POLICY AND PRACTICE ST

SSAS Policy
SSAS Practice Statement

DOCUMENT CODE	ICERT-INDI-SSAS
VERSION	1.0
DATE	16 March 2026

tinexta
infocert

SUMMARY

1.1 General overview — Remote qualified signature service

The remote qualified electronic signature service enables the subject of a qualified certificate to generate qualified electronic signatures or seals using a qualified signature creation device (**QSCD**) remotely, whereby the private signature key is generated and stored within the QSCD itself in a secure environment by the Qualified Trust Service Provider (QTSP), which manages the keys on behalf of the signer.

In the remote signature model, the private key associated with the qualified certificate is not held directly by the signer on a personal physical device, but is stored and protected within a cryptographic system managed by a qualified trust service provider. The service is designed to ensure that the private key cannot be exported and that its use is restricted exclusively to signature activation mechanisms that guarantee the signer's sole control.

In particular, the system ensures that:

- the signature key pair is generated in a secure environment within the remote QSCD;
- the private key cannot be exported and is protected against unauthorised access;
- the use of the key is subject to the signer's authentication and an explicit request for a signature;
- appropriate tracking and control measures are in place to support security checks and audits.

The service is provided in accordance with the Regulation [1] and subsequent amendments, as well as the applicable technical standards, including ETSI TS 119 431-1, which sets out the security, management and operational requirements for remote signature systems and signature activation mechanisms, as well as ETSI EN 319 401 and DS/EN 419241-1:2018.

This policy and practice statement describes the policies, practices, security measures and controls adopted by Tinexta Infocert to ensure the correct generation, protection and use of signature keys in the context of the qualified remote signature service, as well as the reliability of the service and compliance with the principle of the signer's sole control.

The structure of this document is aligned with the IETF RFC 3647 framework – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – which is used as a guide.

1.2 Document name and identifier

This document is identified by the document code **ICERT-INDI-SSASP**. The version and release level are shown in the header of each page.

Specific Object Identifiers (OIDs) are associated with the document,

The Object Identifier (OID) identifying Tinexta Infocert is: 1.3.76.36.

The policies relating to remote qualified electronic signature services are as follows:

Description	OID
Policy and Practice Statement – Qualified Remote Signature Service – One-time signing key	1.3.76.36.1.1.4000.1 compliant with the EUSPv2 policy 0.4.0.19431.1.1.4
Policy and Practice Statement – Qualified Remote Signature Service	1.3.76.36.1.1.4000.2 compliant with the EUSPv2 policy 0.4.0.19431.1.1.4
Policy and Practice Statement – Qualified Automated Remote Signature Service	1.3.76.36.1.1.4000.3 compliant with EUSPv2 policy 0.4.0.19431.1.1.4
Policy and Practice Statement – Qualified Remote Seal Service	1.3.76.36.1.1.4000.4 compliant with EUSPv2 policy 0.4.0.19431.1.1.4

Table 1 – Policy for qualified electronic signature services

1.3 Participants and responsibilities

1.3.1 SSASP – Qualified Signature Activation Service Provider

The Signature Activation Service Provider (SSASP) is the entity that provides the remote qualified electronic signature service, ensuring the generation, safekeeping and activation of private signature keys within a remote qualified signature creation device (remote QSCD).

The service is provided in accordance with the Regulation [1] and subsequent amendments and additions, which governs the security, management and operational requirements of remote systems for the creation of qualified signatures.

Tinexta Infocert S.p.A. operates as a qualified SSASP, ensuring that:

- the signature key pair is generated in certified cryptographic modules;
- the signature key pair is generated in a secure environment;
- the private key cannot be exported;
- the keys are stored in certified cryptographic modules;
- the use of the private key is subject to the Subject's authentication;
- the Subject's exclusive control over the initiation of the signing process is guaranteed;
- all relevant operations are logged and subject to security measures and audits.

The full details of the organisation acting as the SSASP are as follows:

Company name	**Tinexta Infocert – Public Limited Company** **A company subject to the management and coordination of Tinexta S.p.A.**
Registered office	**Piazzale Flaminio 1/B, 00196, Rome (RM)**
Operational offices	**Via Marco e Marcelliano 45, 00147, Rome (RM) Via Fernanda Wittgens 2, 20123 Milan (MI)**

	Piazza Luigi da Porto No. 3, 35131 Padua (PD)
Legal representative	**Danilo Cattaneo – in his capacity as Managing Director**
Telephone number	**+39 06 836691**
VAT number/Tax code	**07945211006**
Company Registration No.	**Business Register No. 07945211006** – *REA No.* **RM – 1064345**
Website	**https://www.infocert.it**

The SSASP operates in coordination with the Certification Authority with regard to the issuance and management of the qualified certificate associated with the signature keys.

For the purposes of this policy and practice statement, the Certification Authority may be Infocert itself or an external QTSP.

1.3.2 Certification Authority – Certification Authority

The Certification Authority (CA) is the body responsible for issuing, publishing, suspending and revoking the qualified certificates associated with the signing keys generated and stored in the remote QSCD. For details of this role, please refer to the Certification Authority policy and practice statement.

The CA:

- verifies the identity of the Party in accordance with the procedures set out in Article 24 of the Regulation
  [1] in its current version
- issues the qualified certificate containing the public key corresponding to the private key held in the remote QSCD;
- ensures compliance with the requirements laid down by current legislation and applicable standards.

The CA and the SSASP operate in a coordinated manner but with distinct roles:

- the CA is responsible for linking the subject's identity to the public key;
- the SSASP is responsible for the protection and activation of the private key.

1.3.3 Registration Authority (RA)

Registration Authorities (RAs) are bodies delegated to carry out the identification of the subject, the collection of applications for the issue of qualified certificates and authentication for the remote signature service.

RAs may, amongst other things, carry out the following activities:

- identifying the Subject or the Subscriber,
- recording the Subject's data,
- forwarding the Subject's data to the CA's systems,
- collecting the application for a qualified certificate,

- initiating the public key certification procedure;
- support during the suspension, revocation or renewal of the certificate and the service.

RAs operate on the basis of a mandate granted by the qualified service provider and in accordance with the procedures described in this Manual or in that of the CA.

1.3.4 Subject or Signer

The **Subject** (or Signer) is the natural or legal person with whom the following are associated:

- the pair of signing keys generated in the remote QSCD;
- the qualified certificate containing the public key corresponding to the private signature key.

In the context of the remote signature service, the signer exercises exclusive control over their private key through the strong authentication and activation mechanisms provided by the system.

1.3.5 User or Relying Party

This is the party that receives an electronic document signed with a qualified electronic signature generated via the remote service and that relies on:

- the validity of the qualified certificate;
- on the reliability of the remote signing service; on compliance with the security requirements and exclusive control stipulated by the applicable legislation.

1.3.6 Subscriber

The subscriber is the natural or legal person who requests the activation of the qualified remote signature service on behalf of the Subject, possibly bearing the costs in their capacity as a QTSP Customer. Where applicable, this role may also be assumed by the RA.

The Subscriber may be the same as the Subject, where a natural person requests the Service on their own behalf. In other situations, the Subscriber may be a body or organisation acting on behalf of natural persons linked by commercial relationships or within the framework of an organisational structure. Finally, the Subscriber may also be a natural person vested with the powers to represent the legal person.

1.3.7 Authority

1.3.7.1 Agency for Digital Italy – AgID

The Agency for Digital Italy (**AgID**) is the supervisory body for trust service providers. In this capacity, AgID supervises qualified trust service providers established in Italy to ensure they comply with the requirements set out in the Regulation [1].

1.3.7.2 Conformity Assessment Body (CAB)

The Conformity Assessment Body (**CAB**) is

a body accredited in accordance with the provisions of the Regulation [1], which is authorised to assess the conformity of the qualified trust service provider and the qualified trust services it provides with the applicable regulations and standards.

1.4 Use of the certificate

1.4.1 Permitted uses

I The remote qualified electronic signature service provided by InfoCert enables the signer to generate qualified electronic signatures using a private key stored in a remote qualified signature creation device (remote QSCD), in accordance with the Regulation [1] and the applicable technical standards.

The service may only be used by the signer to whom the following are associated:

- the pair of signature keys generated in the remote QSCD;
- the qualified certificate containing the corresponding public key;
- the electronic identification means (eID means) associated with the service.

Use of the private signature key is permitted only following authentication of the signer and activation of the signing process in accordance with the procedures provided for by the system, which guarantee the signer's exclusive control over the key.

Signatures generated via the service are intended for the signing of electronic documents in the contexts provided for by current legislation and, together with the associated certificate, produce the legal effects recognised for a qualified electronic signature.

Verification of signatures affixed via the service is carried out using the associated qualified certificate, in accordance with the technical procedures set out in industry standards.

