In.Te.S.A. S.p.A.
Qualified Trust Service Provider
pursuant to Regulation (EU) No910/2014 (eIDAS)

Operating Manual for remote qualified electronic signature procedures within the scope of CA Auto Bank services

***Document Code**: MO_CAAB*

OID: 1.3.76.21.1.50.8

Drafting: Antonio Raia

Approval: Simone Baldini

Issue Date: 15/06/2026

Version: 01

Revisions

Version n°: 01	***Revision Date: 15/06/2026***
Description of changes:	none
Reasons:	first release

Summary

Legal References

Consolidated Text - DPR 445/00 and subsequent amendments and additions	Presidential Decree of 28 December 2000, n. 445. "*Consolidated text of legislative and regulatory provisions regarding administrative documentation*". Referred to as **TU**.
CAD - DLGS 82/05 and subsequent amendments and additions	Legislative Decree 7 March 2005, n. 82 - "*Digital Administration Code*". Referred to as **CAD**.
DPCM 22/02/2013 and subsequent amendments and additions	Decree of the President of the Council of Ministers 22 February 2013. "Technical rules regarding the generation, affixing and verification of advanced, qualified and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3), 32(3)(b), 35(2), 36(2), and 71." (of the CAD, editor's note). Referred to as **DPCM**
Regulation (EU) N. 910/2014 (eIDAS) and subsequent amendments and additions	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC Referred to as **eIDAS Reg.**
Regulation (EU) N. 2016/679 GDPR - General Data Protection Regulation and subsequent amendments and additions	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Referred to as **GDPR**.
DECISION No. 147/2019 and subsequent amendments and additions	Guidelines containing the "Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic signatures and seals, and qualified electronic time stamps". Referred to as **DETERMINATION.**
AgID Communication 0016101 of 7 June 2016	"agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016", concerning "Request for clarification regarding the use of digital signatures in specific closed user environments". Referred to as **Com. AgID 7/6/2016**.
Fourth AML Directive	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC
Fifth AML Directive	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU

Definitions and Acronyms

AgID	*Agency for Digital Italy (Agenzia per l'Italia Digitale).* - *www.agid.gov.it*. Supervisory Body pursuant to EU Reg. 910/2014. Referred to as **Agenzia**.
QTSP Qualified Trust Service Provider.	*Natural or legal person who provides one or more qualified trust services.* In this document, it refers to **In.Te.S.A. S.p.A.**
Qualified trust service	Electronic service provided by a QTSP and consisting of the elements referred to in Article 3, points 16) and 17) of EU Regulation 910/2014 (eIDAS). In this document, it is QTSP In.Te.S.A. S.p.A. that provides qualified electronic signature and electronic time stamping services and other services related to these.
Qualified Electronic Signature Certificate	Electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or pseudonym of that person. It is issued by a qualified trust service

	provider and complies with the requirements set out in Annex I to Regulation (EU) No 910/2014 (eIDAS).
Private Key	The element of the asymmetric key pair, used by the Holder, by which the digital signature is affixed to the electronic document.
Public key	The element of the asymmetric key pair intended to be made public, which is used to verify the digital signature on the electronic document.
CRL	Certificate Revocation List, a list of revoked or suspended certificates that are no longer considered valid by the Certification Authority that issued them.
OCSP	Online Certificate Status Protocol: service for verifying the validity status of the Certificate, according to the OCSP protocol.
Electronic document	The electronic document containing the computerised representation of legally relevant acts, facts or data.
QES - Qualified Electronic Signature	Electronic signature created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures. In Italy, this coincides with the "Digital Signature" defined in the CAD.
Remote Signature	Particular qualified electronic signature procedure, generated on an HSM held and managed under the responsibility of the QTSP, ensuring the Holder's exclusive control over the private keys.
HSM - Hardware Security Module	Devices for creating qualified electronic signatures, if they comply with the requirements set out in Annex II to Regulation (EU) No 910/2014. Also referred to as Signature Devices.
Qualified Electronic Time Stamp	Data in electronic form that links other data in electronic form to a specific time and date, thereby proving that the latter data existed at that time. Meets the requirements of Article 42 of the eIDAS Regulation.
CA - Certification Authority	Authority that issues certificates for electronic signatures.
LRA – Local Registration Authority	Entity that, under the mandate of the QTSP, is responsible for identifying, recording and verifying information (specifically the Holder's identity) necessary for the QTSP to issue the Qualified Certificate. In this Manual, LRA refers to companies belonging to the CA Auto Bank Banking Group (https://www.ca-autobank.com/en/group/corporate-structure/).
Certificate Register	The combination of one or more computer archives, kept by the Certifier, containing all the Certificates issued.
Applicant *Certification request*	The natural person requesting the certificate, i.e. who submits a certification request to the QTSP.
Holder	The Natural Person to whom the qualified signature certificate is issued and who is authorized to use it to affix their digital signature.
Customer *Prospect*	This is the customer (or potential customer, known as a prospect) of CA Auto Bank.
Time Reference	Information containing the date and time, which is associated with one or more electronic documents.
TSA - Time Stamping Authority	Authority issuing electronic time stamps.
Audit Journal	A collection of records, including those made automatically by devices installed at the QTSP, kept in such a way as to guarantee the authenticity of the entries and allow the reconstruction, with the necessary accuracy, of all events relevant to security (DPCM).
CPS - CP	*CPS - Certification Practice Statement e CP - Certificate Policy for Qualified Electronic Signature and Electronic Seal Certificates* of the QTSP INTESA: this document constitutes the Practice Statement of the QTSP and describes the rules and operating procedures for the issuance of qualified electronic signature and electronic seal certificates, as defined in Regulation (EU) 910/2014 (eIDAS). It is published on the Agency's website and by the QTSP at the following URL: *https://www.intesa.it/e-trustcom/*
URL	*Uniform Resource Locator:* It is a sequence of characters that uniquely identifies the address of a resource on a computer network, such as a document, web page or portal located on a host server and made accessible to a client.

A. Introduction

This document is the *Operating Manual for the remote qualified electronic signature procedure of the Qualified Trust Service Provider In.Te.S.A. S.p.A. within the scope of services provided by CA Auto Bank S.p.A.* Single-member company – Corso Orbassano no. 367, 10137 Turin – Share capital €700,000,000 fully paid up – www.ca-autobank.com – Turin Register of Companies no. 08349560014 - Tax code and VAT no. 08349560014 - Registered in the Register of Banks no. 5764 - Parent company of the CA Auto Bank Banking Group - Registered in the Register of Banking Groups ABI code 3445 - Registered in the Single Register of Insurance Intermediaries (RUI) no. D000164561 - Management and Coordination pursuant to Art. 2497 of the Italian Civil Code - Crédit Agricole Consumer Finance S.A.

The Operating Manual describes the procedures and related rules implemented by the QTSP INTESA for the issuance of Qualified Certificates, pursuant to EU Reg. 910/2014, for the generation and verification of the qualified electronic signature of the Customer of one of the companies controlled by CA Auto Bank S.p.A. (hereinafter also referred as to FCA Bank) within the scope of the services offered by the latter. The content of this Operating Manual complies with the technical rules contained in the Decree of the President of the Council of Ministers of 22 February 2013 (hereinafter DPCM) and Legislative Decree No. 82 of 7 March 2005, containing the 'Digital Administration Code' as subsequently amended and supplemented (hereinafter 'CAD') and complies with EU Regulation 910/2014 (hereinafter, eIDAS Regulation); in particular:

- CAD - Chapter II, Section II, which regulates electronic signatures and certifying authorities;
- CAD - Chapter VII, which sets out the procedures for establishing the technical rules provided for in the Code.

