Technical Annex

Qualified signature and authentication certificates on a device or CNS, remote qualified signature and seal certificates and services

1. EXTERNAL REFERENCES 1
2. – SERVICE DESCRIPTION INTRODUCTION 1
3. TECHNICAL AND REGULATORY SPECIFICATIONS 4
4. SLA and KPIs 14

1. EXTERNAL REFERENCES

Documentation	Detailed links
CP and CPS (Policy and Practice Statement) for the issuance of qualified certificates	https://qtsp.infocert.it/pdf/ICERT_INDI_MO_ENG.pdf
CP and CPS (Policy and Practice Statement) for the issuance of authentication certificates	https://qtsp.infocert.it/pdf/ICERT_INDI_MOCA_ENG.pdf
SP and PS (Policy and Practice Statement) for qualified remote signature and seal services	https://qtsp.infocert.it/pdf/ICERT_INDI_SSAS_ENG.pdf
SP and PS (Policy and Practice Statement) for the Identity Verification Service	https://qtsp.infocert.it/pdf/ICERT-INDI-IPSPS_ENG.pdf
CP for CNS authentication certificates	https://qtsp.infocert.it/pdf/ICERT_INDI_CPCA_CNS_ENG.pdf
PDS (PKI Disclosure Statement) for qualified certificates	https://qtsp.infocert.it/pdf/ICERT_INDI_PDS-ENG.pdf
Support links (FAQs, videos, guides)	https://knowledgecenter.infocert.digital/

2. SERVICE DESCRIPTION – INTRODUCTION

Tinexta Infocert S.p.A. (hereinafter, "Infocert"), for the purposes of this document, acts as a qualified trust service provider (hereinafter, "QTSP" – Qualified Trust Service Provider), in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183 (hereinafter the "eIDAS Regulation"), for the provision of the following services:

- issuing qualified electronic signature certificates and electronic seals, either on a physical device or remotely;

- issuing authentication certificates, including those on CNS (National Services Card) devices;
- the provision of qualified electronic signature and seal services remotely.

These services (hereinafter collectively referred to as the "Service") are provided in accordance with the respective policy and practice statements (hereinafter also referred to as "CPS" – Certificate Practice Statement or "PS" – Practice Statement) and, where applicable, Infocert's PKI Disclosure Statement (PDS).

For the Services listed above, Infocert has obtained a conformity assessment from the conformity assessment body CSQA Certificazioni S.r.l., in accordance with the eIDAS Regulation and the applicable ETSI standards, including ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 431, in accordance with the eIDAS assessment scheme defined by ACCREDIA, in compliance with the standards ETSI EN 319 403 and UNI CEI EN ISO/IEC 17065:2012.

Infocert is also accredited by the Agency for Digital Italy (AgID) and is included in the European Trusted List of qualified trust service providers (Trusted Service List – TSL), published by the European Commission.

Within the scope of the Services covered by this Technical Annex:

- Infocert acts as a Certification Authority (CA) for the identification of individuals, and the issuance and management of qualified certificates and authentication services;
- Infocert also acts as a Server Signature Application Service Provider ('SSASP') for remote qualified electronic signature and seal services, including the management of remote devices used to create signatures or seals.

Qualified certificates and qualified electronic signature and seal services enable the signing of electronic documents with legal effect in accordance with the eIDAS Regulation. In particular, a qualified electronic signature has the same legal effect as a handwritten signature.

Authentication certificates, on the other hand, enable the digital identification of the subject and secure access to digital systems and services, ensuring a unique association between the subject and the credentials used.

The Service is based on public-key cryptographic mechanisms, which guarantee the authenticity of origin, data integrity and non-repudiation of the operations carried out. To this end, each subject is assigned a pair of cryptographic keys (public and private), linked to a digital certificate (hereinafter, the 'Certificate') containing the subject's identification details.