1.4.2 Prohibited uses

Any use of the remote qualified signature service that contravenes:

- the contractual terms and conditions entered into by the User;
- the provisions of this policy and practice statement;
- the usage limits specified in the associated qualified certificate (key usage, extended key usage, user notice);
- the authentication and activation procedures provided for by the system.

In particular, it is prohibited to:

- attempting to access or activate the private key without complying with the prescribed authentication procedures;

- to use credentials or means of electronic identification associated with the service in an improper or unauthorised manner;
- to use the service for purposes other than the generation of qualified electronic signatures.

1.5 Administration of the policy and practice statement

1.5.1 Contact details

Tinexta Infocert is responsible for the drafting, publication and updating of this document. Any questions, complaints, comments or requests for clarification regarding this policy and practice statement should be addressed to the following contact details:

Company name	**Tinexta Infocert – Public Limited Company** **Head of the Remote Signature Service Via** **Fernanda Wittgens No. 2, 20123 Milan (MI)**
Telephone number	**06 836691**
Contact Centre	**https://help.infocert.it/contatti/ for further details**
Website	**https://www.firma.infocert.it, https://www.infocert.it**
Email	**firma.digitale@legalmail.it**

The Data Subject or the subscriber may request a copy of the documentation relating to them.

1.5.2 Persons responsible for approving the policy and practice statement

The policy and practice statement is reviewed by the Head of Security and Policy, the Data Protection Officer, the QTSP Manager and the Legal Manager, and is approved by the Company Management.

1.5.3 Approval procedures

The drafting and approval of the manual follow the procedures set out in the Company's ISO 9001:2015 Quality Management System.

At least once a year, the Trust Service Provider carries out a compliance check to ensure this policy and practice statement is in line with its certification service delivery process.

1.6 Definitions and Acronyms

1.6.1 Definitions

The definitions used in the drafting of this document are listed below. For terms defined by the eIDAS Regulation [1] and the CAD [2], please refer to the definitions set out therein. Where appropriate, the corresponding English term – generally used in publications, standards and technical documents – is indicated in square brackets.

Term	*Definition*
Conformity Assessment Body	A body accredited under the eIDAS Regulation as competent to

Term	Definition
(Conformity Assessment) (CAB)	carry out the conformity assessment of the qualified trust service provider and the qualified trust services it provides. It draws up the CAR.
Conformity Assessment Report (CAR) (CAR)	A report in which the conformity assessment body confirms that the qualified trust service provider and the trust services themselves comply with the requirements of the Regulation (see eIDAS [1]).
Electronic signature certificate	An electronic certificate that links the validation data of an electronic signature to a natural person and confirms at least that person's name or pseudonym (see eIDAS [1]).
Electronic seal certificate certificate	An electronic certificate that links the validation data of an electronic seal to a legal person and confirms the name of that person (see eIDAS [1]).
Qualified electronic signature certificate	An electronic signature certificate issued by a qualified trust service provider and complying with the requirements set out in Annex I to the eIDAS Regulation (see eIDAS [1]).
Qualified electronic seal certificate (QSealC)	An electronic seal certificate issued by a and complies with the requirements set out in Annex III to the eIDAS Regulation (see eIDAS [1]).
Private key/Signing key	The element of the asymmetric key pair used by the Subject to affix a qualified electronic signature to an (see CAD [2]).
Public key	The element of the asymmetric key pair intended to be made public, used to verify the qualified electronic signature affixed to the electronic document by the Signatory (see CAD [2]).
One-Time Signing Key	A certified signing key associated with, used and deactivated on the basis of a single authorisation, linked to a single signing session for the data/documents to be signed (DTBS/R(s))
Client	A party with whom Infocert has entered into a service provision contract in return for payment
Emergency Code (ERC)	Security code issued to the party to submit a request for suspend a certificate via the TSP's portals.
Validation	The process of verifying and confirming the validity of an electronic signature (see eIDAS [1]).
Validation data	Data used to validate an electronic signature (see eIDAS [1]).
Personal identification data	A set of data that makes it possible to establish the identity of a natural or legal person, or of a natural person representing a legal person (see eIDAS [1]).
Data for creating an electronic signature	The unique data used by the signer to create an electronic signature (see eIDAS [1]).
Device for creating an electronic signature (SSCD – secure system creation device)	Software or hardware configured to create an electronic signature (see eIDAS [1]).
Device for creating a (QSCD)	An electronic signature creation device that meets the requirements set out in Annex II to the eIDAS Regulation (see eIDAS [1]).
Electronic document	Any content stored in electronic form, in particular text or audio, visual or audiovisual recording (see eIDAS [1]).
Automatic signature	A specific electronic signature procedure carried out following authorisation by the signatory, who retains exclusive control over their signing keys, without the need for their constant and continuous supervision.
Qualified electronic signature	An advanced electronic signature created by a qualified electronic signature creation device and based on a qualified certificate for (see eIDAS [1]).
Remote signature	A specific qualified electronic signature procedure, generated on an HSM, which ensures that the subjects of private keys have exclusive control over them

Term	Definition
Signer	A natural person who creates an electronic signature (see eIDAS [1]).
Electronic identification	The process whereby personal identification data in electronic form that represents a single natural or legal person, or a single natural person representing a legal person (see eIDAS [1]).
Certificate Revocation List (CRL)	This is a list of certificates that have been rendered 'invalid' before their natural expiry date. The operation is called revocation if permanent, and suspension if temporary. When a certificate is revoked or suspended, its is added to the CRL, which is then published in the public register.
Policy and Practice Statement	This defines the procedures that the SSASP applies in the provision of the service. In drafting of the Manual, the guidelines set out by the Supervisory Authority and those found in international literature were followed.
Means of electronic	A physical and/or non-physical entity containing personal identification data and used for authentication for an online service (see eIDAS [1]).
Online Certificate Status Protocol (OCSP)	A protocol defined by the IETF in RFC 6960, which enables applications to verify the validity of a certificate more quickly and accurately than a CRL, with which it shares data.
One-Time Password (OTP)	A One-Time Password (OTP) is a password that is valid for a single transaction only. The OTP is generated and made available to the Subscriber immediately prior to the application of the qualified electronic signature. It may be based on hardware devices or on software procedures.
Relying party (User/Relying party)	A natural or legal person who relies on electronic identification or a trust service (see eIDAS [1]).
Trust service provider	A natural or legal person who provides one or more trust services, either as a qualified trust service provider or as a non-qualified trust service provider (see eIDAS [1]).
Qualified trust service provider	A trust service provider that provides one or more qualified trust services and to which the supervisory body grants the status of qualified trust service provider (see eIDAS [1]).
Product	Hardware or software, or their relevant components, intended to be used for the provision of trust services (see eIDAS [1]).
Revocation or suspension of a certificate	This is the process by which the CA revokes the validity of the certificate before its natural expiry.
Trust service	An electronic service normally provided for a fee and comprising the following elements: the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, certified electronic delivery services and certificates relating to such services; or the creation, verification and validation of website authentication certificates; or the storage of electronic signatures, seals or certificates relating to such services (see eIDAS [1]).
Qualified trust service	A trust service that meets the relevant requirements set out in the Regulation (see eIDAS [1]).
Electronic seal	Data in electronic form, attached to or logically associated with other data in electronic form, to guarantee the origin and integrity of the latter (see eIDAS [1]).
Qualified electronic seal	An advanced electronic seal created by a device for creating a qualified electronic seal and based on a qualified certificate for electronic seals (see eIDAS [1]).
Member State	Member State of the European Union
Coordinated Universal Time (Coordinated Universal Time)	Time scale with precision to the second, as defined in ITU-R Recommendation TF.460-5.
Electronic time stamping	Data in electronic form that links other data in electronic form to a specific time and date, thereby proving that the latter existed at that time (see eIDAS [1]).

Time stamp	An electronic time stamp that meets the requirements set out in Article

Term	Definition
qualified electronic	42 of the eIDAS Regulation (see eIDAS [1]).

