reference should be made to legislation and regulations currently in force.

In this context, Qualified Certificate Holders are limited to the persons identified by Fineco who, pursuant to a specific agreement with QTSP INTESA, are authorised to act as Registration Authority.

The process allows the Holder to activate the procedure related to the remote signature of documents and/or contracts relating to products and services offered by the Bank.

A.3. Validity

The contents described in this document apply to QTSP INTESA, i.e. to its logistics and technical infrastructure and to its staff, to Holders of certificates issued by the latter and to those who use such certificates to verify the authenticity and integrity of documents to which a qualified and relevant electronic signature is affixed, also making use of the time stamps issued by INTESA.

The use of keys and their related certificates is regulated in accordance with art. 5, par. 4 of the DPCM. For the purposes set out in this manual, the keys for the creation and verification of the signature and related services can be broken down into the following categories:

- *signing (or signature) keys*, used to generate and verify signatures applied to or associated with documents;
- *CA keys*, used to generate and verify signatures applied to qualified certificates, provide information on the certificate validity status or sign certificates relating to time-stamping keys;
- *time-stamping keys*, used to generate and verify time stamps.

B. General information

The purpose of this document is to describe, in general terms, the procedures and related rules used by the accredited QTSP INTESA to issue qualified certificates.

Compliance with such rules and procedures allows INTESA to be included on the list of Qualified Trust Service Providers (QTSP) in accordance with the eIDAS Regulation.

As such, in accordance with the aforementioned regulations, other parties are involved: these will be identified in more detail further on in this document.

B.1. Operations Manual version identification details

This document is the English translation of version no. **05**, issued on **13/03/2020** in accordance with art. 40 of the DPCM, of the *Operations Manual for the Remote Digital Signing procedure in the context of the Services provided by FinecoBank S.p.A.*

The object identifier for this document is **1.3.76.21.1.3.1.161**.

This Operations Manual is published and available to consult electronically:

- on the QTSP website: *www.intesa.it/e-trustcom/*
- on the Fineco website: *finecobank.com*

Note: updated versions of the Operations Manual can only be published with the prior authorisation of AgID - Agency for Digital Italy.

B.2. QTSP – Qualified Trust Service Provider Identification Details

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

Company name	**In.Te.S.A. S.p.A.**
Registered office	**Strada Pianezza, 289** **10151 Turin**
Legal Representative	**Managing Director**
Turin Company Register	**Registration no. 1692/87**
VAT no.	**05262890014**
Telephone no. (main switchboard)	**+39.011.19216.111**
Website address	***www.intesa.it***
E-mail address	***marketing@intesa.it***
Certificate Directory URL	***ldap://x500.e-trustcom.intesa.it***
ISO Object Identifier (OID)	**1.3.76.21.1**

B.3. Responsibility for the Operations Manual

Responsibility for this Operations Manual, pursuant to Art. 40, par. 3, lett. c) of the DPCM, lies with QTSP INTESA. The latter handles its drafting, publication, updating and any revisions, in agreement and in collaboration with the Bank.

INTESA welcomes comments and requests for clarification via the following specific channels:

- by e-mail to: e-trustcom@intesa.it *marketing@intesa.it*
- by phone to: +39 011.192.16.111
- via its HelpDesk service: for calls within Italy: 800.80.50.93
  for calls from outside Italy: +39 02.871.193.396

B.4. Entities involved in the processes

Certain entities within QTSP INTESA's organisational structure are identified as being involved in issuing the certificates.

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

The following personnel – all of whom are members of the QTSP's organisation – are responsible for certification activities in accordance with art. 38 of the DPCM:

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

B.4.1. Certification Authority (CA)

In accordance with the provisions of the DPCM, CAD and the eIDAS Regulation, INTESA performs the activities of Qualified Trust Service Provider. Such activities include qualified trust services involving generating, verifying and certifying electronic signatures, electronic seals and electronic time stamps.

QTSP INTESA identification details are provided in the previous paragraph *B.2*.

B.4.2. Registration Authority (RA)

Due to the special type of service offered (remote digital signing as part of the Bank's applications described in this Operation Manual), QTSP INTESA has authorised Fineco to act as Local Registration Authority (LRA).

More specifically, the Bank performs the following activities:

- Positive identification of the Applicant / Holder.
- Registration of the Applicant.

The Bank, in carrying out its function as Registration Authority, must ensure that Holder identification activities are carried out in accordance with current regulations.