The cryptographic keys are generated, stored and used by means of secure devices for the creation of signatures or seals (Qualified Signature/Seal Creation Device – QSCD), which may consist of:

- physical devices held by the subject (e.g. smart cards, USB tokens);
- remote devices managed by InfoCert within high-security infrastructures

Certificates and associated services are identified by specific Object Identifiers (OIDs), which define the provider, the type of use and the applicable policies. A detailed description of the OIDs is contained in the respective policy and practice statements.

This Technical Annex forms an integral and essential part of the service purchase contract (hereinafter the "Agreement") entered into with the Customer.

The General Activation Condition (hereinafter the "GAC"), of which this Technical Annex forms an integral part, applies to any party that activates, uses or relies on the Service; it being understood that, in dealings with the Customer, the provisions of the Agreement also apply.

2.1 Definition of the Parties

Customer
A natural or legal person who has entered into the contract for the purchase of the Services ("Agreement"), thereby assuming the associated financial obligations. The Customer may be the same person as the subscriber.

Subject / Holder
A natural or legal person in whose name the Certificate is issued.
In the case of certificates issued in the name of a natural person, the subject is the person to whom the data contained in the Certificate relates and who uses the Certificate as part of the Service.
In the case of certificates issued to a legal person, the subject is the organisation to which the Certificate relates.

Subscriber
A natural or legal person who requests Infocert to issue Certificates and/or activate the Service. The subscriber may be the same as the Subject, if they are applying for a Certificate for themselves, or may be a third party requesting the Service on behalf of one or more Subjects.

In particular, the subscriber may:

- apply for certificates for themselves, as a natural person, and be the same as the Subject;
- request certificates relating to a legal entity, acting as its representative or delegate;
- be an organisation that is a subscriber for parties associated with it, within the context of, for example, commercial relationships (e.g. customers) or an organisational structure (e.g. employees or contractors).

User / Relying Party
A party that relies on a certificate, an electronic signature, an electronic seal or a certificate-based authentication process for the purpose of verifying the Subject's identity, the origin of a document or the integrity of data.

Issuing Authority
An entity responsible for issuing physical devices (such as smart cards or tokens) intended to contain CNS (National Services Card) authentication certificates. The Issuing Authority is responsible for the issuance process and for managing the lifecycle of the CNS device.

Interested Third Party
A natural or legal person with an interest in the information contained in the Certificate relating to the Subject's role and/or organisation, and who is authorised, where applicable, to request its amendment, suspension or revocation. This may be the same as the subscriber.

3. TECHNICAL AND REGULATORY SPECIFICATIONS

3.1 Provision and Use of the Service

The Service is provided by Infocert to the Customer, in accordance with this Technical Annex, the General Activation Conditions (GAC), the applicable legislation and the relevant policy and practice statements.
The issue of certificates and the activation of the Service are subject to the submission of an activation request prepared by Infocert (hereinafter, the "Activation Request"). This request consists of a form, which may also be in electronic format, that expressly refers to this Technical Annex, the GTC and the Privacy Policy as the contractual terms of the Service.
In the case of certificates issued in the name of a natural person, the Activation Request is accepted or signed by the Individual.
In the case of certificates issued in the name of a legal person, the Activation Request is accepted or signed by the subscriber, acting as a representative or authorised person, in accordance with the policy and practice statements.
The activation of the Certificate by Infocert is subject to the successful completion of the Subject's identification procedure, carried out in accordance with the procedures described in the policy and practice statements. Should the identification procedure fail, the Certificate cannot be used.
The Service is deemed to be activated following acceptance of the Activation Request and the subsequent issue of the Certificate, together with the generation of the cryptographic key pair, carried out on a physical device or, in the case of remote Services, on infrastructure managed by Infocert in its capacity as an SSASP.
The Certificate may be used by the User to sign electronic documents or to authenticate access to digital services, using tools at their disposal or made available by Infocert or the subscriber, in accordance with the procedures set out by the Service.
Infocert, in its capacity as a Certification Authority and, where applicable, as a Server Signature Application Service Provider (SSASP), retains information relating to the identity of the Subject, the Certificate, the cryptographic keys and the service logs for a period of not less than twenty (20) years from the expiry of the Certificate and, in any event, not exceeding twenty–three (23) years from its date of issue, in accordance with the provisions of the applicable legislation and the policy and practice statements.
In the event of cessation of business, Infocert shall arrange for the transfer of the aforementioned information to a third party that guarantees compliance with the same security and retention conditions, in accordance with applicable legislation and the policy and practice statements.
The General Terms and Conditions (GTC), this Technical Annex, the relevant policy and practice statements and the applicable information documentation are made available by Infocert on its official website and may be consulted by the Entity, the subscriber and any relying parties prior to the activation and during the use of the