Table 2 – Definitions

1.6.2 Acronyms and Abbreviations

Acronym	Definition
AgID	Agency for Digital Italy: Supervisory Authority for Fiduciary Service Providers Fiduciary
CA	Certification Authority
SSASP	Server Signing Application Service Provider
SSA (SSAS)	Server Signing Application (Service)
CAB	Conformity Assessment Body
CAD	Digital Administration Code
CAR	Conformity Assessment Report – Conformity Assessment Report
CC	Common Criteria
CIE	Electronic Identity Card
CRL	Certificate Revocation List
DMZ	Demilitarised Zone
DN	Distinguishing Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority
eID	Electronic Identity
eIDAS	Regulation on Electronic Identification and Digital Signatures
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: a secure device for generating signatures, with functionality similar to that of smartcards, but with superior memory and performance capabilities
HTTP	HyperText Transfer Protocol
IDP	Identity Provider
IETF	Internet Engineering Task Force
IR	Registration Authority Officer
ISO	International Organisation for Standardisation: founded in 1946, ISO is an international organisation comprising national standardisation bodies standardisation
ITU	International Telecommunication Union: founded in 1865, it is the responsible for setting standards in telecommunications
IUT	Unique Subject Identifier: a code associated with the Subject that uniquely identifies them to the CA; the Subject has different codes for each certificate they hold
LDAP	Lightweight Directory Access Protocol: a protocol used to access the certificate registry
LoA	Level of Assurance
LoIP	Level of Identity Proofing
NCA	National Competent Authority
OID	Object Identifier: consists of a sequence of numbers, registered in accordance with the procedure set out in the ISO/IEC 6523 standard, which identifies a specific object within a hierarchy
OTP	One-Time Password
PEC	Certified Email
PIN	Personal Identification Number: a code associated with a secure , used by the User to access the device's functions
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure: a set of resources,

Acronym	Definition
	processes and technological means that enable trusted third parties to verify and/or vouch for the identity of an entity, as well as to associate a to an individual
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
QSealC	Qualified Electronic Seal Certificate
RA	Registration Authority
RFC	Request for Comment: a document containing information or specifications regarding new research, innovations and methodologies in the IT sector, submitted by the authors for review by the community
RSA	Derived from the initials of the algorithm's inventors: River, Shamir, Adleman
SGSI	Information Security Management System
SPID	Public Digital Identity System
SSCD – QSSCD	Secure Signature Creation Device: a device for creating an electronic signature Qualified Secure Signature Creation Device: a qualified device for the creating an electronic signature
TIN	Tax Identification Number
UUID	Universally Unique Identifier
URL	Uniform Resource Locator
VAT Code	Value Added Tax Code
X500	ITU-T standard for LDAP and directory services
X509	ITU-T standard for PKIs

Table 5 – Acronyms and abbreviations

2 PUBLICATION AND ARCHIVING

2.1 Publication and availability of documentation

Documentation relating to the Remote Signature service, including this Manual and the general terms and conditions of service, is published on the Tinexta Infocert website and is available 24 hours a day, 7 days a week.

2.2 Publication of certification information

The publication of information relating to certification, the status of certificates, CRLs/OCSPs and, in general, matters specific to the CA is governed by the documentation of the relevant CA.

2.3 Publication period or frequency

2.3.1 Frequency of publication of the policy and practice statement

The policy and practice statement is published as set out in paragraph 1.5.1 at varying intervals whenever changes occur, but no less frequently than once a year, as specified in paragraph 1.5.3. If the changes are significant, the SSASP must undergo an audit by an accredited CAB, submit the certification report (*CAR – Conformity Assessment Report*) and the policy and practice statement to the Supervisory Authority (AgID).

2.3.2 Frequency of publication of revocation and suspension lists

N/A

2.4 Control of access to public archives

The policy and practice statements are public; the SSASP is freely accessible for public consultation and has implemented all necessary measures to prevent unauthorised modifications or deletions.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Name

3.1.1 Types of names

Please refer to the Certificate Policy/Certificate Practice Statement (hereinafter the policy and practice statement of the CA) of the Certification Authority in question.

3.1.2 The need for the name to have a meaning

Please refer to the CA's policy and practice statement

3.1.3 Anonymity and pseudonymity of subscribers

Please refer to the CA policy and practice statement.

3.1.4 Rules for interpreting name types

Please refer to the CA policy and practice statement.

3.1.5 Uniqueness of names

Please refer to the CA policy and practice statement.

3.1.6 Recognition, authentication and role of registered trademarks

Please refer to the CA policy and practice statement.

3.2 Initial identity validation

Activation of the remote qualified electronic signature service is subject to the prior identification of the Subject in accordance with the procedures laid down for the issue of the qualified certificate.

Identification procedures are carried out by the Certification Authority and/or the Registration Authority. The SSASP relies on these checks to generate the key pair in the remote QSCD and to associate the service with the signer.

3.2.1 Method for demonstrating possession of the private key

In the remote qualified signature service, the cryptographic key pair associated with the qualified certificate is generated within the remote qualified signature creation device (remote QSCD), in a secure environment and in such a way as to ensure that the private key cannot be exported.

Proof of possession of the private key associated with the public key to be certified is ensured by the process of generating the key pair within

the remote QSCD and by the link between this process and the request for the issue of the qualified certificate through the signing of a CSR with the generated private key.

The procedures by which the Certification Authority verifies Proof of Possession for the purposes of issuing the qualified certificate are set out in the CA's policy and practice statement.

This policy and practice statement does not set out in detail the procedures for verifying Proof of Possession carried out by the Certification Authority.

3.2.2 Authentication of the legal person's identity

In the case of certificates relating to legal entities, the service is activated in relation to an identified natural person acting as a representative or authorised person.

Following the checks carried out by the CA/RA regarding powers of representation, the SSASP links the private key stored in the remote QSCD to the natural person authorised to activate the seal.

3.2.3 Authentication of the identity of a natural person

The authentication of the natural person's identity for the purposes of issuing the qualified certificate associated with the remote signature service is carried out in accordance with the procedures established by the Certification Authority and, where applicable, by the delegated Registration Authorities (RAs).

3.2.4 Unverified information regarding the Subject or the Subscriber

The SSASP does not carry out independent checks on the attributes included in the qualified certificate. Any unverified information remains the responsibility of the Certification Authority in accordance with its own policies.

3.3 Identification and authentication in case of renewal or reissue with new keys

In the context of the remote qualified signature service, the identification of the Subject for the purposes of issuing the qualified certificate is carried out in accordance with the procedures established by the Certification Authority.

The SSASP, on the other hand, is responsible for authenticating the Subject for the purposes of using the private key stored in the remote QSCD and initiating the signing process.

3.3.1 Identification and authentication of a Subject in the event of reissue with new keys

In the context of the remote qualified signature service, where a new key pair is to be generated within the remote QSCD upon renewal or reissue of the qualified certificate, the Subject's identification for the purposes of issuing the new certificate is carried out in accordance with the procedures established by the Certification Authority.

The SSASP is responsible for authenticating the Subject for access to the service and for the use

the private key stored in the remote QSCD. Before the Subject can use the new private key to generate qualified electronic signatures, the system requires the Subject to be authenticated using the mechanisms provided by the service.

These authentication mechanisms are designed to ensure that only the legitimate Subject can initiate the signing process and that the private key is used under their exclusive control, in accordance with the security requirements set out in the applicable legislation and relevant technical standards.

3.3.2 Identification and authentication of a Subject in the event of reissuance with new keys following revocation

In the event of the reissue of a qualified certificate involving the generation of a new key pair following the revocation of the previous certificate, the identification of the Subject for the purposes of issuing the new certificate is carried out in accordance with the procedures established by the Certification Authority.

In the remote qualified signature service, the new key pair is generated within the remote QSCD. The use of the private key for generating signatures is permitted only following authentication of the Subject in accordance with the mechanisms provided for by the service and managed by the SSASP.

3.3.3 Identification and authentication of a Subject for certificate renewal

In the case of the renewal of a qualified certificate, the identification of the Subject for the purposes of issuing the new certificate is carried out in accordance with the procedures established by the Certification Authority, and the renewal request is signed with the current private key.

3.4 Identification and authentication for revocation or suspension requests

Requests for the revocation or suspension of qualified certificates associated with the remote signature service are handled by the Certification Authority, in accordance with the procedures described in the relevant Certification Policy (CP) and Certification Practice Statement (CPS).

Following the revocation of a qualified certificate associated with the remote signature service, the SSASP shall destroy the corresponding private key stored in the remote QSCD, in accordance with the security procedures laid down by the service.

This policy and practice statement does not set out in detail the operational procedures for the revocation or suspension of certificates, which form part of the certificate lifecycle managed by the Certification Authority.

3.4.1 Request by the Party

n/a

3.4.2 Request by the Subscriber

n/a

4 OPERATIONS

4.1 Request and activation of the service

4.1.1 Who can request the service

The remote qualified electronic signature service may be requested by the signer or by a subscriber authorised to request the service on behalf of the signer or to bear the costs thereof, within the limits set out in the contractual documentation. Activation may take place via the channels made available by Infocert and/or via authorised Registration Authorities.

In the case of legal entities, the request is submitted by an identified natural person acting as a legal representative or a person holding a power of attorney, in accordance with the prescribed procedures.

4.1.2 Activation Process and Responsibilities

The process for registering and activating the remote qualified electronic signature service involves:

- the identification of the signer in accordance with the procedures of the Certification Authority and/or the Registration Authority;
- the generation of the key pair within the remote QSCD;
- the issue by the CA of the qualified certificate associated with the public key;
- the linking of the signer's identity, the qualified certificate, the private key and the authentication methods authorised for signature activation.