C. Obligations

C.1. Obligations of the Qualified Trust Service Provider (QTSP)

In performing its role, the Qualified Trust Service Provider (also referred to as the *Accredited Certification Authority*) operates in accordance with the provisions of:

- the CAD - Italian Legislative Decree no. 82 of 7 March 2005 and subsequent amendments.
- Technical Standards: Decree of the President of the Council of Ministers of 22 February 2013.
- Privacy Regulations
- Regulation (EU) 910/2014 (eIDAS)

In particular, the QTSP:

- implements all appropriate organisational and technical measures to prevent damage to third parties;
- complies with the technical standards set out in the DPCM as amended and supplemented;
- guarantees that its Quality System complies with ISO 9001 standards;
- ensures that the signature generation device (HSM) satisfies the security requirements provided for in Art. 29 of the eIDAS Regulation;
- issues and publishes the Qualified Certificate, in accordance with the provisions of art. 32 of the CAD, in compliance with Privacy Regulations;
- provides applicants with clear and explicit information on the certification process, technical requirements to access it, characteristics of the signatures issued on the basis of the certification service and limitations on their use;

- acts in respect of the security measures for the processing of personal data, as provided for by the Privacy Regulations;
- is not a data repository for the generation of the Holder's signature;
- revokes or suspends the Qualified Certified if requested by the Holder or the Interested Third Party;
- guarantees precise specification of the date and time of issue, revocation and suspension of electronic certificates;
- keeps a record, including electronically, of all information relating to the Qualified Certificate for 20 (twenty) years, particularly for the purpose of providing proof of certification in the event of legal proceedings;
- ensures that the identification code (exclusive to the QTSP) assigned to each Holder is unique among its users;
- provides all information that may be useful to persons applying to use the certification service in a durable medium. This information includes: the precise terms and conditions for using the certificate, including any limitations on its use, the existence of an optional accreditation scheme and the complaint and dispute-resolution procedures. Such information, which may be sent electronically, must be written in plain and clear language and be provided prior to the agreement between the service applicant and the QTSP;
- uses reliable systems to manage the certificate directory in a way that ensures that only authorized persons can make entries and changes, that the authenticity of the information is verifiable, that certificates are only available for public consultation if permitted by the Holder of the certificate, and that the operator can identify any events that may compromise the security requirements;
- records the issuance of qualified certificates in the audit journal, specifying the date and time of generation.

Furthermore, the QTSP:

- generates a Qualified Certificate for each of the advanced electronic signature keys used by AgID to sign the public list of Qualified Trust Service Providers (QTSPs), and publishes it in its own certificate directory in accordance with art. 42 of the DPCM;
- provides, or recommends, an electronic signature verification system, as referred to in art. 14 of the DPCM;
- keeps a copy of the list, signed by AGID, of the certificates relating to the keys of the accredited certification authorities, in accordance with Art. 43 of the DPCM, publishing it electronically as provided for in art. 42, par. 3, of the DPCM.

The QTSP performs periodic audits of the LRA's premises to ensure compliance with the regulations, this Operations Manual and the provisions of the mandate agreement, in accordance with a sampling plan shared with the LRA.

C.2. Obligations of the Holder

The Holder requesting a Qualified Certificate for digital signatures for the services described in this Operations Manual is a customer of the Bank acting as Registration Authority.

As such, the Holder may receive a Qualified Certificate for remote digital signatures in order to sign contracts and documents related to products and/or services offered by the Bank.

The Holder is obliged to keep the information required to use the private signing key in a proper manner and to take all organizational and technical measures to avoid damage to others (Art. 32, par. 1, of the CAD).

The key Holder must also:

- provide all information requested by the QTSP, guaranteeing its accuracy under his/her own responsibility;
- send the certification application using the methods specified in this Operations Manual;
- notify the QTSP, via the Bank, of any changes to the information provided at the time of registering: personal details, address, phone numbers, e-mail addresses, etc.;
- store the information that enables the private key to be used with the utmost care and diligence;
- immediately inform the Bank in the event of loss or theft of the codes used to access his/her signing keys; the Bank will immediately take steps to deactivate the aforementioned codes and block the digital signature service access channels;
- send any requests for revocation or suspension of the Qualified Certificate in accordance with the instructions provided in this Operations Manual.

C.3. Obligations of certificate users

The User (*Relying Party*) is any person who receives a digitally signed document and, for the purposes of verifying its validity, avails of the Qualified Certificate used by the Holder to sign that document.

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

Persons who avail of a Qualified Certificate to verify the validity of a digitally signed document are required to:

- verify the validity of the certificate containing the public key of the Holder who signed the message and the time of its issue, in accordance with the standards in force at the time of its issue;
- verify the certificate validity status using the OCSP protocol or by accessing the Revocation Lists;
- verify the validity of the certification path, based on the public list of qualified trust service providers (QTSPs);
- verify the existence of any limitations on the use of the certificate used by the Holder in accordance with the Operations Manual of the Trust Service Provider that issued the certificate used by the Holder to sign electronic documents.

The obligations set out above are automatically fulfilled by Verification Software in compliance with current regulations (art. 14 of the DPCM).

C.4. Obligations of the Interested Third Party

Fineco is the interested Third Party for the purposes of the services described in this Operations Manual.

As such, the Bank must verify that the Customer meets all the necessary requirements before authorising the Customer's request for the Qualified Certificate for remote digital signatures.

The Bank, in its capacity as Interested Third Party, provides support to the Holder; more specifically, the Bank is responsible for notifying QTSP INTESA of:

- any further limitations on the use of the Qualified Certificate for Digital Signatures, in addition to those provided for in paragraph *F.5.1*;
- specific information relating to the Holder, including, but not limited to, any representative powers attributed to the Holder.