For anything not expressly provided for in this Operating Manual, reference shall be made to current and future regulations governing the specific case.

In this context, the Holders of a Qualified Certificate are only those identified by CA Auto Bank itself, which, by virtue of a specific agreement with the Certification Authority, is authorised to perform the function of Registration Authority.

The process allows the Holder to initiate the Remote Digital Signature procedure for documents, deeds, contracts and orders relating to products and services provided or distributed by CA Auto Bank.

The activities described in this Operating Manual are carried out in accordance with EU Regulation 910/2014 (eIDAS).

A.1. Intellectual Property

This Operating Manual is the exclusive property of In.Te.S.A. S.p.A., which owns all related intellectual rights. The activities described herein for the QTSP function are covered by intellectual property rights.

A.2. Validity

The provisions of this document apply to QTSP INTESA (its logistical and technical infrastructure, as well as its personnel), to the Holders of certificates issued by it and to those who use such certificates to verify the authenticity and integrity of documents bearing a qualified electronic signature relating to them, including by using qualified time stamps issued by INTESA, as well as to CA Auto Bank in its capacity as Local Registration Authority.

The use of keys and related certificates issued is governed by the provisions of applicable legislation, which stipulates that signature creation and verification keys and related services are divided into the following types:

a) signature keys, used to generate and verify signatures affixed to or associated with documents;
b) certification keys, used to generate and verify signatures affixed to qualified certificates, information on the validity status of the certificate or the signing of certificates relating to electronic time validation keys;
c) timestamping keys, used to generate and verify timestamps;
d) keys used to sign information on the validity status of certificates (OCSP);
e) keys used to sign the separate attribute certificate.

B. General information

The purpose of this document is to provide a general description of the procedures and related rules governing the issuance of qualified certificates by QTSP INTESA.

The aforementioned rules and procedures stem from compliance with current reference regulations, which allow INTESA to be included in the list of accredited certification authority.

Therefore, in order to comply with the aforementioned regulations, it will be necessary to involve several entities, which will be better identified later in this document.

B.1. Operating Manual Version Data

This document is version n. ***01*** of the ***Certification Practice Statement (Operational Manual) for procedures relating to the issuance of qualified certificates and remote qualified electronic signatures within the scope of CA Auto Bank services*** issued in compliance with current eIDAS regulations.

The object identifier of this document is ***1.3.76.21.1.50.8***.

This Certification Practice Statement (Operating Manual), hereinafter also referred to as 'CPS', is published and available for consultation online:

- at the QTSP website, *https://www.intesa.it/e-trustcom/*
- at the Agency website, *www.agid.gov.it*

Note: updated versions of this CPS (Operating Manual) may only be published with the prior authorisation of the Agency.

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

The QTSP is ***In.Te.S.A. S.p.A.***, the identification details of which are provided below.

Company name	*In.Te.S.A. S.p.A.*
Registered office address	*Strada Pianezza, 289* *10151 Turin*
Legal Representative	Chief Executive Officer
Turin Companies Register	Registration No. 1692/87
VAT number	*05262890014*
Website	*www.intesa.it*
Certified e-mail address	*intesa@pec.trustedmail.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21*

B.3. Responsibility for the Operating Manual

The responsibility for this CPS (Operating Manual), pursuant to current eIDAS regulations, lies with the QTSP INTESA, which handles its drafting and publication.

Should it be necessary to update or revise this document, Intesa will communicate this without delay to CA Auto Bank and proceed with the changes in agreement with them.

To collect observations and requests for clarification, INTESA has set up:

- an e-mail address: *marketing@intesa.it*
- Help Desk service for calls from Italy: 800.80.50.93
  for calls from abroad: +39 02.39.30.90.66

B.4. Entities Involved

Within the QTSP structure, entities involved in the processes relating to the issuance of certificates are identified.

These actors operate in compliance with the rules and processes put in place by the QTSP, carrying out the activities assigned to them within their area of competence.

B.4.1. Certification Authority (CA)

INTESA, operating in compliance with DPCM, CAD, and eIDAS Regulation, performs the activities of a Qualified Trust Service Provider. Key personnel within QTSP INTESA include

These activities include qualified trust services for the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps.

The identification details of the QTSP INTESA are provided in paragraph *B.2* above.

The personnel responsible for certification activities, in accordance with applicable regulations, are divided into the following roles:

a) Security Manager.
b) Head of Certification and Time Validation Service.
c) Head of Technical Systems Operations.
d) Head of Technical and Logistical Services.
e) Head of Auditing.

The figures listed above all belong to the QTSP INTESA organisation.

B.4.2. Local Registration Authority (LRA)

For the specific service type offered (remote qualified electronic signature within banking/financial applications) described in this CPS (Operating Manual), QTSP INTESA may delegate Registration Authority functions to CA Auto Bank via a specific mandate.

CA Auto Bank, as the LRA, commits to:

- Identifying the Holder;
- Registering the Holder.

CA Auto Bank, in exercising its function as Registration Authority, shall ensure that the recognition process is carried out in compliance with current legislation and the provisions of this CPS (Operating Manual).

In particular, CA Auto Bank, in compliance with anti-money laundering regulations, as provided for by the Fourth and Fifth AML Directives and subsequent amendments and additions, as well as by the Provisions on customer due diligence for the prevention of money laundering and terrorist financing, may identify the Holder and verify their identity with certainty (see contents of customer due diligence obligations) even if they do not physically present themselves at the Dealer (affiliated with the LRA and authorised to identify customers as defined in the affiliation agreement) or the CA Auto Bank office in charge.

C. Obligations

C.1. Obligations of the QTSP

The QTSP operates in conformity with the CAD, DPCM 22/02/2013, GDPR Regulation and eIDAS Regulation. Specifically, the QTSP:

- adopts suitable technical and organizational measures to avoid damage to others;
- ensures its Quality System complies with ISO 9001;
- ensures the signature creation device (HSM) meets security requirements (Art. 29 eIDAS);
- issues and makes public the qualified certificate, unless otherwise specified by the Holder;
- informs applicants explicitly about terms, conditions, and usage limits of signatures issued on the basis of the certification service;
- complies with security measures for the processing of personal data (GDPR);
- does not become the sole custodian of the data used to create the holder's signature;
- publishes the revocation and suspension of the electronic certificate in the event of a request by the holder or the third party concerned;
- ensures the precise determination of the date and time of issue, revocation and suspension of electronic certificates;

- keeps records, including electronic records, of all information relating to the qualified certificate for 20 (twenty) years, in particular in order to provide proof of certification in any legal proceedings;
- ensures that the identification code (exclusively pertaining to the QTSP) assigned to each Holder is unique within its user base;
- provides all useful information to those requesting the certification service on durable media. This includes: the exact terms and conditions relating to the use of the certificate, including any limitations on use, the existence of an optional accreditation system, and the complaint and dispute resolution procedures. This information, which may be transmitted electronically, must be written in clear language and provided before the agreement between the service applicant and the QTSP is concluded;
- uses reliable systems for managing the certificate register in such a way as to ensure that only authorised persons can make entries and changes, that the authenticity of the information can be verified, that certificates are accessible for public consultation only in cases permitted by the certificate holder, and that the operator can detect any event that compromises security requirements;
- records the issuance of qualified certificates in the control log, specifying the date and time of generation.