The SSASP is responsible for the correct generation and safekeeping of the private key within the remote QSCD, as well as for configuring the signature activation mechanisms in such a way as to ensure the signer's exclusive control.

The CA is responsible for verifying the identity of the Subject and for issuing the qualified certificate in accordance with its own policies.

The service is deemed to have been activated when the signer is able to authenticate themselves and generate qualified electronic signatures via the remote QSCD, in accordance with the service rules.

4.2 Processing of the request

4.2.1 Performance of identification and authentication functions

The identification of the Subject for the purposes of issuing the qualified certificate is carried out in accordance with the procedures of the Certification Authority and/or the Registration Authority. The authentication of the Subject for the purposes of using the private key stored in the remote QSCD

and to initiate the signing process is, however, carried out by the SSASP, in accordance with the procedures laid down by the service. The SSASP uses two-factor authentication systems not necessarily based on digital certificates, the private keys of which are stored on devices that meet the requirements set out in Annex II of Regulation [1] of the European Parliament and of the Council. This level corresponds to Level of Assurance (LoA) 3 of the ISO/IEC 29115 standard (Substantial). At this level, the signer is issued with a user ID, a password and OTP (One-Time Password) systems, managed via SMS and/or applications, which ensure compliance with the requirements laid down by the legislation. Biometric access systems may also be used, in accordance with the provisions of the Italian Data Protection Authority.

Depending on the configured process, Infocert can make the following authentication methods available to the signer:

A. One-Time Password via SMS

B. Time-based one-time password

C. Implicit authentication with QR code

D. Implicit authentication via push notification

E. TOTP via hardware device

F. Authorisation assertion.

4.2.1.1 Natural person

In the case of a natural person, identification is carried out by the CA/RA or by a designated IPSP.

Upon receiving confirmation that the identification process has been successful, the SSASP generates the key pair in the remote QSCD and associates the service with the Subject.

4.2.1.2 Legal entity

In the case of a legal entity, the identification of the authorised natural person is carried out by the CA/RA.

The SSASP associates the service with the authorised natural person, ensuring that the activation of the private key is conditional upon their authentication.

Verification of powers of representation falls within the remit of the CA.

4.2.1.3 Registration

Following a request for the remote qualified electronic signature service, the SSASP creates a user account in its systems linked to the requested remote signature service.

The user account is used for the operational management of the service and to link:

- the service subject;

- the remote signature service activated;
- the key pair generated in the remote QSCD;
- the qualified certificate issued by the Certification Authority;
- the authentication methods used to activate the signature.

The user account is created prior to the issue of the qualified certificate, which is subsequently requested by the SSASP from the Certification Authority – even if this is different from the remote signature service provider – by signing a CSR with the Subject's private key.

4.2.2 Approval or rejection of the service request

The request to activate the remote qualified electronic signature service is assessed on the basis of the outcome of the Subject's identification checks and the accuracy of the information provided.

If the checks carried out by the CA are successful, the SSASP proceeds with activating the service, generating the key pair in the remote QSCD and requesting the issue of the qualified certificate from the Certification Authority.

If the checks are unsuccessful or incomplete, the application may be rejected or suspended until any issues have been resolved.

The issue of the qualified certificate remains, in all cases, the responsibility of the Certification Authority, in accordance with its own policies and procedures.

4.2.3 Maximum processing time for the certificate application

The time required to process the application for activation of the remote qualified electronic signature service depends on the completion of the identification procedures for the applicant, the verification of the information provided and the availability of the data necessary for service activation.

Once the CA has completed these checks, the SSASP proceeds to generate the key pair in the remote QSCD and to request the issue of the qualified certificate from the Certification Authority.

The time taken to issue the qualified certificate is determined by the Certification Authority's operational procedures.

4.3 Key generation and activation in the QSCD

4.3.1 SSASP operations for key generation or management

4.3.1.1 Generation of the key pair in the QSCD

The cryptographic key pair used for the remote qualified electronic signature service is generated within the QSCD, in a secure environment managed by the SSASP.

Keys are generated using cryptographic modules that comply with the requirements applicable to qualified signature creation devices. The private key cannot be exported and is stored within the QSCD for the entire duration of the service.

The corresponding public key is used by the SSASP to request the Certification Authority to issue the qualified certificate associated with the Subject.

The private key may only be used via the signature activation mechanisms provided by the service and under the Subject's sole control.

4.3.1.2 Types of keys in the remote signature service

The remote electronic signature service provides for various types of keys, depending on the service's operational model.

In particular, the service may provide for:

- persistent keys, permanently associated with the Subject and used to generate signatures throughout the validity period of the qualified certificate;
- one-time keys, generated for the purpose of signing a single transaction;
- keys used in automated signing processes, activated in accordance with the procedures laid down by the service
- keys used for the generation of digital seals.

In all cases, private keys are generated and stored in the remote QSCD, and their use is permitted only following the Subject's authentication in accordance with one of the methods mentioned above or, where applicable, those provided by the RA, and following the activation of the signing process via the configured service systems.

4.3.2 Notification to subscribers of the certificate's issue

The issue of the qualified certificate is the responsibility of the Certification Authority, which notifies the subscriber of the information required to use the certificate in accordance with the CA's own policies.

4.3.3 Activation

4.3.3.1 Operational activation of the keys

Following confirmation of the issue of the qualified certificate, the SSASP proceeds with the operational activation of the private key stored in the remote QSCD.

Operational activation consists of linking the private key with:

- the qualified certificate issued by the Certification Authority;
- the authentication methods authorised for signature activation.

From that point onwards, the private key may be used to generate qualified electronic signatures via the remote signature service, subject to the signer undergoing at least substantial-level authentication in accordance with the procedures laid down by the service.

The private key is used to generate a qualified signature exclusively via the Signature Activation process.

For each signing operation:

- The signer initiates the signing process using their credentials;
- the Signature Activation Data (SAD) is generated and validated;
- the QSCD verifies the validity of the SAD and the status of the key

Only if the result is positive is the private key used to generate the signature or seal.

4.3.3.2 Associating the certificate with the keys

The private key generated in the remote QSCD is associated with the qualified certificate issued by the Certification Authority via the corresponding public key.

Before allowing the signature to be activated, the SSASP verifies that the associated certificate is valid and has not been suspended or revoked, based on the information provided by the CA.

Management of the certificate's status remains the responsibility of the Certification Authority, whilst the SSASP is responsible for preventing the key from being activated in the event of an invalid certificate.

4.4 Authorisation of the signing operation

4.4.1 Conclusive actions authorising the signing operation

The request for the signing operation is deemed to have been made when the signer, following authentication to the service, explicitly authorises the use of the private key stored in the remote QSCD to generate the signature.

The following constitute conclusive evidence of a request for the signing operation:

- the signer's authentication using the authentication methods associated with the service.
- the explicit expression of authorisation (consent) for the signature operation via the mechanisms provided by the system.

Following these operations, the system proceeds to activate the private key in the remote QSCD and generate the qualified electronic signature, ensuring that the use of the private key takes place under the signer's exclusive control.

4.4.2 Signature generation

Following the signer's authentication and authorisation of the signing operation in accordance with the procedures provided for by the service, the system uses the private key stored in the QSCD to generate the qualified electronic signature, which is returned to the subscriber's process.

The SSASP ensures the technical traceability of the signing operation within its own systems, in compliance with applicable regulations and standards.

4.4.3 Notification of the successful execution of the signing operation

Notification is provided to the Party that the signature operation has been successfully completed, together with its timestamp.

4.5 Use of the key pair and certificate

4.5.1 Use of the private key by the Signatory

In the remote qualified electronic signature service, the private key is stored in the QSCD and is not physically available to the signer.

The Signer is responsible for:

- the proper safekeeping and protection of the authentication means associated with the service;
- for the confidentiality of the codes or authentication factors used to activate the signature;
- for using the service exclusively for the purposes permitted by the contract and applicable legislation.

The Signatory must not:

- allow third parties to use their authentication means;
- request or authorise signing operations without giving their informed consent;
- use the service if they believe their means of authentication have been compromised.

The private key is used exclusively via the signature activation process provided by the service, following authentication and the generation and validation of the Signature Activation Data (SAD).

Any usage restrictions included in the qualified certificate are the responsibility of the Certification Authority and must be complied with by the signer.

4.5.2 Use of the public key and verification of the signature by End Users

Any person receiving a document signed using the remote signature service must:

- verify the validity of the qualified electronic signature;
- verify the status of the qualified certificate (not expired, not revoked, not suspended) using the services provided by the Certification Authority;
- check for any restrictions on use or value stated in the certificate.

Verification of the signature and the certificate is the responsibility of the party relying on the signature.