3.1.1 Digital Certificate and cryptographic keys

The Digital Certificate is an electronic document, issued and signed by Infocert in its capacity as a Certification Authority, which certifies the association between the Subject's identity and a pair of cryptographic keys (public key and private key), used for electronic signatures, electronic seals or authentication.
The private key is used by the Subject to carry out signing, sealing or authentication operations,

whilst the public key is made available via the Certificate for the purpose of verifying these operations.
The cryptographic keys are generated and used by means of secure cryptographic devices, in accordance with the applicable legislation and the relevant policy and practice statements.
Infocert guarantees the correct association between the Subject, the Certificate and the cryptographic keys, in accordance with the provisions of the applicable legislation and the policy and practice statements.
The Certificate may contain restrictions on its use and/or scope. Any restrictions on the use of the Certificate are set out in the Certificate itself and/or in the policy and practice statements.

3.1.2 Identity verification process

The identification of the Subject is carried out by Infocert in its capacity as a Certification Authority (CA) or by a delegated party acting as a Registration Authority (RA).
The identification procedures are set out in the IPSPS policy and practice statement and comply with the applicable regulations.

A) Natural person

The Subject is identified using one of the prescribed methods, based on verification of identity through identification documents and/or electronic identification tools, as well as on the collection of the information necessary for the issue of the Certificate.

B) Legal entity

Where certificates or digital seals are issued in the name of a legal person, the subscriber (legal representative or delegate) is identified in accordance with the procedures laid down for natural persons.
Infocert also verifies the subscriber's powers of representation and the details relating to the legal entity, for the purposes of issuing the certificate and ensuring it is correctly associated with the entity.

3.1.3 Authentication Process

The use of the private key associated with a certificate is subject to the authentication of the Subject, in order to ensure exclusive control over the use of data for the creation of the electronic signature or seal.
The Subject is authenticated through the use of credentials and/or devices associated with them, in accordance with the procedures set out by the Service and the policy and practice statements.
In the case of signature and/or authentication devices (such as smart cards, tokens or CNS), authentication takes place through the use of a personal code or other equivalent mechanism provided by the device.
In the case of remote signature or seal services, authentication is managed by Infocert, in its capacity as SSASP, or by a delegated party, using the mechanisms provided for by the Service.
The authentication and activation process ensures that the private key is used under the Subject's sole control and that every operation can be traced back to them.

3.1.4 Renewal of the Service and reissue of the certificate with a new key

Renewal of the Service consists of its continuation beyond its expiry date, where applicable, and, in the case of certificates, involves the issue of a new Certificate and the generation of a new pair

of cryptographic keys.
Renewal may be requested before the expiry of the Certificate or the Service, in accordance with the procedures set out in the policy and practice statements.
Renewal is not permitted in the cases set out in the policy and practice statement and, in any event, where the Certificate or Service has expired, been revoked or suspended, or where the data and information associated with the Entity are no longer valid or up to date. In such cases, a new activation is required. The procedure for reissuing the certificate is described in the relevant policy and practice statement.