The Interested Third Party's revocation or suspension requests must be submitted immediately if the Holder ceases to meet the requirements according on the basis of which the Qualified Certificate was issued.

C.5. Obligations of External Registration Authorities

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

- positive identification of the Holder;
- Holder registration;
- providing the Holder with codes that enable him/her to access his/her signing key in accordance with Art. 8 and Art. 10, par. 2, of the DPCM.

QTSP INTESA has provided Fineco with a mandate to act as a Registration Authority by entering into a Mandate Agreement signed by both parties.

This contract sets out the obligations to be observed by the Bank appointed by INTESA to act as LRA, requiring supervision by the QTSP; more specifically, the Bank is required to:

- ensure that Holder identification activities are carried out in accordance with local regulations (the CAD, eIDAS Reg., the DPCM and subsequent amendments and supplements, and anti-money laundering regulations);
- use and process personal data obtained during the Holder identification and registration process in accordance with Privacy Regulations;

- securely store the documentation collected during the identification stage and the document providing consent to use the personal data, and make them available to QTSP INTESA upon request;
- grant access to its premises to QTSP personnel, or third parties appointed by the same, to comply with audit requirements; such access must also be granted to auditors appointed by the Supervisory Body (AgID);
- notify QTSP INTESA without delay, via the RA Department (*uff_ra@intesa.it*) or specific INTESA contact persons, of any event or incident related to the points referred to above, and of any security breach or loss of integrity that have a significant impact on the services covered by this Operations Manual or holders' personal data.

Bank personnel, in compliance with the provisions of current legislation on anti-money laundering and the internal regulations of the Bank itself, or in accordance with similar procedures adopted in compliance with anti-money laundering legislation in force at the time when the identification was carried out (even if that precedes publication of this Operations Manual), perform all the tasks necessary to identify and register the Applicant.

The documentation related to the aforementioned activities, required for the issuance of the Qualified Certificate, is to be stored by the Bank, in accordance with legal requirements, for 20 (twenty) years from the date of termination of the relationship.

D. Liability and limitations on compensation

D.1. Liability of the QTSP INTESA – Limitations on compensation

QTSP INTESA is liable towards Holders for compliance with all obligations arising from performance of the activities provided for by the DPCM, Privacy Regulations, the CAD and the eIDAS Regulation (as amended and supplemented), and all relevant applicable regulations, as described in par. *C.1 - Obligations of the Qualified Trust Service Provider (QTSP)*.

Except in cases of intention or negligence (in accordance with art. 13 of the eIDAS Reg.), QTSP INTESA shall not be held liable for consequences arising from use of the certificates other than as envisaged by art. 5 of the DPCM, and in particular for failure by the Holder and the Interested Third Party to act in compliance with this Operations Manual and/or with the regulations in force.

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

QTSP INTESA shall not be held liable for damages resulting from improper use of the Qualified Certificate for remote digital signatures, in relation to the limitation on its use as specified in par. *F.5.1*.

The Holder, having read this Operations Manual, must take all appropriate special due diligence measures to prevent damage to third parties associated with improper use of the material provided by QTSP INTESA. In particular, OTP devices and secret codes required to access the signing keys must be stored with due diligence.

D.2. Insurance

QTSP INTESA has insurance policies in place to cover risks associated with the activities and damage to third parties, the content of which satisfies the requirements for performing the professional activities in question.

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

E. Fees

The digital signing service is provided to the Holder free of charge, and as such is not subject to fees.

F. User identification and registration methods for the purposes of issuing the Qualified Certificate

F.1. User identification

QTSP INTESA must positively verify the identity of each applicant when they first apply for a Qualified Certificate for digital signatures.

This task is delegated to the Bank and, in accordance with the provisions of current Anti-Money Laundering regulations, will result in the identification and registration of the Holder.

The identification service can be managed in two ways:

1. ***Via a Personal Financial Advisor*** - the Holder can ask to be contacted by a Personal Financial Advisor who will set up an appointment and provide assistance with all procedures involved in opening a Current Account, including identification in accordance with anti-money laundering regulations. **NB**: this identification method is online available for the Italian market.
2. ***Directly online*** - the Holder applies to open a Current Account directly online. In this case, identification is carried out by the Bank in accordance with applicable anti-money laundering legislation.

In the event of renewal applications submitted prior to the expiry of the Qualified Certificate (previously issued), the activity does not need to be repeated: the Holder is only required to notify QTSP INTESA via the Bank of any changes to his/her registration details.

The following registration data is required to set up the service:

- name and surname;
- date of birth;
- municipality or foreign country of birth;
- tax code;
- home residence;
- address to which hard copy communications should be sent;
- mobile phone number;
- e-mail address;
- type and number of the identification document provided;
- authority that issued the document, date and place of issue and expiry date.

To access its services, Fineco provides its customers with a *User Code* and an *Activation Code*, via which it is possible to set up the password needed to access the reserved area of the *finecobank.com* website, and a *Personal Identification Number* (PIN, comprising 8 numeric characters) to ensure secure access to payment services and to the remote signature service provided by the Bank.