4.5.3 Limitations on the use of the service and the certificate

The use of the remote signature service and the qualified certificate is subject to the service's terms and conditions and to any restrictions specified in the qualified certificate.

4.6 Renewal

The renewal of the qualified certificate associated with the remote signature service is carried out by the Certification Authority in accordance with its own policies and procedures.

The subject submits a renewal request to the Certification Authority, upon which a new key pair is generated, along with a certificate request containing the same data as the previous certificate and signed with the previous certificate.

The SSASP maintains the association between the renewed certificate and the authentication mechanisms and generates a new key pair to be associated with the renewed certificate.

4.6.1 Reasons for renewal

The reasons for renewal are governed by the CA's policies and practices.

4.6.2 Who can request renewal

Certificate renewal may be requested by the subject, in accordance with the policies and practices of the Certification Authority.

4.6.3 Processing the certificate renewal request

Renewal is requested from the CA via the Signature service, which will generate the new key pair to request the CA to issue the new certificate.

4.7 Reissuance with new keys

The re-issuance of the certificate with the generation of a new key pair (re-key) allows

the already identified party to obtain a new qualified certificate associated with a different key pair.

4.7.1 Reasons for reissuing with new keys

Reissuing the certificate with a new key (re-key) allows an already identified Subject who holds a certificate to certify a different key pair, whilst retaining the same identification details. The expiry date of the new certificate is defined contractually.

Examples, which are not exhaustive, include the re-certification of a new key pair on a remote device as the certificate's expiry date approaches or on a device being decommissioned, or the replacement of weak cryptographic keys with cryptographic keys generated using more robust algorithms.

This procedure applies exclusively to certificates issued by Infocert.

4.7.2 Who can request re-issuance with new keys

The request may be made by the Holder or the subscriber before the certificate expires or thereafter, provided that all the information supplied at the time of the previous issue and the evidence gathered during the identification phase are still valid. If the identity document is no longer valid, the certificate cannot be reissued.

4.7.3 Processing the request for reissue with new keys

Reissuance with new keys is carried out via a service provided by the CA, within the framework of the commercial and contractual relationships established with the Subject and with the RA, where applicable.

4.8 Amendment of the certificate

n/a

4.9 Revocation and suspension of the certificate

The revocation or suspension of a qualified certificate is the sole responsibility of the Certification Authority.

Upon receiving notification of revocation or suspension, the SSASP prevents the use of the private key in the remote QSCD and, in the event of revocation, proceeds to destroy the key itself.

4.10 Services relating to the status of the certificate

N/A

4.11 Termination of SSASP services

Termination of the remote signing service entails the blocking of the private key's use and its destruction in the QSCD in accordance with controlled and traceable procedures.

Destruction ensures that any copies or residual information cannot be used to reconstruct the key.

4.12 Third-party storage and key recovery

There is no provision for the private key (signing key) to be held by third parties outside the remote QSCD infrastructure.

The service provides for backup mechanisms for the signing key within the remote QSCD infrastructure, in order to ensure service continuity.

All private keys, including signing keys, infrastructure keys and control keys, are stored exclusively in a secure form and are never stored in an unsecured state.

Should a private key be exported from the remote QSCD for backup purposes, it is protected in such a way as to guarantee confidentiality and integrity with a level of security at least equivalent to that guaranteed within the QSCD; only cryptographic algorithms and parameters of equivalent or greater strength are used.

The backup, storage and restoration of keys are carried out exclusively by authorised personnel. The master keys used to protect user keys and operational keys are subject to backup, storage and restoration under multiple controls (at least dual control) and are held outside the QSCD exclusively in a protected form.

The number of copies of datasets containing keys is limited to the minimum necessary to ensure the operational continuity of the service.

5 SECURITY MEASURES AND CONTROLS

The TSP Infocert has implemented a security system for the information system relating to the digital certification service. The security system implemented is structured across three levels:

- a physical level, which aims to ensure the security of the premises where the TSP operates the service,
- a procedural level, covering purely organisational aspects,
- a logical level, through the implementation of hardware and software measures that address the issues and risks associated with the type of service and the infrastructure used.

This security system is designed to prevent risks arising from the malfunctioning of systems, the network and applications, as well as from the unauthorised interception or alteration of data.

An extract from the Infocert security policy is available on request to the certified email address infocert@legalmail.it.

Security policies at Infocert are reviewed at least once a year and are also updated in response to any significant changes. Each review is recorded within the document itself, even if no changes were required.

5.1 Physical security

For the provision of the services covered by this document, Tinexta Infocert utilises public clouds and private cloud infrastructures located in Italy.

Access to the data centres is governed by Infocert's security procedures. Within the data centres hosting the Certification Authorities and certain components of the SSASP service, such as the SAM (Signature Activation Module) and the cryptographic module, there are High Security Trusted Zones (HSTZs), access to which requires additional security measures and specific authorisations.

5.1.1 Waste disposal

Infocert operates an ISO 14001-certified management system for sustainable environmental management.

The organisation follows internal procedures for the secure erasure of data on its HSM devices, using suppliers who guarantee secure erasure.

It also implements a waste management cycle compliant with current national regulations through procedures for managing and monitoring the life cycle of waste, and uses only authorised suppliers for the transport and disposal of such waste.

5.2 Procedural controls

5.2.1 Key roles

Key roles are filled by individuals possessing the necessary experience, professionalism and technical and legal expertise, which are continuously verified through annual assessments.

The list of names and the organisational chart of key role holders was filed with AgID at the time of the first accreditation and is constantly updated to reflect the natural evolution of the company's organisation.

5.3 Staff monitoring

5.3.1 Required qualifications, experience and authorisations

Once the annual Human Resources plan has been drawn up, the Head of Department/Organisational Unit identifies the characteristics and skills required of the candidate to be recruited (*job profile*). Subsequently, in consultation with the recruitment manager, the recruitment and selection process is initiated.

5.3.2 Procedures for verifying previous experience

Shortlisted candidates take part in the selection process, beginning with an initial interview with the recruitment manager to assess their suitability and motivation, followed by a technical interview with the Head of Department/Organisational Unit, aimed at verifying the skills declared by the candidate. Further assessment tools include practical exercises and tests.

5.3.3 Training requirements

To ensure that no single individual can compromise or alter the overall security of the system or carry out unauthorised activities, the operational management of the system is entrusted to different individuals, each with separate and clearly defined tasks. The staff responsible for designing and delivering the certification service are InfoCert employees and have been selected on the basis of their experience in the design, implementation and management of IT services, demonstrating reliability and confidentiality. Training sessions are scheduled periodically to raise awareness of the assigned tasks. In particular, before staff are assigned to operational duties, training sessions are conducted to provide them with all the necessary skills (technical, organisational and procedural) to carry out their assigned tasks.

5.3.4 Frequency of training updates

At the start of each year, a training needs analysis is carried out to determine the training activities to be delivered during the year. The analysis is structured as follows:

- A meeting with senior management to gather data on the training needs required to achieve the company's objectives;
- Interviews with managers to identify the specific training needs of

their respective areas;
- Submission of the collected data to senior management for finalisation and approval of the Training Plan.

By the end of February, the Training Plan thus finalised is shared with staff.

5.3.5 Attendance in the work shift rotation

Attendance at the workplace or via remote working (smart working) is spread across a time slot from 08:00 to 19:00, Monday to Friday.

Supervision of production areas during night shifts and on public holidays is ensured through an on-call rota drawn up by the head of the organisational unit on a monthly basis, with at least 10 (ten) days' notice. Depending on requirements, interventions may be carried out remotely (remote intervention) or may require access to the premises.

Provided that the necessary technical and professional requirements are met, the Company shall ensure that as many employees as possible take turns on on-call duty, giving priority to those who request it.

5.3.6 Penalties for unauthorised actions

Reference is made to the 'National Collective Labour Agreement for Metalworkers and Plant Installers in the Private Sector' regarding the procedure for imposing sanctions on employees.

5.3.7 Checks on non-staff personnel

Access for non-staff personnel is governed by a specific company policy.

5.3.8 Documentation that staff must provide

Upon recruitment, the employee must provide a copy of a valid identity document, a copy of a valid health card and a photograph. They must then complete and sign the consent form for the processing of personal data and the undertaking not to disclose confidential information and/or documents. Finally, they must familiarise themselves with the Code of Ethics and the Infocert Netiquette.

5.4 Management of QTSP events

Events relating to the management of the SSAS and the lifecycle of keys are recorded in accordance with the procedures set out in the compliant retention systems and described in the relevant security manual.

5.4.1 Types of events recorded

The following are recorded:

- security events, start-up, shutdown, system crashes and hardware failures of SSASP systems;
- events relating to the management of signing keys in the remote QSCD (generation, activation, destruction, and any backups and restores);

- events relating to the management of signing sessions and the validation of Signature Activation Data (SAD);
- Subject authentication events;
- logical access to SSASP applications;
- physical access to the high-security premises where the remote QSCD systems are located.