The Certification Authority provides or indicates at least one system that allows digital signatures to be verified.

In addition, the QTSP:

- generates a qualified certificate for each of the advanced electronic signature keys used by the Agency for Digital Italy to sign the public list of Certification Authorities, and publishes it in its certificate register;
- indicates an electronic signature verification system;
- keeps a copy of the list, signed by the Agency for Digital Italy, of certificates relating to certification keys and makes it accessible electronically as required by applicable legislation.

C.2. Obligations of the Holder

The applicant for a qualified certificate (Holder) for the services described in this CPS (Operating) Manual is a customer of CA Auto Bank, or a person affiliated with the latter's organisation, which acts as the Registration Authority.

The Holder will receive a qualified certificate for Remote Qualified Electronic Signatures, which can be used to sign contracts and documents relating to products and/or services offered by CA Auto Bank, in the manner described in paragraph *I. Operating procedures for signing documents*.

The Holder is required to store the information necessary for the use of their private signature key (e.g. OTP codes received on their mobile phone) in an appropriate manner and to take all appropriate organisational and technical measures to prevent damage to others (CAD, Art. 32, paragraph 1).

The key Holder must also:

- provide all information requested by the QTSP, guaranteeing its reliability under their own responsibility;
- submit the certification request in accordance with the procedures indicated in this CPS (Operating Manual);
- notify the QTSP, including through CA Auto Bank, of any changes to the information provided at the time of registration: personal details, residence, telephone numbers, e-mail address, etc.;
- store the information required to use the private key with the utmost care and diligence;
- immediately notify the QTSP, through CA Auto Bank, in the event of loss or theft of the codes and/or devices used to access their signature keys (e.g. mobile phone) so that CA Auto Bank and the QTSP can immediately block the certificate and the channels of access to them;
    - forward any requests for revocation and suspension of the qualified certificate as indicated in this CPS (Operating Manual).

C.3. Obligations of the certificate users

The user (Relying Party) is anyone who receives a digitally signed document and, in order to verify its validity, uses the Qualified Certificate used by the Holder to sign the document itself.

The verification of the digital signature and the subsequent extraction of the signed objects can be carried out with any software capable of processing signed files in accordance with the eIDAS Regulation.

Those who use a Qualified Certificate to verify the validity of a digitally signed document are required to:

- verify the validity of the certificate containing the Holder's public key of the message signatory, in accordance with the standards in force at the time of its issue;
- verify the validity status of the certificate using the OCSP protocol or by accessing the Certificate Revocation Lists (CRL);
- verify the validity of the certification path, based on the public list of QTSPs;
- verify the existence of any restrictions on the use of the certificate used by the Holder.

C.4. Obligations of the Interested Third Party

The Interested Third Party, in the services described in this CPS (Operating Manual), is represented by the companies of the CA Auto Bank group where the latter need to issue the Applicant with a qualified certificate that also contains the specific LRA data.

In such circumstances, the affiliate CA Auto Bank, in its capacity as Interested Third Party:

- verifies that the Customer meets all the necessary requirements and authorises the Customer to request the issuance of the Qualified Certificate for Remote Digital Signature;
- provides support to the Holder;
- informs the QTSP of any additional restrictions on the use of the Qualified Certificate for Digital Signature other than those provided for in paragraph *F.1.1*

CA Auto Bank or its affiliates, as Interested Third Parties, may therefore inform the QTSP of any restrictions on the use of the certificate, any powers of representation, and must communicate any changes thereto.

By way of example, the following circumstances are listed:

- change or termination of powers of representation;
- change in internal roles and qualifications;
- termination of employment.

The request for revocation or suspension by the Interested Third Party shall be immediately forwarded to the CA when the requirements on the basis of which the Holder was issued a qualified certificate for electronic signature are no longer met.

C.5. Obligations of External Registration Authorities (LRA)

For reasons related to the provision of the service, QTSP INTESA uses additional entities (hereinafter LRAs – Local Registration Authorities) throughout the EU to carry out part of the activities of the Registration Department.

QTSP In.Te.S.A. S.p.A. may delegate the function of Registration Authority to the CA Auto Bank subsidiaries of the banking group by means of a specific Mandate document.

In particular, LRAs perform the following activities:

- certain identification of the applicant for the qualified certificate;
- registration of the Holder;
- delivery to the Holder of the devices and/or codes that will allow them to access their signature key;
- sending of the signed documentation to the RA Office of QTSP INTESA, unless otherwise agreed in the Mandate.

The Mandate specifies the obligations to be complied with by CA Auto Bank, to which QTSP INTESA assigns the role of LRA and which QTSP is required to supervise.

In particular, the LRA is required to:

- ensure that the identification activity carried out complies with current legislation (anti-money laundering legislation, CAD, DPCM, eIDAS Regulation);
- enable the tracking of the LRA operator who carried out the identification of the Holder;
- use and process the personal data acquired during the recognition phase in accordance with the GDPR;
- make the material collected during the identification and registration phase available to INTESA;
- securely store the documentation collected during the identification and registration phase, then send it to the RA Office of QTSP INTESA at the request of the QTSP itself;
- allow access to its premises by QTSP personnel, or third parties appointed by the QTSP, in order to fulfil inspection (audit) obligations; such access must also be granted to auditors appointed by the Supervisory Body (AgID);
- report without delay to QTSP INTESA, through the RA Office (*uff_ra@intesa.it*) or its INTESA contacts, any event or incident relating to the points indicated above, as well as any security breaches or integrity losses that have a significant impact on the services covered by this CPS (Operating Manual) or on the personal data of the Holders.

C.5.1. Identification of the Holder

The identification process, carried out in full compliance with anti-money laundering regulations, takes place in one or more of the following ways:

- *Canonica*: the Applicant is identified in accordance with anti-money laundering regulations in person at a CA Auto Bank Dealer (affiliated with the LRA and authorised to identify customers as defined in the affiliation agreement).
- *Remote video identification*: in 'operator' mode or, alternatively, 'self + due diligence' mode, as described in more detail in paragraph *F.1.2*.

Through the above procedures, QTSP INTESA, through the anti-money laundering practices implemented by its subsidiary CA Auto Bank (banking LRA), obtains all the information required by current legislation to verify the identity of the applicant, in complete security and with full respect for privacy.

D. Liability and limitations on compensation

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

QTSP INTESA is responsible to the Holders for the fulfilment of all obligations arising from the performance of the activities provided for by the DPCM, the GDPR, the CAD and the eIDAS Regulation (and any subsequent amendments and additions thereto), as described in paragraph *C.1. Obligations of the QTSP*.

INTESA, except in cases of wilful misconduct or negligence (eIDAS Regulation, Art. 13), shall not be held liable for the consequences arising from the use of certificates for purposes other than those for which they were issued, and in particular from the failure of the Holder and the Interested Third Party to comply with the provisions of this CPS (Operating Manual) and/or from their failure to comply with current legislation.

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 the Authorities, riots or acts of war that also or only affect entities of whose services INTESA avails for the purposes of providing its certification services.

INTESA QTSP shall not be held liable for damages resulting from the improper use of the Qualified Certificate for Remote Digital Signatures in relation to the limitations of use as specified in paragraphs *F.1.1* or *F.3.1*.