These credentials can be changed/updated by the Holder at a later date using the service provided by the Bank.

F.2. OTP Service

For subsequent operations (issuing the Qualified Certificate at the time of the first digital signature procedure), instead of using the more traditional OTP tools (One Time Password) based on physical tokens, the Customer can use an alternative service called ***OTP Service***.

This service provides Customers who have performed the activation process with a high level of security and consists of generating and sending a text message to the Customer's mobile phone. This OTP message is basically a "disposable" OTP code, to be used in addition to the standard device PIN for digital signing of documents and contracts relating to products or services offered by the Bank.

The text message, in addition to the OTP code, includes elements specific to the individual transaction requested by the Customer, specifically:

- each OTP code generated is associated with an individual transaction requested by the Customer and is not reusable under any circumstances;

- activation of the Service is permitted only to customers whose mobile telephone number, previously registered in Customer Database, has been "certified";
- activation of the Service is an essential step required to obtain the Qualified Certificate for digital signatures.

Also in this phase, further information and an emergency code will be provided, which the Holder may use at any time to suspend the Qualified Certificate issued to him/her. For the applications described in this Operations Manual, the OTP code described previously will serve as the emergency code.

To certify the mobile phone number, the Customer must enter the restricted area of the *finecobank.com* website by entering the user code and password, and then:

- go to the *"Contact Management"* section;
- enter the mobile phone number to be certified in the specific form, confirming the operation using the PIN;
- wait to receive a text message (to the mobile number provided) with the verification code (an e-mail with this information is also sent);
- confirm the operation on the website by entering the verification code received.

Confirmation of successful certification is sent by email to the Customer and a text message is sent to the mobile phone number that has just been activated.

In the customer switches mobile number, the service will automatically be transferred to the new number following certification of the same. Until that time, the service will continue to be active on the previous number.

In order to ensure maximum security, in the event of changing mobile phone number, two text messages will be sent, one to the old number and one to the new one, verifying that the Customer owns both numbers.

F.3. Mobile Code

Following the entry into force of the PSD2 European Regulation, a free service has been implemented via the Fineco App that increases security standards in terms of Strong Customer Authentication; this is known as a Mobile Code.

Using the Mobile Code, users are not required to enter the *Device PIN + OTP Code*; instead, a *Voice Password + Device PIN* can be used (see par *F.4*).

To activate the service, users must download the latest version of the Fineco App and follow the guided procedure that enables a personal Mobile Code to be created.

To activate the Mobile Code, users will be asked to:

- choose a personal 7-digit code (Mobile Code), which must be memorised;
- confirm the operation using the *device PIN* (the device PIN is the 8-digit code that is used by both the Fineco website and the App to confirm transactions made using the device, e.g.: bank or wire transfers, mobile top-ups);
- enter the OTP code sent by SMS to the certified mobile number.

IMPORTANT! When the activation process is complete, the Customer may choose to associate the code set (Mobile Code) with a piece of biometric identification data (*TouchID*, *Fingerprint* or *FaceID*). This provides the option of using face (*FaceID*) or digital fingerprint recognition (*TouchID*, *Fingerprint*) for applications that require the Mobile Code, making the process easier, quicker and more secure.

If the Customer chooses not to add biometric identification data, he/she will be required to enter the 7-digit code to confirm each transaction that requires the Mobile Code.

The Mobile Code can be activated at any time via the *Settings* section of the Fineco App, by selecting "*Mobile Code > Add"*.

F.4. Voice Password

Another option in terms of Strong Customer Authentication is to use the *Voice Password + Device PIN* instead of the *Mobile Code* or *Device PIN + OTP Code*.

How to access the Voice Password from the Reserved Area of the Fineco website:

- Provide *consent to biometric data processing* and enter the Device PIN to book an appointment.

- Users will then receive a call from the following number: 02.2899.2899.
  Note! In order to be connected to the operator, users must answer the call with the word "*Pronto*" [hello]. If the user fails to speak, the call will remain muted and will be disconnected after ten seconds.
- During activation, the user will be asked to repeat the following phrase between three and five times: *"My bank recognises the sound of my voice".* This allows the system to record the timbre of the voice.

If the *Voice Password* is not set up during the code activation stage, the steps listed above can be performed via the *Reserved Area* of the Fineco website, in the "*Account management > Your Fineco codes > Voice Password*" section.

Remember that the service can only be activated if the mobile number has been certified. To certify the mobile number, go to "*Account Management > Your contacts*" and follow the instructions.

F.5. Qualified Certificate for digital signatures

Following a request to QTSP INTESA – and provided that the Customer is in possession of a *certified mobile phone* and has been identified by the Bank in accordance with current laws and regulations, including on the subject of money-laundering prevention, and internal regulations of the Bank – a Qualified Certificate for digital signatures will be issued only at the beginning of the first digital signature procedure performed via the Bank's website (par. *I*).