As regards the identification of the Subject and the issuance of the certificate, the relevant logs are managed by the Certification Authority.

Each event is recorded with the system date and time.

5.4.2 Frequency of processing and storage of the audit log

The processing and grouping of data, as well as its storage on Infocert's compliant retention services, is carried out at a frequency defined by SSASP procedures.

5.4.3 Retention period for SSAS events

SSASP logs are retained for a period compliant with the regulatory requirements applicable to qualified trust services.

Where the QTSP is Infocert, the retention period is at least 20 years from the expiry of the certificate, up to a maximum of 23 years from the date of issue.

5.4.4 Notification in the event of identified vulnerabilities

Any significant vulnerabilities are managed within the SSASP's information security management system and dealt with in accordance with incident management procedures.

5.4.5 Vulnerability assessments

Infocert periodically carries out vulnerability assessments and penetration tests on the System. Based on the results, it implements all necessary countermeasures to secure the applications.

5.5 Archiving of reports

5.5.1 Types of reports archived

Reports relating to the most significant SSAS events are drawn up and archived. The reports are retained for 20 years by the SSASP through Infocert's document retention services, in accordance with regulations governing electronic documents.

5.5.2 Protection of reports

Protection is guaranteed by Infocert's document retention services, which comply with regulations governing

.

5.5.3 Minutes backup procedures

Infocert's electronic document archiving services implement a backup policy and procedure, as set out in the security manual for those services.

5.5.4 Requirements for the time-stamping of records

n/a

5.5.5 Archive storage system

Minutes are collected via ad hoc automated procedures; storage is carried out in accordance with the procedures set out by Infocert's services for the compliant preservation of electronic documents and described in the security manual.

5.5.6 Procedures for retrieving and verifying the information contained in the archives

All data is stored using Infocert's archiving services in accordance with the regulations governing electronic documents, which provide for regular checks on the system's status and data integrity. Data is produced in accordance with the relevant regulations.

5.6 Disaster recovery

5.6.1 Incident management procedures

The QTSP has set out the incident management procedures within the scope of the ISO 27001-certified IMS. Any incident, as soon as it is detected, is subject to a thorough analysis, the identification of corrective measures and the drawing up of a report by the service manager. The report is digitally signed; a copy is also sent to AgID, together with a statement of the remedial actions aimed at eliminating the causes that may have given rise to the incident, if these are under Infocert's control.

5.6.2 Corruption of hardware, software or data

In the event of a failure of the HSM secure signing device containing the signing keys, the backup copy of the signing keys is used and there is no need to revoke the corresponding CA certificate.

Software and data are subject to regular backups in accordance with internal procedures.

5.6.3 Provision of SSASP services in the event of disasters

Infocert has adopted the necessary procedures to ensure service continuity even in highly critical situations or in the event of a disaster, in accordance with the Security Policies.

5.7 Termination of the SSASP service

In the event of the termination of the remote qualified electronic signature service, the SSASP shall notify the Supervisory Authority within the time limits set out in the applicable legislation and inform signers, subscribers and any other parties contractually involved of the procedures set out in the Termination Plan.

6 TECHNOLOGICAL SECURITY CONTROLS

6.1.1 Key pair generation Generation of the Subject's key pair

Asymmetric keys are generated within a Secure Signature Creation Device (QSCD) of the HSM type, using the native functions offered by the device itself.

6.1.2 Delivery of the private key to the Subject

The private key is stored exclusively within the cryptographic device.

6.1.3 Delivery of the public key to the CA

The public key is transmitted to the Certification Authority for the issuance of the qualified certificate in accordance with secure and traceable procedures implemented by the SSASP.

6.1.4 Delivery of the public key to users

N/A

6.1.5 Algorithm and key length

The asymmetric key pair is generated within the remote hardware cryptographic device referred to above.

The subject's keys may be issued in accordance with the following specifications:

1) EC asymmetric keys based on one of the elliptic curves specified in the document 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity (ENISA), with a length of not less than 256 bits.

   - BrainpoolP256r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7)}
   - BrainpoolP384r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP384r1(11)}
   - BrainpoolP512r1: {iso(1) identified-organisation(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP512r1(13)}
   - Secp256r1: {iso(1) member-body(2) us(840) ansi-x962(10045) curves(3) prime(1) prime256v1(7)}
   - Secp384r1: {iso(1) identified-organisation(3) certicom(132) curve(0) ansip384r1(34)}
   - Secp521r1: {iso(1) identified-organisation(3) certicom(132) curve(0) ansip521r1(35)}

2) RSA asymmetric keys with a length of not less than 3072 bits.

6.1.6 Quality controls and public key generation

The devices used are certified to high security standards (see § 6.2.1) and ensure that the public key is valid and random. Before issuing the certificate, the CA verifies that the public key has not already been used.

6.1.7 Purpose of the key

6.1.7.1 Use of the CA key

n/a

6.1.7.2 Subject key usage

The purpose of use of the Subject's key is determined by the KeyUsage extension as defined in the X.509 standard. The extensions are set by the CA.

6.2 Protection of the private key and engineering controls of the cryptographic module

6.2.1 Cryptographic module controls and standards

The cryptographic modules used by Infocert for the Subject's remote and automated signing keys are included in the list of notified QSCDs as defined in Regulation [1]:

- TRISS Trust Remote InfoCert Signing Server version 1.0.2,
- Qualified Signature and Seal Creation Device (QSCD) Intesi PkBox, version 3.4.

6.2.2 Multi-person control of the private key

Critical operations on keys (backup, restoration, destruction, master key management) are subject to dual control.

6.2.3 Deposit of the CA's private key with a third party

n/a

6.2.4 Backup of the private key

The signing key is backed up in a secure manner, with a level of security equivalent to or higher than that of the QSCD.

Operations are carried out exclusively by authorised personnel, and master keys are managed under multiple controls.

The number of copies is limited to the minimum necessary to ensure service continuity.

6.2.5 Storage of the private key

There are no provisions for storing the signing key outside the regulated backup mechanisms.

6.2.6 Transfer of the private key from one cryptographic module to another

Should the key be transferred between cryptographic modules to ensure service continuity, the transfer takes place in encrypted form and is protected with an equivalent level of security

6.2.7 Storage of the private key on a cryptographic module

The certification key is generated and stored in a secure area of the cryptographic device, managed by the SSASP, which prevents its export. Furthermore, should the security measures be breached, the device's operating system will either lock the device or render it unreadable.

6.2.8 Method of activating the private key

N/A

6.2.9 Method of deactivating the private key

The signing key is automatically deactivated at the end of the signing session

6.2.10 Method for destroying the private key

Infocert staff designated for this role are responsible for destroying the private key when the certificate has expired or been revoked, in accordance with the security procedures set out in the security policies and the device manufacturer's specifications.

6.3 Other aspects of key management

n/a

6.3.1 Storage of the public key

n/a

6.3.2 Validity period of the certificate and key pair

The validity period of the certificate and the types of keys, as described in paragraph 4.3.1.2, is determined on the basis of:

- the state of the art in technology;
- the state of the art in cryptographic knowledge;
- the intended use of the certificate itself.

To this end, Tinexta InfoCert adopts cryptographic parameters consistent with the relevant standards and the latest European guidelines, including the recommendations of the European Cybersecurity Certification Group (ECCG) published by ENISA regarding cryptographic mechanisms.
The key lifetime is limited by the certificate's validity period, in accordance with the policies and practices defined

by the CA.

6.4 Private key activation data

Please refer to sections 4.3.3 and 6.3.

6.5 Cybersecurity controls

6.5.1 Specific security requirements for computers

The operating systems of the computers used by SSASP for key generation are hardened; that is, they are configured to minimise the impact of any vulnerabilities by removing all features not required for the operation and management of the SSAS.

Access by system administrators – appointed for this purpose in accordance with the provisions of current legislation – is granted via a 'root on demand' application, which permits the use of root user privileges only following individual authentication. Access is tracked, logged and retained in accordance with the SSASP's security policies

6.6 Operations on control systems

Infocert attaches strategic importance to the secure handling of information and recognises the need to develop, maintain, monitor and continuously improve an Information Security Management System (ISMS), in accordance with the ISO/IEC 27001 standard for activities EA:33–35.

The ISMS includes procedures and controls for:

- Asset Management;
- Access Control;
- Physical and Environmental Security;
- Operational Security;
- Communications Security;
- Systems Acquisition, Development and Maintenance;
- Incident Management;
- Business Continuity.

All procedures are approved by the relevant managers and shared internally via the Infocert document management system.