After reading this CPS (Operating Manual), the Holder must take all appropriate 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/or 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 by CA Auto Bank to its Cusomers. Any tariffs for issuance, renewal, or revocation will be indicated in the contracts between the Customer and CA Auto Bank.

F. User identification and registration methods

F.1. User identification

The QTSP must verify the Applicant's identity with certainty upon the first request for the issuance of a qualified certificate. The verification of the Holder's identity by the QTSP can be carried out in the following ways:

- **De visu, remote** (only for country managers and CA Auto Bank personnel): identification is carried out via a videoconference system with quality and security characteristics evaluated by a CAB (Conformity Assessment Body) pursuant to the eIDAS Regulation (see par. F.1.2.1).
- **Electronic Identities:** by authenticating the Applicant with their electronic identity credentials notified in accordance with Art. 9 of the eIDAS Regulation (see par. F.4).

In addition to the methods indicated above, there are other cases in which the activity of certain recognition of users is delegated to CA Auto Bank which, acting as LRA and in compliance with current Anti-Money Laundering legislation, will identify and register the Holder.

In cases of long-term certificates, for subsequent renewals, if carried out when the qualified certificate is still valid, this activity must not be repeated: it will be the Holder's responsibility to communicate to the QTSP, through CA Auto Bank, any changes regarding their registration data.

In cases of one-shot certificates, the indications in the following par. F.5 apply instead.

The registration data necessary for the execution of the service object of this document are:

- Name and Surname;
- Date of birth;
- City and/or country of birth;
- Tax Code (or other unique identifier);
- Residence address;
- Personal mobile phone number;
- Email address;
- Type and number of the identity document exhibited;
- Authority that issued the document and date and place of issuance and expiration (if present).

The Applicant's personal mobile number will be used by the QTSP to send one-time numeric codes (hereinafter called OTP codes or simply OTP) capable of guaranteeing secure access to the remote signature service made available by CA Auto Bank.

In addition to the OTP, in the event the Holder uses long-term qualified certificates, all necessary information and a Personal Identification Number (PIN) will be provided, to be used in combination with the OTP as a second authentication factor.

The same PIN may be used as an *emergency code* (for example, in case of loss and/or unavailability of the OTP) to *urgently suspend* the valid qualified certificate issued to them (par. H.4).

For the use case of long-term certificates, the necessary information is also provided to the Holder to allow them to change the previously provided mobile number at any time.

Prior to the issuance of a qualified certificate, the Holder must also:

• Read the CPS (Operational Manual) of the QTSP INTESA;

• Authorize the processing of their personal data for purposes related to the issuance of a qualified certificate for electronic signature.

The documentation relating to the registration of Holders is stored for 20 (twenty) years.

F.1.1. Limitations on the use

The Qualified Certificate for digital signatures, issued as part of the services described in this Manual and offered by CA Auto Bank, includes a limitation on its use, which must be present both in the language of the country where the Applicant resides and in English.

The standard formula is as follows (in English):

> *"This certificate may only be used for unattended/automatic digital signature for the signature of documents concerning products and/or services offered or distributed by| Name of Bank or Company belonging CA Auto Bank Group".*

Any further specific usage limits may be agreed upon with CA Auto Bank.

INTESA is not liable for damages resulting from the use of a qualified certificate that exceeds the limits placed on it or resulting from exceeding such limit.

F.1.2. Remote User Identification

In compliance with current regulations, where the process of the specific CAAB subsidiary (National operating unit) foresees it, the recognition of the Holder can be performed through a remote identification procedure via webcam, in assisted mode with an operator or, alternatively, in video-self mode.

The service allows the customer to connect at the most convenient time without necessarily having to move from their location to perform this procedure.

F.1.2.1. Video identification with bank operator

This mode provides for an interaction between the applicant and the operator completely «online» and assisted, favouring the user experience and facilitating those less accustomed to the use of technologies.

It is specified that the video identification mode described in this paragraph is carried out within the scope and for Anti-Money Laundering purposes. The identification service develops as follows:

- The Applicant, possessing a device (PC, tablet, smartphone) enabled for an Internet connection and equipped with both a webcam and a functioning audio system, receives an invitation containing a link to access the recognition platform.
- The Applicant connects to the recognition platform. Within this platform, the Applicant finds a form that guides them in entering the data useful for the set-up of the video recognition process (personal data, contact data including email and mobile phone, etc.) and in the live acquisition of the images of the identification document.
- The good quality of the audio-video connection is fundamental for the identification procedure to be carried out successfully; in fact, in case of line disturbances and/or problems that make the certain verification of the Applicant's identity impossible, the operator will interrupt the session, inviting the Applicant to make a new appointment when the encountered problems are resolved..
- Once the data entry and document upload phase is completed, the Applicant can continue the session by activating the webcam connection as soon as possible.
- At the beginning of the video recognition session, the operator will identify themselves and ask the Applicant for consent to the video recording.

- During the online session (via webcam), the operator asks the applicant to present themselves with the identification documents previously sent and checks that the documents are the same, verifying that the Applicant is recognizable in the document photo. Furthermore, the operator asks the subject to perform extemporaneous actions to ascertain the real presence of the applicant at the remote station.
- During the session, the operator will verify possession and control of the email and mobile number indicated at the start of the recognition session, sending the applicant one-time codes on the two contact channels (e.g., OTP/SMS and a magic link via email) which must be verified before proceeding.
- The audio/video recording of the session must be of good quality (color image, clear and focused definition, adequate brightness and contrast, distinguishable recording of the framed ID document). The entire audio/video session must be fluid and continuous, without any interruption.

  The operator performing the identification may exclude the admissibility of the audio/video session for any reason, including the potential inadequacy of the document presented by the applicant (for example, because it is worn or lacking the listed characteristics).

The applicant's personal mobile number will then be used by the QTSP to send one-time numeric codes (OTP) capable of guaranteeing secure access to the remote signature service made available by CA Auto Bank.

F.1.2.2. Video identification with QTSP operator (for country managers and bank personnel)

For the issuance of long-term certificates in favor of country managers and CA Auto Bank personnel, the identification mode described in the previous paragraph F.1.2.1 can be used with QTSP operators who will carry out the activity in compliance with the eIDAS Regulation. In this case, the following steps apply in addition:

- During the document acquisition phase, the video recognition platform allows the Applicant to choose the PIN and the emergency code that they can use with the certificate that will be released at the end of the recognition; furthermore, the privacy policy, process information, Operating Manual, and any Policies related to certificate use are shown and made available, and relative consents are mandatorily collected.
- Once the checks relating to the presented ID documents are completed, the Applicant is given the necessary information to allow them, subsequently, to use the qualified certificate that will be issued.
- In particular, it is illustrated how to use, for signature purposes, the OTP/SMS received on the mobile number registered and verified during the video recognition session and the Personal Identification Number (PIN), to be used in combination with the OTP as a second authentication factor.
- At the end of the process, the signature certificate is issued by the Certification Authority, and the Applicant, now Certificate Holder, is also associated with a unique identifier at the QTSP.

The entire session is recorded in audio and video mode, and the sequence is then encrypted with a public key made available by the Certification Authority. The CA itself keeps the private key and makes it available only in case of litigation to a party expert and/or supervisory bodies requesting a check on the activities performed. The audio/video traces are kept by QTSP INTESA for 20 (twenty) years.

F.1.2.3. Video identification in "Self & Due Diligence" mode

As an alternative to the video recognition described in previous paragraphs, a possible video identification mode is represented by the “self + due diligence” mode.