3.1.5 Suspension or Revocation of the r Service

The Certificate or the Service may be suspended or revoked in accordance with the procedures set out in the policy and practice statements.
Suspension or revocation may take place at the request of the Subject or the subscriber, where applicable, or on the initiative of Infocert in the cases set out in the applicable legislation or the policy and practice statements.
Suspension entails the temporary interruption of the Certificate's validity or the use of the Service, whilst revocation results in their definitive termination.
Following suspension or revocation, the use of the Certificate or the Service is no longer permitted.
In the case of remote signature or seal services, suspension entails the blocking of the use of cryptographic keys, whilst revocation results in their destruction, in accordance with the policy and practice statements.

3.1.6 Reliance on the Service

In order to rely on a signed electronic document or on a certificate-based authentication process, the User / Relying Party is required to verify the validity of the Service's output and its suitability for the intended use,
To this end, they must verify the validity of the Certificate, the outcome of the signature, the electronic seal or the authentication process, any restrictions on use or validity, and that the Certificate has been issued by a trust service provider compliant with the applicable legislation, including through tools made available by Infocert, public validators of the European Union or any third-party tools, for which Infocert provides no guarantee.

3.2 Products and Services

3.2.1 Qualified Signature and Authentication Certificates on a Device

The devices held by the subject, which contain the cryptographic keys of the Certificate, may contain, in addition to qualified signature certificates, 'authentication certificates' or 'authentication certificates – CNS'.
The Certificates are identified by Object Identifiers (OIDs), i.e. a code that identifies the QTSP, the intended use of the Certificate and the policy with which it complies.
The OIDs relating to qualified signature certificates on physical devices are described in paragraph 1.2 of the ICERT-INDI-MO policy and practice statement.
The OIDs relating to authentication certificates on physical devices are described in paragraph 1.2

of the ICERT-INDI-MOCA policy and practice statement.
The OIDs relating to CNS authentication certificates are described in section 2.1 of the ICERT-INDI-CPCA-CNS policy and practice statement.

The configurable devices, all of which are fitted with an internal cryptographic chip, are as follows:

- The USB or wireless token (hereinafter also referred to as *the 'business key')* is a device that can be used on any PC equipped with a USB port or wireless connection.
  To use the business key, simply connect it to the computer's USB port or wireless connection, install the drivers and software provided (if necessary), and launch the signing software to select the documents to be signed or access online digital services by entering the PIN associated with the device.

- A *smart card* is an electronic card that requires a dedicated smart card reader in order to be used. To use the smart card, you must connect the smart card reader to the computer via a USB cable, insert the card into the reader, check that it is recognised by the relevant drivers, and use compatible software to apply digital signatures or access online services via authentication.

These devices can be used to apply digital signatures using a Qualified Signature Certificate or to authenticate access to certain online services using an Authentication Certificate or CNS authentication. Should a security flaw be discovered that compromises its compliant use, the device may become unusable and must be replaced as soon as possible to prevent the signatures issued from being invalidated.
Certificates may contain further usage restrictions, as described in more detail in the relevant policy and practice statement

3.2.1.1 Qualified Signature Certificates on a device

These certificates are issued on secure physical devices such as smart cards or business keys. The subject is required to take good care of the signature device and the associated access credentials, adopting appropriate organisational and technical measures to prevent harm to third parties and to ensure the exclusively personal and secure use of the device and credentials.
The Qualified Signature Certificate is valid for three years from its date of issue, or until the date of publication of its revocation or suspension, if these occur prior to the expiry date.

3.2.1.2 Device-based Authentication Certificate

The Authentication Certificate issued by Tinexta Infocert serves as a digital tool for the subject's authentication. The Authentication Certificate is used for the subject's digital identification and for secure access to digital services. The procedures for its issue, management and use are set out in the ICERT-INDI-MOCA policy and practice statement. It can be used for a variety of digital services requiring a high level of security, such as secure authentication, access to IT systems and encrypted transactions. The process for the issue, management and use of the Certificate is strictly governed by the ICERT-INDI-MOCA policy and practice statement.
The Authentication Certificate is valid for three years from its date of issue, or until the date of publication of its revocation or suspension, if these occur prior to the expiry date.