6.7 Network security controls

Infocert has designed a network security infrastructure for the qualified remote signature service, based on logical and physical segregation mechanisms, multi-level firewalls and the use of secure cryptographic protocols, in order to protect:

- communications between the SSAS and the CA's systems;
- communications between the SSAS and the remote QSCD;
- communications between applications invoking the signing service and the SSAS;
- communications between administrators/operators and the SSAS.

Communications take place exclusively via encrypted channels using state-of-the-art secure protocols (e.g. TLS), in order to guarantee the confidentiality and integrity of the data exchanged, including signature activation data.

Infocert's systems and networks are connected to the Internet in a controlled manner via firewalls, which allow the connection to be divided into areas of progressively higher security: the Internet, DMZ (Demilitarised Zone) or perimeter networks, and internal networks. All traffic flowing between the various areas is subject to approval by the firewall, based on a set of established rules. The rules defined on the firewalls are designed according to the principles of 'default deny' (anything not expressly permitted is prohibited by default; in other words, the rules will only allow what is strictly necessary for the application to function correctly) and 'defence in depth' (successive layers of defence are organised, first at network level through successive firewall barriers, and finally through system-level hardening).

7 KEY FORMAT

7.1 Supported Signature Algorithms

Cryptographic Operation	Algorithm	Key Sizes	Padding	Hash Algorithm	Applicable Standards
Digital signature generation	RSA PKCS#1 v1.5	3072-bit to 4096-bit	RSASSAPKCS1 -v1.5	SHA256 SHA384 SHA512 SHA3-256 SHA3-384 SHA3-512	IETF RFC 3447
Digital signature generation	RSA PKCS#1 PSS	3072-bit to 4096-bit	RSASSA-PSS	SHA256 SHA384 SHA512	IETF RFC 3447
Digital signature generation	ECDSA Brainpool P256r1	256-bit	Not applicable	SHA-256 SHA3-256	SOGIS v1.2
Digital signature generation	ECDSA Brainpool P320r1	320-bit	Not applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA BrainpoolP384r1	384-bit	Not applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA BrainpoolP512r1	512-bit	Not applicable	SHA-512 SHA3-512	SOGIS v1.2
Digital signature generation	ECDSA Secp256r1	256-bit	Not applicable	SHA-256 SHA3-256	SOGIS v1.2
Digital signature generation	ECDSA Secp384r1	384-bit	Not applicable	SHA-384 SHA3-384	SOGIS v1.2
Digital signature generation	ECDSA Secp521r1	521-bit	Not applicable	SHA-512 SHA3-512	SOGIS v1.2

8 COMPLIANCE CHECKS AND ASSESSMENTS

To obtain the status of a qualified or non-qualified trust service provider, in accordance with the Regulation [1], it is necessary to complete the procedure set out in Article 21 of the aforementioned Regulation.

Infocert has submitted the relevant application to AgID to obtain recognition as a 'qualified trust service provider', attaching a Conformity Assessment Report (CAR) issued by an assessment body authorised by the relevant national body (CAB), which in Italy is ACCREDIA.

8.1 Frequency or circumstances for the conformity assessment

The conformity assessment is repeated every two years, but the CAB carries out a surveillance audit every year.

8.2 Identity and qualifications of the person carrying out the audit

The audit is carried out by:

Company name	**CSQA Certification S.r.l.**
Registered office	**Via S. Gaetano 74, 36016 Thiene (VI)**
Telephone number	**+39 0445 313011**
VAT number/Tax code	**02603680246**
Company Registration No.	**Business Register No. 02603680246** – *REA No.* **RM - 258305**
Website	**http://www.csqa.it**

8.3 Relationship between Infocert and CAB

Infocert provides the Service as a qualified trust service provider in accordance with the Regulation [1], based on a conformity assessment carried out by the Conformity Assessment Body CSQA Certificazioni S.r.l., in accordance with the aforementioned Regulation and the ETSI EN 319 401 standard, in accordance with the eIDAS assessment scheme defined by ACCREDIA against the standards ETSI EN 319 403 and UNI CEI EN ISO/IEC 17065:2012.

8.4 Areas subject to assessment

The CAB is required to assess compliance with the policy and practice statement, the Regulations and the applicable legislation regarding the procedures adopted, the organisation of the SSASP, the allocation of roles, staff training and contractual documentation.

8.5 Actions in the event of non-compliance

In the event of a major non-conformity, the CAB will decide whether to submit the report to AgID as normal, or to reserve the right to repeat the audit once the non-conformity has been rectified.

Infocert undertakes to resolve all non-conformities in a timely manner, implementing all necessary improvement and rectification measures.

9 OTHER LEGAL AND BUSINESS ASPECTS

9.1 Fees

9.1.1 Fees for the issue, renewal and reissue of certificates with new keys

The costs of the remote signature service depend on the configuration required, based on fees set out in the service contract between the Customer and Infocert.

In other cases, the fees are available on the websites https://www.firma.infocert.it/ and http://ecommerce.infocert.it.

The SSASP may enter into commercial agreements with CAs, RAs and/or Customers providing for specific fees.

9.1.2 Fees for access to certificates

n/a.

9.1.3 Fees for access to information on the suspension and revocation status of certificates

n/a.

9.1.4 Fees for other services

Fees are available on the websites https://www.firma.infocert.it/ and http://ecommerce.infocert.it.

9.1.5 Refund policies

If the service is purchased by a person who, under the relevant legislation, qualifies as a consumer, they have the right to withdraw from the contract within 14 days of the date of conclusion of the contract and receive a refund of the price paid, provided that the service has not been activated. Instructions on how to exercise the right of withdrawal and request a refund are available on the website https://help.infocert.it/.

9.2 Financial liability

9.2.1 Insurance cover

Infocert has taken out an appropriate insurance policy to cover the risks associated with its activities and any damage caused to third parties, as required by AgID Decision No. 185/2017. The policy provides for the following limits of cover:

- 10,000,000 euros per claim;
- €10,000,000 per policy year.

9.2.2 Other activities

n/a

9.2.3 Insurance cover for end users

See section 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The activities covered by this Manual do not involve the handling of confidential information.

9.3.2 Information not falling within the scope of application confidential information

n/a

9.3.3 Responsibility for the protection of confidential information

n/a

9.4 Privacy

Information relating to the Data Subject and the Subscriber which SSASP obtains in the course of its normal activities is to be regarded, unless express consent is given, as confidential and not to be disclosed, with the exception of information explicitly intended for public use (public key). In particular, personal data is processed by Infocert in accordance with the provisions of the Digital Administration Code, Legislative Decree No. 196 of 30 June 2003 and European Regulation 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, which has been fully binding since 25 May 2018.

9.4.1 Privacy Programme

Infocert adopts a set of policies through which it implements and integrates the protection of personal data within its ISO 27001-certified Information Security Management System, sharing the process of continuous improvement with that system.

9.4.2 Data treated as personal

Data falling within the relevant definition set out in current legislation [3] is treated as personal data; personal data is therefore defined as any information relating to an identified or identifiable natural person, even indirectly, by reference to any other information, including a personal identification number.

9.4.3 Data not considered personal

Data which is intended to be made public by the technical management of the SSASP – namely, public keys, certificates (if requested by the Data Subject), and the dates of revocation and suspension of the certificate – is not considered personal data.

9.4.4 Data subject

Company name	**Tinexta Infocert S.p.A**
Registered office	**Piazzale Flaminio No. 1/B**
	00196 Rome
Email	**richieste.privacy@legalmail.it**

9.4.5 Privacy policy and consent to the processing of personal data

The privacy policy is available on the website www.infocert.it. InfoCert shall, where necessary, obtain consent to the processing in the manner and form required by law [3] prior to the provision of the service. Specific notices may be available on the Customer's website, which, where necessary, may obtain consent to the processing on behalf of InfoCert.

9.4.6 Disclosure of data following a request from the Authority

The disclosure of data at the request of the authorities is mandatory and is carried out in the manner determined on a case-by-case basis by the authority itself.

9.4.7 Other grounds for disclosure

None.

9.5 Intellectual property

9.6 Representations and warranties

Infocert remains responsible for compliance with the procedures set out in its information security policy, even where certain functions are delegated to another party, in accordance with Article 2.4.1 of the Annex to Commission Implementing Regulation (EU) 2015/1502.

9.7 Limitations of warranty

Infocert gives no warranty (i) as to the proper functioning and security of the hardware and software used by the Entity; (ii) as to any use of the private key that differs from that provided for by the applicable regulations and this policy and practice statement; (iii) as to the regular and uninterrupted operation of national and/or international electricity and telephone lines; (iv) as to the validity and relevance, including for evidential purposes, of the qualified electronic signature or of any message, deed or document associated with it or created using the keys to which the certificate relates, without prejudice to the legal effect of a handwritten signature recognised as equivalent to a qualified electronic signature, pursuant to Article 25 of the Regulation [1]; (v) as to the confidentiality and/or integrity

of any message, deed or document associated with the signing certificate or created using the keys to which the certificate relates (in the sense that any breaches of the latter are, as a rule, detectable by the Signatory or the recipient through the appropriate verification procedure).