Due Diligence means the possibility, by CA Auto Bank, to adopt the practices foreseen by the legislation regarding identity verification pursuant to Directive (EU) 2018/843 and subsequent amendments, including the relative implementations at the level of individual Member States.

This specific identification case involves integrating the video self within the banking due diligence process so that, in addition to the execution of the video self, a reinforcing action in the banking/financial scope regarding the Applicant is conceivable.

Such action, being carried out within a regulated and secured context, such as that of AML due diligence processes, is functional for confirming the Applicant's identity and their will to obtain the certificate.

The process provides that the user, during the identification phase, is guided by the system to perform a series of steps within a recorded video session.

The Applicant will be required to:

- Upload or photograph their identity document for acquisition (personal data and photo);
- Verify the email address and mobile number via OTP and/or Verification Link;
- Record their own face via a *video selfie* (for biometric comparison), simultaneously performing some guided random actions of the face, aimed at verifying *liveness*. The stream will subsequently be analyzed using facial recognition algorithms to detect face movements.

The verification process occurs automatically, through a *Face Recognition* algorithm, for biometric matching between the ID document photo and the face recording (via some frames).

In *unattended* mode for the applicant, a series of checks are then performed, including:

- Check on personal data;
- Verification of legibility and authenticity of acquired ID document images and comparison between Video Self frames and the photo on the ID document;
- Comparison between data entered in the portal and those reported in the loaded ID documents;
- Verification of liveness

Below are the possible reinforcing actions foreseen by CA Auto Bank and its subsidiaries to support the Holder's identification:

- Acquisition of identification data and verification against a valid identity document of which a copy is acquired;
- Acquisition of a copy of the card containing the tax code or other unique code to ensure uniqueness for the user's registry, if foreseen in cases of high-risk assessment;
- Acquisition of an additional valid identification document of which a copy is acquired in cases of high-risk assessment;
- Acquisition of a copy of income document (where requested in case of financing);
- Verification of the email account via One Time Password (OTP) sent via email or other one-time verification code (e.g., magic link);
- Asynchronous data check performed by an operator, if foreseen by applicable law;
- Where foreseen, checks via authoritative third-party sources on acquired data and documents.

Through this identification model, the prospect customer of the CA Auto Bank group company is able to access a bank's services and sign an account opening contract or product purchase with a qualified certificate issued after a video-self procedure, which is then perfected at the end of the operations falling within normal activities for the correct completion of due diligence pursuant to current AML legislation.

In addition to the above, the identification and issuance process must provide that:

1. Such certificate contains stringent usage limits;
2. The contract signed with such certificate remains at the disposal of the bank alone until further checks aimed at the certain identification of the Applicant are completed, within the scope of due diligence procedures adopted by CA Auto Bank and described in AML policies;
3. The checks aimed at certain identification of the Applicant referred to in point 2 do not involve the use of the previously issued certificate;
4. Such certificate may be used only for signing the opening of an account;
5. The use of the certificate itself is inhibited until the checks in point 2 are completed;
6. If the onboarding process is not completed, the contract must be destroyed.

In case of a positive outcome, the video will be accepted by the system; otherwise, the user will be invited, in scenarios where it is foreseen, to perform video identification with an operator, if available, or to go to the intermediary's offices to perform due diligence, and the video will be deleted.

Note: The identification method described in this paragraph is not permitted in the German market. Customers of German entities must rely on the alternative methods described in this manual that comply with local BaFin standards.

Where available, customers of German entities may complete a remote customer identification procedure through access to the customer's online banking account. Such procedure is supplemented by a video-based selfie process incorporating facial recognition technology and real-time interaction (liveness) controls for the purpose of biometric verification, in accordance with applicable regulatory requirements.

F.1.3. Identification performed by CA Auto Bank in de visu mode

In addition to the identifications previously described, Intesa may delegate the activity of certain identification to CA Auto Bank in *de visu* (face-to-face) mode.

Identification must occur in conformity with par. *B.4.2*, that is, in line with relevant AML legislation (in accordance with the regulations governing identity verification pursuant to Directive (EU) 2018/843, as amended, in compliance with the relevant implementations at the level of individual Member States, as well as the Joint Guidelines of the European Supervisory Authorities, issued pursuant to Article 17 and Article 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence measures) and must be completed and perfected before the qualified certificate is issued.

CA Auto Bank will apply and verify the correct completion of the following measures, applicable depending on the product and the operation chosen by the customer:

- Acquisition of identification data and verification against a valid identity document of which a copy is acquired;
- Acquisition of a copy of the card containing the tax code or other unique code, if foreseen, in cases of high-risk assessment;
- Acquisition of an additional valid identification document of which a copy is acquired in cases of high-risk assessment;
- Acquisition of a copy of income document (where requested in case of financing);
- Where foreseen, checks via authoritative third-party sources on acquired data and documents;

Finally, for clients for whom one of the previous checks fails or presents anomalies, supplementary documentation will be requested.

F.2. Registration of users requesting certification

Following the phase of certain identification, the registration of Holders' data is performed in the Certification Authority's archives.

This operation may be performed via a software application directly callable from CA Auto Bank applications.

Without prejudice to the certain identification of the Holder, where in the registration phase there are material errors in the data acquired for the Holder's registration, preparatory to certificate issuance, the latter will be revoked and one will be re-issued after correction of registration data.

In cases where the certificate is of the *one-shot* type, revocation will not be performed due to technological constraints deriving from international standards underlying X.509 certificate management.

F.3. Digital signature certificates in particular closed user groups

It is possible to issue a qualified electronic signature certificate before the identification of the Holder is concluded only in case of special circumstances attributable to limited uses of digital signature in closed user contexts that do not allow the generated digital signatures to produce any legal effect if the verification of the certificate Holder's identity does not end with a positive outcome.

This possibility was confirmed by AgID with communication to CAs dated June 7, 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", having as its subject matter "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*" (Request for clarification regarding the use of digital signatures in specific closed user environments).

Specifically, this use case addresses the issuance of the Qualified Certificate in circumstances attributable to limited uses of qualified electronic signature in closed user contexts, where signatures do not produce legal effects until the Holder identification verification is successful.

Typically, this is the case where the object of subscription is a deed requiring the subscription of two or more parties, without which it is *juridically imperfect*.

This type of certificate, in full compliance with the provisions contained in AgID communication 0016101.07-06-2016, in the presence of certain domain restrictions and areas of use, allows the use of digital signatures before completing the due process of identity verification of the Holder, under the following conditions:

Restriction	Liability
1. The process is attributable exclusively to remote signature systems;	Certification Authority
2. Use must occur in closed user groups;	Certification Authority
3. The qualified certificate must contain stringent usage limits regarding the specific relationship between Holder and co-interested/co-signer (par F.1.1);	Certification Authority
4. The certificate must be clearly distinguishable from those issued using more traditional procedures. The Holder's qualified certificate must contain a specific OID, which can be found in the CPS (operating manual), where this particular process and its restricted scope are described (par. F.3.2);	Certification Authority
5. Stringent application limits must exist. The application must limit objects of subscription to documents proposed by the co-interested and co-signer party. Documents must be juridically imperfect (e.g., contracts for service adhesion) until signed by the co-interested and co-signer party;	Co-interested and Co-signer
6. If Holder identity verification is made through a face-to-face meeting, the verifier must be personnel of the certification authority or delegated by it, but not of the co-interested and co-singer party if different from the certification authority;	Certification Authority
7. The co-interested and co-signer party may perform identity verification on behalf of the certification authority, through audio-video sessions, and approved by AgID, or in application AML legislation, where applicable.	Co-interested and Co-signer
8. Upon affixing the Holder's signature, the Certification Authority commits not to affix the time stamp.	Certification Authority
9. Upon affixing the Holder's signature, the Co-interested and Co-signer party commits not to affix the time stamp.	Co-interested and Co-signer
10. The time stamp must be affixed mandatorily after the signature of the co-interested and co-signer party which makes the deed juridically perfect;	Co-interested and Co-signer
11. Until the signature and timestamp in point 10 are affixed, the object signed by the Holder alone must not be provided to anyone and, if identity verification fails, must be destroyed keeping track of events in special logs. In this case, as a measure to better protect the Prospect Customer, the certificate is revoked.	Co-interested and Co-signer

F.3.1. Specific limitation on the use

To comply with point 3) of paragraph *F.3*, the same limitation son the use described in paragraph *F.1.1* may be used, bearing in mind the same considerations defined therein.