3.2.1.3 CNS Authentication Certificate – National Services Card

The CNS Authentication Certificate is issued by an 'Issuing Authority' and serves as a digital means of authenticating the subject for access to dedicated online services. The Issuing Authority grants Tinexta InfoCert a non-exclusive mandate to act as a Certification Authority (CA) for the issue of CNS certificates. The Issuing Authority authorises Tinexta InfoCert, in its capacity as a CA, to delegate the processing of CNS applications and the issue of CNS certificates to third parties appointed by InfoCert as Registration Authorities.

This certificate is essential for guaranteeing the integrity and authenticity of the subject's digital communications, by unequivocally linking their identity to the registered public key. The process of issuing, managing and using the Certificate is governed by the InfoCert policy ICERT-INDI-CPCA-CNS, available on the Certification Authority's website, and by the Issuing Authority's policy and practice statement, available on the latter's website.

The operational procedures adopted by the Issuing Authority and by the Certification Authority itself for the provision of digital certification services are set out in the CNS policy and practice statement drawn up and made available by the Issuing Authority itself.

The CNS Authentication Certificate is valid for three years from the date of issue, or until the date of publication of its revocation or suspension, if these occur prior to that date. The Certificate and the device may be renewed only once. After the first renewal, the Certificate and the device must be reissued

3.2.2 Qualified Certificates for Remote Signatures/Seals and Remote Signature and Seal Services

In the context of the remote services described in this section, Tinexta Infocert acts as a Certification Authority with regard to the identification of the individual and the issue of the qualified certificate, whilst it acts as an SSASP with regard to the remote activation and management of keys for the use of the qualified signature associated with that specific certificate.

The specific OIDs relating to qualified certificates for remote signatures and seals are described in paragraph 1.2 of the ICERT-INDI-MO policy and practice statement.

The specific OIDs relating to the remote signature and seal service are described in paragraph 1.2 of the ICERT-INDI-SSAS policy and practice statement.

3.2.2.1 Remote Signature

In the event of a request for a Remote Signature Certificate, the Service involves the generation of a pair of cryptographic keys and the issuance of a Qualified Remote Electronic Signature Certificate valid for three years. Remote signing enables the subject to apply digital signatures without the need to use personal physical devices, such as USB tokens or smart cards.

Remote signing certificates issued by Tinexta Infocert are used via specific IT procedures that connect securely to the Remote Signing service provided by Infocert in its capacity as an SSASP. This service is provided through the use of a secure cryptographic device (**QSCD**) managed by the QTSP.

The Service provides the subject with an IT procedure, implemented on Infocert's systems or those of the subscriber (if different from the subject), through which the subject can manage their own Subscription Certificate and keys.

Remote Signature Certificates may be issued within a domain provided by the subscriber other than the subject. Should the Subscriber request the issue, on behalf of the Certificate Holders, of

certificates whose use is restricted exclusively to the IT domain for which they were issued, such certificates may only be used within the domain(s) defined by the Subscriber. These certificates are classified as Long-Term and may be subject to one of the usage restrictions set out in the policy and practice statement.
The cryptographic keys required for signing are stored in a QSCD, managed by Infocert. The subject retains exclusive control over the application of the signature through an authentication process, which may, for example, involve the combined use of a PIN and an OTP. Each signing session requires a new authentication to ensure the security of the process, and operations can be carried out on both desktop computers and smartphones, and may be managed by the SSASP or by a delegate appointed by the SSASP.
Remote signing can be carried out using signing applications provided by Infocert or can be integrated via API into the application provided by the subscriber.
Remote signing requires the configuration of a username and password and can be activated either directly via the TOP (*Trust Onboarding Platform*) process or via the Tinexta Infocert MySign portal, in accordance with the instructions sent by email, which the subject can access using the aforementioned credentials to manage the certificate in terms of authentication methods, usage and revocation; or via the procedures provided by the subscriber's application.
The private key is used following a specific request for a signature or seal relating to the Subject, subject to authentication and in accordance with the security mechanisms provided by the Service. The process for activating the signature or seal is structured to ensure the Subject's expression of intent in relation to the individual transaction and their exclusive control over the use of the private key stored in the remote QSCD.