InfoCert guarantees only the operation of the Service, in accordance with the levels set out in paragraph 9.15 of the policy and practice statement.

9.8 Limitations of liability

InfoCert assumes no obligation to monitor the content, type or electronic format of the documents and/or, where applicable, the *hashes* transmitted via the IT procedure specified by the subscriber or the Subject, and accepts no liability regarding the validity of such documents and hashes or their traceability to the Subject's actual intent.

Except in cases of wilful misconduct or negligence, InfoCert accepts no liability for direct or indirect damages suffered by Subjects and/or third parties as a result of the use or non-use of the service provided in accordance with the provisions of this Manual

InfoCert shall not be liable for any direct and/or indirect damage arising, including but not limited to, (i) the loss, (ii) the improper storage, (iii) the improper use of identification and authentication tools, and/or (iv) the Subject's failure to comply with the above.

Furthermore, from the stage of drawing up the Contract for remote signature services, and also during its performance, InfoCert shall not be liable for any damage and/or delays caused by the malfunction or failure of the IT system or the internet.

InfoCert, except in cases of wilful misconduct or negligence, shall not be liable for any direct or indirect damages of any nature or extent that may be incurred by the Data Subject, the subscriber and/or third parties as a result of tampering with or interference in the service or equipment carried out by third parties not authorised by InfoCert.

9.9 Indemnities

InfoCert shall be liable solely for any damage directly caused, whether through wilful misconduct or negligence, to any natural or legal person, as a result of a failure to fulfil the obligations set out in the Regulations [1] and InfoCert's failure to take all appropriate measures to prevent such damage.

In the case referred to in the preceding paragraph, the Subscriber or the Data Subject shall be entitled to receive, by way of compensation for the damage directly suffered as a result of the conduct referred to in the preceding paragraph, an amount which shall in no event exceed the maximum limits provided for, per claim and per year, by Article 3(7) of the Regulations annexed to Determination 185/2017.

No reimbursement may be claimed if the failure to use the service is attributable to the

of the certification service or to the telecommunications network operator, or if it results from unforeseeable circumstances, force majeure or causes not attributable to InfoCert, such as, by way of example, strikes, riots, earthquakes, acts of terrorism, civil unrest, organised sabotage, chemical and/or bacteriological incidents, war, floods, measures taken by the relevant authorities in this regard, or the inadequacy of the facilities, hardware and/or software used by the subscriber.

9.10 Term and termination

9.10.1 Term

Prior to expiry, the Party may request renewal of the certificate either by retaining the same keys or by re-certifying new keys, in accordance with the procedure set out in this policy and practice statement.

9.10.2 Termination

The Contract shall be terminated by operation of law, with the simultaneous suspension of the Service and revocation of the certificate issued, in the event of failure to comply with the clauses specified from time to time in the service provision contract. Termination shall take effect by operation of law when the party concerned notifies the other party, by certified email (PEC) or registered letter with acknowledgement of receipt, that it intends to invoke this clause.

In all cases of termination, the effects produced by the Contract up to that point shall remain unaffected.

The Party acknowledges that, in the event of termination of the Contract, for whatever reason, it will no longer be possible to use the Service.

9.10.3 Effects of termination

Termination shall result in the immediate deactivation of the service.

9.10.4 Official communication channels

Please refer to the contact details set out in paragraph 1.5.1.

9.10.5 Revision of the Policy and Practice Statement

The SSASP reserves the right to make changes to this document for technical reasons or due to changes in procedures arising either from legislation or regulations, or to optimise the workflow. Each new version of the policy and practice statement supersedes and replaces previous versions, which nevertheless remain applicable to certificates issued during their period of validity and until their first expiry date.

Changes that do not have a significant impact on users result in an increase in the document's release number, whilst changes with a significant impact on users (such as, for example, major changes to operational procedures) result in an increase in the document's version number. In all cases, the manual will be promptly published and made available in accordance with the prescribed procedures. Any technical or procedural changes to this policy and practice statement will be promptly communicated to the RAs and the accredited CAB.

If the changes are significant, the SSASP must undergo an audit by an accredited CAB, submit the certification report (*CAR – Conformity Assessment Report*) and the policy and practice statement to the Supervisory Authority (AgID), and await authorisation for publication.

9.10.6 Revision history

Information	*Details*
Version/Release No.:	**1.0**
Version/Release Date:	**16 March 2026**
Description of changes:	**First version**
Reasons:	**New Qualified Service**

Table 7 – Version 1.0

9.10.7 Revision procedures

The revision of the policy and practice statement follows the same procedures as those laid down for its drafting and approval, as set out in Chapter 2 of this document, within the framework of the Quality Management System and the Information Security Management System adopted by Infocert.

Every amendment is subject to internal verification by the departments responsible for security, compliance, legal and regulatory matters, as well as by the departments responsible for providing the remote signature service.

Revisions are approved by senior management prior to the publication of the new version of the document.

9.10.8 Notification period and procedure

The Policy and Practice Statement is published:

- in electronic electronic on the website website of the TSP (address: http://www.firma.infocert.it/doc/manuali.htm);
- in electronic format in the public register of certification authorities maintained by AgID;
- in paper format, it may be requested from the Registration Authorities or the end-user contact.

9.10.9 Cases in which the OID must change

n/a

9.11 Dispute resolution

Please refer to the contractual documents governing the service for details of the dispute resolution procedures.

9.12 Competent court

Please refer to the contractual terms governing the service for details regarding the competent court.

9.13 Applicable law

The law applicable to this policy and practice statement is Italian law.

Below is a non-exhaustive list of the main applicable regulatory references:

[1] EU Regulation No 910/2014, as amended, 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 (also referred to as *the eIDAS Regulation*).

[2] Legislative Decree No. 82 of 7 March 2005 (Official Gazette No. 112 of 16 May 2005) – Digital Administration Code (also referred to as CAD) and subsequent amendments and additions

[3] Legislative Decree No. 196 of 30 June 2003 (Official Gazette No. 174 of 29 July 2003) – Privacy Code and subsequent amendments and Regulations, and 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 (in force since 25 May 2018).

[4] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and the relevant national transposition legislation.

[5] Preliminary assessment – 24 September 2015 [4367555] Processing of personal data as part of the 'Issuance process with webcam verification' for qualified or digital electronic signatures.

[6] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015, known as the Payment Services Directive – PSD2.

[7] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017, supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards.

[8] Certificate Policy – Certificate Practice Statement ICERT-INDI-MO

[9] CPS Addendum – Acceptable forms of identification.

All circulars and resolutions of the Supervisory Authority also apply, as well as the implementing acts provided for in the eIDAS Regulation [1].

9.14 Miscellaneous Provisions

Please refer to the contractual documents governing the service for any other provisions not included in this Manual.

9.15 Other provisions

Unless otherwise agreed in the contract, the service is available during the following hours:

Service	*Time*
Remote Signature Service	**From 00:00 to 24:00** **7 days a week (minimum availability 99.0%)**

Table 26 – Service availability times

APPENDIX A

Tools and procedures for applying and verifying digital signatures

Infocert provides a product (called 'Infocert Sign') which can be downloaded free of charge by signers or Users from the website www.firma.infocert.it to enable:

- all parties holding a certificate issued by Infocert to digitally sign documents;
- the verification of signatures affixed to digitally signed documents in accordance with the formats defined by the implementing acts of the Regulation.

The environments in which Infocert Sign operates, the hardware and software requirements, and all instructions for installing the product can be found at the web address given above. Instructions for using the product are included within the product itself and can be accessed via the help function. The Infocert Sign product is capable of signing any type of file. The ability to view the file depends on the availability of suitable viewing software on the user's workstation.

Infocert may make available, for a fee and in accordance with commercial agreements established from time to time with the RAs, subscribers, Entities or Users, additional signature and/or signature verification products or services. Electronic documents signed with certificates issued by Infocert may also be verified using other tools capable of interpreting the relevant signature formats. Such tools fall outside the scope of Infocert's responsibility.

For example, documents signed using certificates issued in accordance with the Infocert CA policy and practice statement, in PAdES format, can also be verified using Adobe Reader®.

WARNING

Some formats allow executable code (macros or commands) to be embedded within the document without altering its binary structure, and such code may activate functions capable of modifying the acts, facts or data represented in the document itself. Digitally signed files containing such structures do not have the legal effect referred to in Article 25(2) of the Regulation [1]; that is to say, they cannot be considered equivalent to a handwritten signature. It is the responsibility of the Signatory to ensure, using the standard features of each product, that no such executable code is present.