F.3.2. Specific OID

To comply with point 4), the certificate issued under these conditions can be distinguished from other certificates in that it contains one of the following OIDs in the field (each defined with reference to the root CA that issued the certificate):

- ***1.3.76.21.1.3.1***.1.1
- ***1.3.76.21.1.5.1***.1.1
- ***1.3.76.21.10.2.1***.2.1

For further information on the OIDs used by the QTSP, please refer to the CPS - Certification Practice Statement and CP - Certificate Policy for Qualified Electronic Signature and Electronic Seal Certificates, published at the following URL *https://www.intesa.it/e-trustcom/*.

F.4. Electronic Identities

F.4.1. Identification via electronic identity notified pursuant to Art. 9 of the eIDAS Regulation

Pursuant to Art. 24, par. 1-bis, letter a) of the eIDAS Reg., QTSP INTESA can comply with the identity verification of the Applicant through an authentication process with notified electronic identity.

In this case, the identification of the Applicant is performed by relying on a notified electronic identity having an assurance level of at least “high”, as defined under the eIDAS framework. Such level guarantees a very high degree of confidence in the claimed identity of the natural person, as it is based on strong identity proofing procedures, secure credential issuance, and robust authentication mechanisms.

The Applicant, after entering the credentials foreseen by the notified electronic identity scheme, performs authentication on the Certification Authority's or Identity Provider's portal. Upon successful authentication, the system receives a set of validated identity attributes transmitted by the notified scheme (e.g. name, surname, date and place of birth, and, where applicable, unique identifiers).

The system then performs consistency checks between the identity data received from the notified electronic identification scheme and the data entered in the digital certificate request. Such verification ensures that the identity attributes are uniquely associated with the Applicant and that there is no discrepancy that could undermine the identification process.

F.4.2. Identification via notified electronic identity at “substantial” assurance level – complementary verification requirements

Where the Applicant’s Member State makes available a notified electronic identity scheme at “substantial” assurance level (LoA Substantial), as defined under Regulation (EU) No 2015/1502, such scheme may be accepted for the purpose of identity verification pursuant to Art. 24, par. 1-bis, letter c) of the eIDAS Regulation, provided that the authentication is combined with additional complementary verification measures that, taken together, ensure a level of confidence equivalent to that required for the issuance of a qualified electronic signature certificate.

In such cases, the authentication via the notified electronic identity at “substantial” level constitutes one element of the overall identity verification process. CA Auto Bank S.p.A., acting in its capacity as LRA, is required to supplement the authentication with additional control measures within its onboarding processes. Such complementary measures shall include, by way of example and without limitation:

- acquisition and verification of a valid identity document, with systems that assess its integrity, authenticity and consistency with the Applicant’s personal data;
- intervention of a qualified operator in back-office, in the operational flows that provide for it;
- query of authoritative databases available in the relevant Member State for cross-checking identity data (equivalent to SCIPAFI or similar national registers);
- ongoing monitoring of the relationship and KYC/AML compliance obligations pursuant to applicable Member State legislation implementing Directive (EU) 2015/849 and subsequent amendments.

The evidence collected in the course of such controls shall be retained by CA Auto Bank S.p.A. for 20 years and made available to the QTSP upon request in the event of an audit. The qualified certificate shall be issued only upon positive completion of both the "substantial" level authentication and the complementary verification measures described above.

For the avoidance of doubt, where the notified electronic identity scheme available in a given Member State reaches an assurance level of "high", the procedure described in section F.4.1 applies directly, without the need for additional complementary measures.

F.5. Identification via credentials used for a previous one-shot certificate

In this mode, the Certification Authority relies on the identification already performed during the issuance of a previous one-shot certificate.

Two types of cases can be identified:

- **a)** The one-shot certificate, issued using the credentials of a previous one-shot certificate, is issued within the same session or signature process in which the previous one-shot certificate was issued.
- **b)** The one-shot certificate, issued using the credentials of a previous one-shot certificate, is issued in a different session or signature process.

In case a): The Applicant, possessing the email and mobile number certified by the Certification Authority during the previous release, can request the new one-shot certificate only after receiving, on the certified email and mobile, the new One-Time codes, which must be verified by the Applicant for the issuance and use of the new certificate, provided that this takes place within the same session or signing process.

In case b): The Applicant, already possessing credentials provided by the Certification Authority or LRA, authenticates to the portal and requests a new one-shot certificate, subject to confirmation or update of registration data. Certified email and mobile cannot be changed. In this case, the Holder must insert the OTP sent to their device (or SMS on the mobile phone) and authorization must be given by the LRA or Interested Third Party.

In both cases, the OTP authentication system is under the control of the CA.

If the Certification Authority, during the previous issuance, certified the possession of *Strong Customer Authentication (SCA)* instruments, such SCA credentials may be used in place of One-Time codes sent by email and mobile phone in *case a)*, or to access the reserved area and send OTP/SMS in *case b)*.

G. Generation of Certification, Time Validation, and Subscription Keys

G.1. Generation of certification keys

Key generation inside signature devices occurs in the presence of the Certification Manager.

This operation is preceded by the initialization of signature devices for the certificate generation system with which the certificates of the Holders and those of the time validation system are signed.

Everything occurs in dual control mode to avoid illicit operations.

Operations subsequent to the generation of certification key pairs are possible only through particular authorization devices (USB tokens): privileged access to HSMs is executable only through keys contained in such devices. For greater security, such keys are divided over multiple devices (logic type "n of m"), so that only the concomitant presence of at least *n* of *m* parts of the key allows operating with privileges. They are kept in separate safes.

Key length complies with regulations in force from time to time.

G.2. Generating time stamp system keys

Time-stamp keys are generated in accordance with applicable legislation.

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

G.3. Generation of signing keys

Once the registration phase – during which the Holder's data is saved in QTSP INTESA's files – is completed, it is possible to proceed with the generation of signing keys.

The Holder may start the key generation procedure and request for the associated Qualified Certificate in one of the modes described in par. *I. Operating procedures for signing documents*.

Subscription key pairs are created on secure signature devices (*HSM – Hardware Security Module*), compliant with specifications in *Annex II* of the eIDAS Reg.

The signing key pairs 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 legislative provisions, 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 applicable legislation.

The Certification Authority generates a qualified certificate for each of the qualified electronic signature keys used by the Agency to sign the public list of CAs and publishes it in its certificate register. The CA must then keep a copy of the list, signed by the department, of the certificates relating to the certification keys and make it available electronically.