3.2.2.2 Automatic remote signature

An automatic signature is a form of remote signature in which the subject uses a key pair specifically intended for this purpose, distinct from all others in their possession, in accordance with the provisions of Article 35(3) of the CAD.
In addition to the provisions of paragraph 3.2.2.1 of this Technical Annex, the Service allows for the automatic generation of signatures on documents sent via automated IT procedures. In such cases, no specific confirmation is required for each individual transaction, as the subject's intent is expressed within the framework of the previously authorised automated procedure. The management of the automatic signature service includes the authentication of the subject using specific tools and the remote management of the digital certificate. The process therefore involves the issue of an automatic signature certificate containing the following usage restriction: *"This certificate is valid only for signatures applied via an automated procedure".*
The automatic signing of documents is carried out by the system only after the Subject has activated the Certificate, without any further human intervention unless the Subject requests a temporary suspension of the Certificate or of its use in the automated procedure. Initial access to the system is via a pre-defined authentication mechanism, which is required only during the first session; thereafter, documents are signed automatically upon upload, in accordance with the authorisations granted. The automatic signature referred to in this paragraph utilises a specific Certificate, intended solely for this type of use. The subject is required to use different Certificates for different automated procedures, in order to minimise the security risks associated with misuse. Only one IT procedure for the transmission of documents may be associated with each Certificate used for an automated signing procedure.

3.2.2.3 One Shot Remote Signature

The One Shot digital signature certificate (hereinafter 'OS' or **'OS** Service') is a remote signature certificate with a validity period limited to the time required to execute the signatures. Where OS Certificates have a duration of 60 minutes, the validity period is shorter than the maximum time required to process a revocation request from the subscriber or the Subject, as specified in the Reference Manual. Once the certificate has been issued and the keys have been used within a signing procedure, the certificate issued by the QTSP expires and the keys must be destroyed. The process therefore involves the issue of an OS signature certificate containing the following usage restriction: *"This certificate may only be used within the specific session or signing procedure for which it was issued."*

The OS Service enables the Holder, subject to verification of their identity and confirmation via an OTP code, to authenticate themselves and use the Remote Signature linked to the Certificate. The issue of the Certificate by Infocert to the Holder is subject to the successful completion of the necessary identification and verification procedure, in accordance with the procedures set out in paragraph 3.1.2 of this Technical Annex.

If the Customer has purchased a pay-as-you-go One Shot signature package from Infocert's e-commerce site or from one of its resellers, these signatures must be used by the Customer within one year of purchasing the package.

3.2.2.4 Qualified electronic seal certificates

Infocert, in its capacity as a Certification Authority, issues qualified electronic seal certificates in the name of legal entities, which enable the subject organisation to affix electronic seals to electronic documents in order to guarantee their origin and integrity.

Qualified seal certificates may be issued in conjunction with the remote seal affixing service provided by Infocert. In this model, Infocert also acts as an SSASP and manages the seal keys within qualified devices for seal creation. The seal affixed via this service is qualified.

This category includes the standard remote qualified seal service and the remote qualified seal service for use within the EPREL framework. EPREL, the European Product Registry for Energy Labelling, is the European Union's database for products subject to energy labelling, which contains the information necessary to ensure transparency and compliance with relevant European legislation.

Infocert may also issue qualified seal certificates not associated with the remote seal affixing service. In such cases, the keys are used on devices or infrastructure under the control of the subscriber or the Organisation. If the device used is not a qualified device for seal creation, the affixed seal is not qualified, but constitutes an advanced electronic seal based on a qualified certificate.