As part of the contractual documentation involved in opening a Fineco current account, the Bank will provide the Customer with the necessary information on regulatory and privacy considerations associated with the issuance of Qualified Certificates, and instructions on how to request such a certificate from QTSP INTESA.

F.5.1. Limitations on the use

The Qualified Certificate for digital signatures, issued as part of the Fineco services described in this Manual, includes the following limitation on its use, which must be present both in Italian and in English:

> "*Il presente certificato è utilizzabile esclusivamente per la sottoscrizione di disposizioni e/o documenti e/o contratti relativi a prodotti e/o servizi di FinecoBank S.p.A. e/o di terzi, offerti da FinecoBank tramite il sito internet e/o l'App Fineco.*".
> "*This certificate may only be used for digital signature of provisions and/or documents and/or contracts concerning products and/or services of FinecoBank S.p.A. and/or of third parties, provided by FinecoBank through the website and/or Fineco's App.*".

G. Generating CA, time-stamp and signing keys

G.1. Generating CA Keys

Keys are generated on signature devices in the presence of the *CA Services Manager*, as provided for in Art. 7 of the DPCM.

Such operations are preceded by initialisation of the signature devices (HSM) for the certificate generation system used to sign the Holder's certificates and for the time-stamping system.

These operations are performed in dual-control mode to prevent illegal activities.

Once a pair of CA keys have been generated, operations can only be performed using specific authorisation devices (USB tokens): privileged access to HSMs can only be gained using the keys contained in such authorisation devices. To increase security, such keys are divided across multiple devices, using an "*n-of-m*"-type logic; as such, operations involving the relevant privileges can only be performed in the simultaneous presence of at least *n* of *m* parts of the key. As such, they are kept in separate dedicated safes.

The length of the CA keys shall comply with the standards in force at the time.

G.2. Generating time stamp system keys

Time-stamp keys are generated in accordance with the provisions of art. 49 of the DPCM.

The length of the time-stamp keys shall comply with the standards in force at the time.

G.3. Generating signing keys

Once the registration process – during which the Holder's data is saved in QTSP INTESA's files – is complete, the signing key can be generated.

The Holder can begin the key generation process and request the associated Qualified Certificate for digital signatures by logging on to the system provided by the Bank using one of the methods described above.

The PIN and OTP (generated using the methods described) are the two pieces of data that the Holder must have exclusive knowledge and possession of in accordance with art. 8, par. 5, lett. d) of the DPCM. He/she will be asked to enter these pieces of data each time he/she wishes to sign a document, in accordance with the provisions of art. 35, par. 2 of the CAD.

This authentication system allows the Holder to retain exclusive control of his/her signing keys, in accordance with art. 7, par. 3, lett. d), of the DPCM.

The signing key pairs (at least 2048-bit long) are created on secure devices, Hardware Security Modules, and comply with the provisions of current legislation.

H. Procedures for issuing certificates

H.1. Procedure for the issuing CA Certificates

Following generation of the CA keys, described in paragraph *G.1*, public key certificates are generated in accordance with the provisions of the DPCM, signed with the relevant private keys and registered in the certificate directory in accordance with the methods provided for.

CA key certificates are sent to AgID using the communication system referred to in art. 12, par. 1 of the DPCM.

H.2. Procedure for issuing signing certificates

QTSP INTESA issues certificates using a system that complies with art. 33 of the DPCM.

After generation of the signing key pair, described in paragraph *G.3*, it is then possible to generate a new certificate request in PKCS#10 format, which automatically provides proof of possession of the private key and verifies the proper functioning of the key pair.

Once the keys have been generated, a certificate request will be sent immediately from the Bank application to the QTSP Certification Authority.

The generation of certificates is recorded in the Audit Journal (art. 18, par. 4, of the DPCM).

H.3. Information contained in the certificates

QTSP INTESA certificates, issued in accordance with this manual, are qualified certificates pursuant to Regulation (EU) no. 910/2014 (eIDAS) and, as such, their inter-operability and recognition at an EU level are guaranteed. The certificates also comply with the provisions of AgID Resolution no. 147/2019 (*Guidelines containing technical standards and recommendations regarding generation of certificates*).

Each Qualified Certificate for digital signatures contains, by way of mere, non-exhaustive example, the following information:

- serial number;
- company name of the QTSP (issuer);
- unique identification number assigned to the Holder by the QTSP;
- name, surname and tax code of the Holder;
- public key value;
- applicable generation and verification algorithms;
- beginning and end of the certificate validity period;
- certificate signing algorithm;
- type of keys;

- limitations on the use of the key pair.

The Qualified Certificate unequivocally identifies the QTSP that issued it (issuer) and contains the data required to verify the digital signature.

All Qualified Certificates issued as part of the services described in this Manual includes at least one limitation on its use (par. *F.5.1*).

H.4. Emergency Code

The QTSP provides an emergency code to be used to request the suspension of the Certificate (DPCM art. 21).

For the applications described in this Operations Manual, the OTP code described previously will serve as an emergency code.