H.2. Procedure for issuing signing certificates

QTSP INTESA issues certificates using a system that complies with regulatory standards.

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 to the QTSP Certification Authority.

The generation of certificates is recorded in the Audit Journal.

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 Qualified Certificate clearly identifies the Certification Authority that issued it and contains the data required to verify the digital signature.

Each Qualified Certificate also comply with the eIDAS Regulation and follows the guidelines set out in the AgID Resolution no. 147/2019 ((*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificate - Guidelines containing technical standards and recommendations regarding generation of certificates*).

All Qualified Certificates issued as part of the services described in this Manual includes at least one limitation on its use (par. *F.1.1*, or par. *F.3.1* for the types of signature referred to in par. *F.3*).

H.3.1. Certificates with limited validity (“one shot”)

For certain processes, typically related to the onboarding of prospective customers, but not exclusively, QTSP Intesa offers a remote qualified electronic signature service, generated on HSM, compliant with regulations, through the use of a qualified certificate with limited validity: maximum 30 minutes from issue or as otherwise agreed with the LRA/Interested Third Party.

In addition to strict time constraints, these certificates are also subject to application constraints that limit their use to documents proposed by the LRA and to usage limits (par. F.1.1) that restrict their legal validity for the purposes of signing the aforementioned documents.

For remote signing using these certificates, it is possible to use online applications that operate through the services provided by the CA or the LRA. In the latter case, the CA shall ensure that the system managed by the LRA guarantees the exclusive knowledge of the data for the creation of the signature by the Holder thanks to appropriate security requirements.

The CA provides web services to enable integration with applications requesting signature services. It is understood that the documents to be signed are normally created by these applications depending on specific requirements.

Given the short duration of one-shot certificates and the strict application and usage restrictions, the user's signature request is authenticated through the OTP/SMS credential component known to the Holder.

H.4. Emergency Code

The Certification Authority guarantees, in accordance with applicable regulations, an *emergency code* to be used to request the ***urgent suspension*** of a Qualified Certificate that is still valid.

In the applications described in this CPS (Operating Manual), the PIN chosen by the Holder at the time of registration may also be considered an emergency code.

I. Operating procedures for signing documents

QTSP INTESA, through the services of CA Auto Bank, makes available to Holders what is necessary to generate qualified electronic signatures in conformity with current legislation.

The particular type of service does not require the provision of a signature application to be installed on one's personal computer, but rather signature functionalities callable either by accessing the reserved area of the CA Auto Bank portal, or directly at the counter of a CA Auto Bank branch/dealer.

The qualified electronic signatures obtainable through these procedures will be absolutely compliant with what is foreseen by applicable legislation regarding the algorithms used.

Furthermore, such documents, as required by regulations, will not contain macro-instructions or executable codes capable of activating functionalities that could, unbeknownst to the subscriber, modify acts, facts, and data represented in the documents themselves.

The different authentication modes are described below which, in compliance with current legislation, allow a Holder, once registered, to proceed with affixing qualified electronic signatures.

To complete and confirm the performance of signature operations, SMSs will be sent. Should the Holder have a smartphone enabled for reading correspondence, upon the Holder's request, alternatively, emails may be sent in place of SMSs.

I.1. Signature Process in Unattended Stations (Home banking)

After having correctly completed certain identification according to the procedures described in this CPS (Operating Manual) and having registered their identification and contact data (email and mobile), the Holder may, at a later time, request their digital certificate and then proceed to sign a document according to the methods described below.

This procedure is currently applicable only to one-shot certificates.

The list of steps performed for affixing the signature is described below:

1. The Holder receives an email at the email address registered at the time of identification.
   The email contains an invitation (URL) that redirects the user inside a portal where the set of documents constituting a specific file/dossier is shown, which must be viewed before proceeding to their subscription.
2. The aforementioned portal, before allowing access, and thus the viewing of the content of the document(s) constituting the dossier, requires the user to enter their own National Identification Number (e.g., tax code or other unique identification data of the holder issued by the State of belonging) and the mobile number registered at the time of identification.
3. The user, once the information indicated above is entered and correctly verified, accesses a page that allows them to see the content of the document(s), navigate it/them, and have full awareness of all points where their signature is required.
4. Once the user, having taken note of the content of the document(s), activates the signature function, an OTP/SMS is sent to the number registered during the identification phase.

   Only when the user has entered the OTP code inside the mask shown by the portal, will the signature process proceed to the generation of a one-shot qualified certificate for automatic signature, characterized by a very limited time duration (par. *H.3.1*), which will be used to affix the qualified electronic signature exclusively on the set of documents previously viewed and approved by the user in the masks referred to in point 3.

Should there be more than one file/dossier to sign, the Holder must reiterate steps 1 to 4 for each file/dossier.

I.2. Signature Process in Attended Stations (CA Auto Bank Banking Group Dealer Counter)

The Holder may proceed to the subscription of a document also at a counter of a Dealer of the companies belonging to the CA Auto Bank banking group.

This use case is applicable exclusively to one-shot certificates.

The list of steps performed for affixing the signature is described below:

1. The user presents themselves at the counter of a CA Auto Bank branch (attended station) and is recognized according to banking anti-money laundering regulations, by an operator assigned to perform identity verification pursuant to AML.
2. Once certain identification pursuant to AML is completed, the operator, after asking for confirmation and registering the Holder's identification data, as well as contact data, prepares and displays to the Holder the file/dossier containing the set of documents to be signed; such visualization occurs within the devices used by the intermediary for performing activities related to AML procedures.
   Since these are devices normally adopted for access to procedures allowing the performance of AML practices, such devices guarantee high security standards.
3. The Holder views the content of the documents to be signed and provides their consent to proceed with subscription. Consent is made explicit by clicking or tapping the individual signature points.
4. Having received the Holder's consent, the operator activates the OTP/SMS sending function on the mobile number registered in the identification phase (steps 1 and 2).
5. The Holder receives the OTP on their mobile and then enters it into the mask displayed by the page on which, a few moments earlier, they had viewed the documents to be signed and revealed their consent to proceed (step 3).
6. After OTP insertion (and its correct verification), the signature process will proceed to the generation of a one-shot qualified certificate for automatic signature, characterized by a very limited time duration (par. *H.3.1*), which will be used to affix the qualified electronic signature exclusively on the set of documents previously viewed and approved by the user in the masks referred to in step 3.
7. Should there be more than one file/dossier to sign, the Holder and the Operator must reiterate steps 2 to 6 for each file/dossier.

I.3. OTP/SMS Type Authentication

This authentication mode requires the user, already previously identified, to use their mobile phone (same number provided and registered in the identification phase) to be able to receive a one-time code (OTP) from the QTSP.

Such OTP must be entered in the signature application in order to confirm one's identity and willingness to sign the specific document.

Upon receipt of the aforementioned OTP, its correctness is verified and, in case of a positive outcome, the qualified electronic signature operation is authorized.

Therefore, when the Holder wishes to sign a document by accessing via the signature portal made available by the Bank, in the case of a one-shot certificate, they will authenticate through the insertion of an OTP received via SMS on the telephone number that only the user possesses. In the case of a three-year certificate, the Holder, in addition to the aforementioned OTP/SMS, must also enter a PIN (information that only the user knows) chosen during the certificate enrollment phase.

J. Operating procedures for verifying signatures

The documents signed with the methods described previously will be exclusively in PDF format: this subscription format is indeed considered easy to use within banking or financial applications.