Qualified seal certificates not associated with the remote service also include certificates with the PSD2 extension, intended for specific regulated areas within the payment services sector.

The application for the issue of a qualified seal certificate must be submitted by a natural person acting in the name and on behalf of the Organisation subject to the seal. Infocert verifies the subscriber's powers of representation and the details relating to the Organisation in accordance with paragraph 3.1.2 of this Annex.

3.3 Obligations and Responsibilities

3.3.1. Obligations and Responsibilities of the User.

The obligations and responsibilities of the User, in relation to the activation and use of the Service, are determined by the applicable legislation, this Technical Annex, the General Terms and

Conditions and the Privacy Policy in force on the date of the Activation Request.
The User is responsible for the truthfulness and accuracy of the data provided as part of the identification process and the Activation Request. Should the User provide untruthful information or engage in conduct likely to compromise the proper identification process, the User shall be liable for any damages that may arise to Infocert and/or third parties, and shall indemnify Infocert against any claims for compensation.
The Data Subject is required to use the Certificate and the Service exclusively for the intended purposes and in compliance with any restrictions on use and/or value specified in the Certificate and in the policy and practice statements.
In the case of certificates on a physical device, the User is required to take due care in safeguarding the device and the relevant access codes or credentials, preventing their use by third parties.
In the case of remote services, where the keys are held by Infocert or by infrastructure managed by it, the User is required to protect the authentication and activation tools for the Service, such as credentials, codes, devices or authentication applications, keeping them personal and confidential.
The User is responsible for transactions carried out using their Certificate and/or via the Service, as well as for any documents signed, even where the IT procedure or documents are made available by the subscriber or by third parties.
The User is required to check the content of documents before signing them and to ensure that they reflect their own intentions.
The User must promptly request the suspension or revocation of the Certificate or the Service in the cases provided for in the policy and practice statements, and is liable for any damages arising from delays in initiating such procedures.
The Party is also required not to use the Certificate or the Service after its expiry, suspension or revocation.
The Subject is also required to notify Infocert without undue delay of any suspicion of compromise, unauthorised use or loss of credentials or authentication tools.

3.3.2 Obligations and Responsibilities of the Subscriber

The obligations set out in this paragraph apply to the subscriber in relation to the role actually performed within the scope of the Service.
It is understood that the Activation Request is signed by the Subject in accordance with the provisions of paragraph 3.1. Where the subscriber is the same as the Subject, the obligations set out for the Subject in paragraph 3.3.1 shall apply in the first instance, without prejudice to the application of the Agreement where the same person is also the Customer.
The subscriber is subject to the GTC, this Technical Annex and the Privacy Policy; where the subscriber is also the Customer, the provisions of the Agreement shall also apply.
The subscriber is required to provide Infocert with accurate, up-to-date and complete data as part of the Service activation process, as well as, where applicable, information relating to the organisation, role or powers of representation to be associated with the Certificate.
Where the subscriber acts in the name and on behalf of a legal entity, they are responsible for the accuracy of the information relating to that entity and for ensuring that they possess the necessary powers to request the activation of the Service or the issue of the Certificate relating to the legal

entity.
Where the subscriber makes the Service available to parties associated with it, within the context of commercial relationships or an organisational structure, they are responsible for managing the Service within their own processes, applications or infrastructure, as well as for its correct integration and interaction with Infocert's systems.
In such cases, the subscriber is responsible for the accuracy and traceability of any documents made available to the User for the purposes of using the Service, it being understood that the expression of intent and the use of the Certificate remain the responsibility of the User.
Where the Subscriber manages user interfaces, applications or front-end components through which the Subject accesses the Service, they are required to develop and maintain them in accordance with the guidelines provided by Infocert, ensuring compliance with current legislation and the prescribed security requirements.
Where the subscriber manages, even indirectly, components of the authentication or activation process for the Service, they are required to ensure that such components are consistent with the procedures and security levels specified for the Service.
Where the subscriber makes the Service available to Users, they are required to ensure that the Users are able to access Infocert's contractual documentation relating to the activation and use of the Service.
The subscriber is required to adopt appropriate technical and organisational measures to ensure the security of the systems, applications and processes used to provide the Service and to interact with Infocert's systems.
The subscriber must not permit the use of the Certificate or the Service after its expiry, suspension or revocation, and must cooperate with Infocert where it is necessary to initiate the relevant procedures.
The subscriber indemnifies Infocert against any liability arising from the non-compliant use of the Certificate or the Service within the scope of its own processes, applications or infrastructure.
The subscriber is also liable for any fraudulent or unauthorised use of the Certificate or the Service by its employees, contractors or authorised users within its organisation or infrastructure.
The subscriber undertakes to cooperate with Infocert in the event of audits, inspections or checks requested by the competent authority or arising from applicable legislation, providing the documentation and information reasonably required.