I. Operating procedures for signing documents

Via the Bank's services, QTSP INTESA provides Holders with an application for digital signatures as required by current law.

This service does not require that the signature application be installed on the Customer's personal computer. The signature function will be made available by accessing the services offered by the Bank in the reserved area of the *finecobank.com* website or via Applications for mobile devices (Smartphones and Tablets using Apple IOS, Android and Windows Phone 8). The qualified electronic signatures obtained using these procedures will comply with the provisions of art. 4, par. 2, of the DPCM, relating to the algorithms used.

As required by art. 4, par. 3 of the DPCM, documents signed using this signature application will not contain macro instructions or executable codes that could activate features that, unbeknownst to the Holder, could edit records, facts and data contained in the documents signed.

In addition, such documents will always be available to the signatory in a specific section of the restricted area of the *finecobank.com* website.

I.1. Issuing Qualified Certificates

As described in par. *F*, if the Customer is not yet the Holder of a Qualified Certificate for digital signatures in relation to FinecoBank services, he/she shall submit a request to QTSP INTESA, via Fineco, to issue a Certificate at the time of starting the first signing procedure using the Bank's website.

In such cases, the Customer must review the Operations Manual, information on the service and the privacy information provided by INTESA. Following that review, the Customer shall submit the request for certification, by applying a *flag* to a specific disclaimer that confirms that he/she is fully aware of all regulatory and privacy aspects in relation to use of the Qualified Certificate. Once the disclaimer has been accepted as referred to above, Fineco shall send the certificate issue request to CA INTESA on behalf of the Customer.

This Operations Manual and the disclaimer shall be available for consultation at any time in the reserved area of the Bank's website.

I.2. Signing process

Once the necessary codes have been obtained in the identification phase, the Customer can begin the document signing procedure using the methods described below.

1. A Holder of a Qualified Certificate for digital signatures visits the reserved area of the *finecobank.com* website or mobile device applications (available on Smartphones and Tablets with *Apple IOS*, *Android* and *Windows Phone 8* operating systems) and enters the user code and password in the dedicated section to request to digitally sign documents and contracts for products or services offered by the Bank.
2. He/she reads the document(s) to be digitally signed and any additional documentation for informational purposes.
3. He/she begins the signing process by entering the device PIN to confirm that he/she wishes to sign the contract(s).

4. He/she waits to receive a message containing the OTP to his/her mobile phone.
5. He/she confirms the operation online by entering the code received. The Customer can then confirm the operation immediately or at a later time (provided the OTP has not expired) by visiting a specific section containing the documents still "*To be confirmed*" and entering the OTP received to the mobile phone. It is also possible to confirm the operation by forwarding the received text message to a dedicated telephone number, without deleting the original message text.
6. After the OTP code has been entered correctly, a text message is sent confirming that the operation has been completed.
7. If the OTP code is not received, the Customer may request a new OTP code by clicking on the "*Have not received the OTP?"* link available in the area where the code is to be entered. The OTP code request may be resubmitted a maximum of 3 times.
8. As an alternative to the *Device PIN + OTP code*, the Customer can use the *Mobile Code*, provided that it has been activated in advance (par. *F.3*), or the *Voice Password + Device PIN* (par. *F.4*).
   NOTE: the Bank reserves the right to decide upon the authentication method associated with the Qualified Certificate for digital signature request on each occasion, including based on changes in applicable regulations.
9. If the allotted time period passes without the system receiving confirmation as specified in point 5, the operation is cancelled without the documents being signed.

J. Operating procedures for verifying signatures

The documents signed using the methods specified above are exclusively prepared in *PDF* format (*PDF electronic signature*, DECISION (EU) 2015/1506, art. 1) and, as such, may be verified using *Adobe Acrobat Reader DC* software, which can be downloaded free of charge from *www.adobe.com*.

K. Procedure for revoking and suspending certificates

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

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

If revocation or suspension is performed at the request of the QTSP or the Interested Third Party (Articles 23, 25, 27 and 29 of the DPCM), the QTSP notifies the Holder of the request and the time that the requested event will become effective.

The date and time at which the revocation will come into effect shall be specified in the request (art. 24, par. 1, of the DPCM).

K.1. Revocation of certificates

A Qualified Certificate for digital signatures may be revoked at the request of the Holder, the Interested Third Party or the Certification Authority (i.e. the QTSP).

Revoked certificates cannot be reactivated under any circumstances.

K.1.1. Revocation at the Holder's request

The Holder may request revocation of his/her Qualified Certificate by accessing a specific section made available as part of the Bank's services, or by contacting the Bank's Customer Services Department directly.

The Bank will notify the QTSP, who will revoke the certificate immediately.

K.1.2. Revocation at the Interested Third Party's request

The Bank, in its capacity as Interested Third Party, may request revocation of the certificate.

The QTSP, having ascertained the validity of the request, will notify the affected Holders of the revocation using the channels agreed upon with the Holder at the time of registering.