The verification of signed documents can be easily performed using the software *Acrobat Reader DC*, an application capable of verifying all types of qualified electronic signature in PDF format produced in the European Union in conformity with the eIDAS Regulation.

Acrobat Reader DC is downloadable for free from the Adobe website, *www.adobe.com/it/*

K. Procedure for revoking and suspending certificates

In conformity with the eIDAS Reg., information on certificate status is available via OCSP protocol, at the URL indicated on the certificate itself.

Revocation and suspension of certificates can also be asserted by their inclusion in the CRL list. The CRL profile is compliant with the RFC 5280 standard. Such list, signed by the Certification Authority issuing the certificate, is updated with pre-established periodicity and compliant with current legislation.

The CRL list is also available on the certificate register.

In cases where revocation or suspension occurs on the initiative of the Certification Authority or the Interested Third Party, the Certification Authority notifies the Holder of the request and the moment when the requested event will come into force.

In the request phase, the date and time starting from which the certificate will result revoked will be specified.

K.1. Revocation of certificates

A valid certificate may be revoked upon request of the Holder, the Interested Third Party, or the Certification Authority (i.e., the QTSP).

The revoked certificate cannot be reactivated in any way.

K.1.1. Revocation at the Holder's request

The Holder may request revocation by accessing a specific section made available within the scope of CA Auto Bank services or by contacting CA Auto Bank Customer Service directly.

The QTSP, notified by CA Auto Bank, which in the meantime will have also blocked the Holder's access codes, will provide for the immediate revocation of the certificate.

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

In cases where CA Auto Bank is configured as an Interested Third Party, it may request the revocation of the certificate.

The QTSP, having ascertained the correctness of the request, will give notice of the revocation to the interested Holders using the communication channels defined with the Holder at the time of registration or subsequently updated and communicated by the Holder to the QTSP, also by means of CA Auto Bank (par. *C.2. Obligations of the* Holder).

K.1.3. Revocation at the QTSP's request

The QTSP intending to revoke the Qualified Certificate, barring cases of motivated urgency, gives prior communication via email or PEC to CA Auto Bank (Interested Third Party cases) and simultaneously communication will be given to the Holder using the email address provided in the certificate request phase or at the residence address, specifying the reasons for revocation as well as the date and time starting from which revocation is effective.

K.1.4. Revocation of certificates relating to CA keys

In the event that:

- the CA key has been compromised,
- the relevant activity ceases,

the QTSP will proceed to revoke the CA certificates 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. (for example in cases where loss/theft of the OTP Token is feared, or checks must be made to have certainty of the effective cessation of the Holder from the duty for which the certificate was issued to them, etc.).

A suspension request may be made by all entities foreseen by applicable legislation (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.

Suspension of certificates is applicable only to valid certificates.

K.2.1. Suspension at the Holder's request

The Holder may request suspension of the certificate by accessing a specific section made available within CA Auto Bank's services, or by contacting CA Auto Bank's Customer Service directly.

The Certification Authority proceeds to suspension which will be communicated to the Holder using specific functions made available within CA Auto Bank services or portals.

The Holder may subsequently request the reinstatement of the certificate according to methods always made available by CA Auto Bank.

In the absence of further notification, the suspended certificate will be revoked automatically at the end of the suspension period, and the revocation date will coincide with the effective date of suspension.

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

In cases where CA Auto Bank is configured as an Interested Third Party, it may request certificate suspension.

The QTSP, having ascertained the correctness of the request, will promptly suspend the certificate and give notice of the suspension to the interested Holders using the communication channels defined with the Holder during the registration phase or subsequently updated and communicated by the Holder to the QTSP, including through CA Auto Bank (par. *C.2. Obligations of the Holder*).

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, or at the residence address, specifying the reasons for the suspension and the date and time from which the suspension will be effective.

In the case where the certificate foresees an Interested Third Party, a similar notice will also be sent to the latter by the QTSP.

L. Method for replacing keys

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

The qualified electronic signature certificates issued by the Certification Authority within the contexts described in this CPS (Operatig Manual) are of two types:

a) **Long term**: duration of 36 (thirty-six) months from issuance

b) **One shot**: duration limited to maximum 30 (thirty) minutes from issuance or as otherwise agreed with the LRA / Interested Third Party.

At the end of the aforementioned periods, in case one intends to proceed with the renewal of the certificate, the generation of a new pair of subscription keys and simultaneously the issuance of a new certificate will become necessary.

In this case, the procedure followed for the issuance of the new certificate will be similar to that indicated in the first release phase, net of the Holder identification phase which will not have to be repeated if the procedure is performed before the expiration of the certificate.

L.2. Replacement of QTSP keys

L.2.1. 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 *P Disaster Management Procedure*.

L.2.2. 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 by applicable legislation.

L.2.3. Replacement of Time stamp system keys (TSA)

Regarding the replacement of time validation system keys, the same indications contained in the analogous section of the *Intesa Operational Manual* published on the QTSP portal apply: https://www.intesa.it/manuali-operativi-e-trustcom/.

M. Certificate Directory

In the certificate directory, INTESA publishes:

- The certificates of subscription keys and of the time validation system.
- The certificates of certification keys (CA and TSCA).
- The certificates issued following the replacement of certification keys.
- Certificates for the signature keys of the Agency for Digital Italy.
- The revocation and suspension lists (CRL).

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

Authorized staff enabled for direct management of the certificate directory may access the room where systems are installed and operate on them only in dual control mode to avoid illicit actions.

N. Personal data protection procedures

Security measures for the protection of personal data are compliant with measures foreseen by European Regulation 679/2016 (GDPR) and subsequent amendments and integrations.

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 par. *M*.
- 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 QTSP certification service.
- DIGITAL ARCHIVE OF TIME STAMPS, contains the time stamps generated by the TSA system.
- 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.

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

P. Disaster Management Procedure

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 but definitive one.

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.

Q. Procedure for applying and defining the time reference

Regarding the modes for affixing and defining the time reference, the same indications contained in the *Intesa Operating Manual* published on the QTSP portal apply.: https://www.intesa.it/manuali-operativi-e-trustcom/.

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 CPS (Operating Manual).

Except for cases foreseen in par. F.3, the affixing of said stamp is a process integrated with the signature operation and does not require any specific activity by the Holder.

The verification of the affixed time stamp is contextual to the verification of the signature.

R. Lead Time and RACI table for issuing certificates

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 for Certificate Issuance vs. LRA*	*CA Auto Bank (acting as) Local RA*	*Issues Certificate publication order vs CA after ID verification*	*Certification Authority*	*Processing Certification Request*
Certificate User, Applicant, Holder	*Request for Certificate Revocation / Suspension vs. RA or LRA*	*Intesa (acting as) Registration Authority (RA) o CA Auto Bank (acting as LRA)*	*Issues Certificate Revocation / Suspension order vs CA after ID verification*	*Certification Authority*	*Processing Revocation / Suspension Request*
Certificate User, Applicant, Holder	*Request for Certificate Reactivation vs. RA or LRA*	*Intesa (acting as) Registration Authority (RA) o CA Auto Bank (acting as LRA)*	*Issues Certificate reactivation order vs CA after ID verification*	*Certification Authority*	*Processing Reactivation Request*

Below is a RACI Table 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 References

ETSI-319.401	ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.412-1	ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 - 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 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC 5905	Network Time Protocol (Protocollo NTP)
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 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

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