3.3.3 Infocert's obligations and responsibilities

Infocert's obligations and responsibilities are exclusively those set out in the applicable legislation, this Technical Annex, the General Activation Conditions (GAC), the Agreement where applicable, and the relevant policy and practice statements.
Infocert, as a provider of qualified trust services, delivers the Service in accordance with the requirements set out in the eIDAS Regulation and the applicable technical standards, as described in the policy and practice statements.
In particular, Infocert is required to:

- ensure that the Service is provided in accordance with the procedures and service levels set out in the policy and practice statements;

- ensure the correct association between the Subject and the Certificate on the basis of the identification procedures adopted;
- manage the lifecycle of Certificates and, where applicable, cryptographic keys, in accordance with the provisions of the policy and practice statements;
- store, in a dedicated, non–modifiable digital archive, the Certificates issued, the identification records and the logs relating to the Service, in accordance with current legislation and in the manner set out in the policy and practice statements.

It is understood that Infocert assumes no obligations beyond those set out above.
In particular, Infocert gives no warranty regarding:

- the proper functioning and security of systems, hardware or software not supplied directly by Infocert, used by the Party or the subscriber to access or use the Service;
- the use of the Certificate or the Service for purposes other than those intended or in breach of any restrictions on use and/or as set out in the Certificate or in the policy and practice statements;
- the proper functioning of communication networks or data transmission systems not directly managed by Infocert;
- the validity, effectiveness or legal relevance of signatures, seals or authentication processes in legal systems other than the Italian one, except to the extent that such effects are expressly recognised and governed by applicable European legislation;

Infocert is not liable for the content of signed documents or for any declarations or expressions of intent made by the User whilst using the Service.

3.3.4 Role and Organisation

In accordance with the policy and practice statement and applicable legislation, including Article 28(3) of the Digital Administration Code (CAD) and AgID Decision No. 121/2019, as amended, the Subject or the subscriber, where applicable, may request that information relating to the Subject's role be included in the Certificate.
Such information may include, by way of example:

- professional qualifications and/or licences;
- powers of representation of natural or legal persons;
- membership of organisations or bodies;
- the exercise of public functions.

The inclusion of such information is carried out in accordance with the procedures set out in the policy and practice statements and is subject to the consent of the Third Party, where required.
The Third Party is the person responsible for the information relating to the role or organisation indicated in the Certificate; this may, but need not, be the same as the subscriber. The Third Party is responsible for ensuring that this information is accurate and up to date and may, in the cases provided for, request the amendment, suspension or revocation of the Certificate.
Where the Certificate states that the Subject belongs to an organisation, it is the responsibility of the Interested Third Party to notify Infocert promptly of any changes relating to such membership.
Applications for certificates that include references to organisations are accepted only if they relate to legal entities with an identifiable and verifiable legal form. Information relating to the

organisation (such as its name or identification details) is included in the Certificate only following the organisation's express authorisation, in accordance with the provisions of the relevant policy and practice statement.

4. 's SLA and KPIs

In terms of service delivery, the monthly service availability figures are set out in detail in the relevant policy and practice statement.