K.1.3. Revocation at the QTSP's request

Except in cases of justifiable urgency, the QTSP may revoke a Qualified Certificate for signatures giving prior notice to the Holder at the email address (or certified email address) provided in the registration phase, specifying the reasons for revocation and the date and time from which the revocation will be effective.

The QTSP will send a similar notice to the Interested Third Party.

K.1.4. Revocation of certificates relating to CA keys

In the event that:

- the CA key has been compromised,
- the signature device (HSM) is faulty,
- the relevant activity ceases,

the QTSP will proceed to revoke the CA certificates (par. *H.1*) and signing certificates signed using the relevant CA key.

The QTSP will notify AgID and the Holders of the revocation within 24 hours.

K.2. Suspension of certificates

As regards suspension and providing notice of the same, the relevant methods are those described in par. *K.1.*

A certificate may be suspended if further investigations are required to determine whether or not the certificate should be revoked.

A suspension request may be made by all entities described in Articles 23, 24 and 25 of the DPCM (QTSP, Holder, Interested Third Party).

In the absence of communication from the Holder, the certificate will be automatically revoked following a suspension period of 90 (ninety) days or, in any case, by the certificate expiry date.

The effective date of revocation will, in any case, coincide with the effective date of suspension.

K.2.1. Suspension at the Holder's request

The Holder may request suspension of the certificate by accessing a specific section made available as part of the Bank's services, or by contacting the Bank's Customer Services Department directly.

The Bank will notify the QTSP, who will suspend the certificate immediately.

The Holder may subsequently request reactivation of the certificate using the methods provided for by the Bank.

In the absence of further notification, the suspended certificate will be revoked automatically at the end of the suspension period.

K.2.2. Suspension at the Interested Third Party's request

The Bank, in its capacity as Interested Third Party, may request suspension of the certificate.

The QTSP, having ascertained the validity of a request, will suspend the certificate immediately and give notice of the suspension to the relevant Holders using the communication channels established with the Holder during the registration phase.

K.2.3. Suspension at the QTSP's request

Except in cases of justifiable urgency, the QTSP may suspend the certificate giving prior notice to the Holder at the certified email address provided in the registration phase, specifying the reasons for the suspension and the date and time from which the suspension will be effective.

The QTSP will send a similar notice to the Interested Third Party.

L. Method for replacing keys

L.1. Replacing qualified certificates and the Holder's keys

For the purposes of the services covered by this manual, digital certificates issued by QTSP INTESA are valid for 12 (twelve) months from the date of issue.

These certificates are automatically renewed for a further two years.

At the end of three years, it will be necessary to perform a procedure similar to that required to issue a new certificate (first issue).

L.1. Replacement of QTSP keys

L.1.1. Emergency replacement of CA keys

The procedure to be followed in the event that the signing device (HSM) containing the CA keys (CA and TSCA) fails, or a disaster occurs at the main operating centre, is covered in par. *P - Procedures for managing catastrophic events*.

L.1.2. Scheduled replacement of CA keys

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

L.1.3. Time stamp system keys (TSA)

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

M. Certificate Directory

M.1. Procedure for managing the Certificate Directory

INTESA publishes the following information in the certificate directory:

- The signing key and time stamp certificates.
- CA key certificates (CA and TSCA).
- Certificates issued following replacement of CA keys.
- Certificates for AgID signing keys (DPCM art. 42, par. 1).
- Revocation and suspension lists (CRL).

Operations involving the certificate directory are only carried out by authorised persons, adequate numbers of whom are present to ensure prevention of illegal activities by a limited number of staff members.

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

Verification that the master copy matches the operational copy is carried out systematically.

M.2. Logical access to the Certificate Directory

The Master Directory is placed within a restricted network protected by appropriate devices. Therefore, only the certificate-issuing server has access to it, to register the certificates issued and the CRL.

Access is possible via the LDAP protocol at ***ldap://x500.e-trustcom.intesa.it***.

QTSP INTESA also grants online access to the CRLs via the http protocol at the URL specified in the CDP (CRL Distribution Point) field of the certificate.

M.3. Physical access to the certificate directory premises

The operators qualified to directly manage the certificate directory can access the location where the system is installed and work there only if their number is deemed adequate to prevent illegal actions.

The systems managers, network managers, maintenance technicians, etc., can enter the location where the system is installed and operate there only in the presence of employees authorized to manage the certificate directory in the manner previously described for authorised operators.

N. Personal data protection procedures

Technical and organisational security measures are appropriate and ensure that the processing of personal data complies with Privacy Regulations.

O. Procedures for managing backup copies

Digital Archives that are subject to backup are as follows:

- CERTIFICATE DIRECTORY - digital archive consisting of contents as set out in section L.1.
- OPERATING INFORMATION, a digital archive where all of the information received from the Holder at the time of registering and applying for a certificate is stored, as well as any revocation and suspension requests, together with the relevant documentation.
- AUDIT JOURNAL, an archive consisting of the set of records automatically generated by the systems installed as part of the TSP certification service (art.36 of the DPCM).
- DIGITAL ARCHIVE OF TIME STAMPS - contains the time stamps generated by the TSA system (art. 49, par. 1, of the DPCM).
- OPERATIONAL REGISTER OF TIME-STAMPING EVENTS - register where events relating to time-stamping activities are automatically saved. Any anomalies or tampering attempts that could affect proper operation of the time-stamping system are recorded here (art. 52 of the DPCM).

The archiving of all backups referred to above is carried out in compliance with the provisions of current regulations.

P. Procedures for managing catastrophic events

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

- Emergency Period management: during this phase, continuity of access to the CRL is guaranteed; delays may occur in issuing such, due to the need to activate the CA backup server (located at the backup site);
- Transition Period management: during this phase, the issuance of certificates is guaranteed, as is activation of additional disaster recovery solutions;
- Return to standard operating mode: at the original site or at an alternative permanent site.

Replicas of the operational copy of the certificate directory are distributed across various locations, meaning that, in the event of a service interruption at one of the sites, certificate directory content can still be accessed and will be up-to-date up until the time of the interruption.

For the purposes of managing the emergency, replication of the certificate directory and of the certificate issuance system data is carried out at the backup site. Within 24 hours, trained personnel will restore CRL issuance functionality. The aforementioned staff receive training not only in managing the SW and HW systems, but also in dealing with emergency situations.

A hard copy of the emergency plan is kept at all sites involved in managing catastrophic events.

Q. Procedure for applying and defining the time reference

All machines included in the QTSP INTESA PKI system are synchronized with the I.N.RI.M. – *Istituto Nazionale di Ricerca Metrologica* (National Institute of Metrological Research) in Turin, formerly the Galileo Ferraris *Istituto Elettrotecnico Nazionale* (National Electrotechnical Institute). This function is performed by specific software installed on each server, which connects to the configured remote servers via the Network Time Protocol.

The Network Time Protocol (NTP) is one of the most accurate and flexible ways to obtain time and date information on the Internet. It continuously synchronises all computers connected via local, metropolitan or global networks (Internet) using a hierarchical pyramid structure.

I.N.RI.M. provides a synchronization service for computer systems connected to the Internet, based on two primary NTP servers installed in the Time and Frequency Standard Laboratory. They are synchronized via a time and date code generator by caesium beam atomic clocks, also used to generate the Italian national time scale UTC (IT). The time gap between I.N.RI.M. NTP servers and the Italian national time scale is monitored and is usually less than a few milliseconds. The synchronization accuracy obtainable depends on the network type and the distance placed between the NTP server and the computer to be synchronized; the typical deviation values are less than a millisecond for systems belonging to the same network and can reach a few hundred milliseconds for remote networks.

The QTSP INTESA software connects the local machine to the INRIM remote server at regular time intervals and, after obtaining the current time, sets the clock of the local machine, using sophisticated algorithms.

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

Each record in the Audit Journal contains a time reference that, generated as described above, is binding on third parties (art. 41 of the DPCM).

Q.1. Procedure for requesting and verifying time stamps

QTSP INTESA applies a time stamp (*qualified electronic time stamp*, in accordance with eIDAS Reg.) to all documents signed by the Holder as part of the services described in this Operations Manual.

Applying this time stamp is a part of the signing process and does not require any specific action on the part of the Holder.

R. Lead Time and RACI table for issuing certificates

R.1. Process lead time

The Table below refers to the "Process Lead Time" for managing requests to Issue, Revoke, Suspend and Reactivate Certificates.

Subject	Request	Entity Involved	Action by the Entity Involved	Entity Involved	Action by the Entity Involved
Certificate User, Applicant, Holder	*Request to Issue Certificate to LRA*	*Bank (acting as) Local RA*	*Issues order to publish Certificate to CA following identity verification*	*Certification Authority*	*Processing Certificate Request*
Certificate User, Applicant, Holder	*Request to Revoke Certificate to RA or LRA*	*INTESA (acting as) Registration Authority (RA) or Bank (acting as LRA)*	*Issues order to revoke Certificate to CA following identity verification*	*Certification Authority*	*Processing Revocation Request*

Certificate User, Applicant, Holder	*Request to Suspend Certificate to RA or LRA*	*INTESA (acting as) Registration Authority (RA) or Bank (acting as LRA)*	*Issues order to suspend Certificate to CA following identity verification*	*Certification Authority*	*Processing Suspension Request*
Certificate User, Applicant, Holder	*Request to Reactivate Certificate to RA or LRA*	*INTESA (acting as) Registration Authority (RA) or Bank (acting as LRA)*	*Issues order to reactivate Certificate to CA following identity verification*	*Certification Authority*	*Processing Reactivation Request*

R.2. RACI Table

Below is a RACI Table (Responsibility Assignment Matrix) outlining the responsibilities of the parties involved in handling requests to Issue, Revoke, Suspend and Reactivate Certificates.

Person Involved	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Certificate User, Applicant, Holder			***X***	***X***

S. Technical Reference Material

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
ETSI TS 103172	ETSI TS 103172 v.2.2.2. - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (NTP Protocol)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (NTP Protocol)

------- END OF DOCUMENT -------