Technical Annex
Advanced Electronic Signature

Contents

***

1. EXTERNAL REFERENCES

Documentation	Detailed links
CP and CPS (Policy and Practice Statement) for the issuance of non-qualified certificates for advanced electronic signatures	https://qtsp.infocert.it/pdf/ICERT_INDI_FEA-ENG.pdf
PDS (PKI Disclosure Statement) for the issuance of non-qualified certificates for advanced electronic signatures	https://qtsp.infocert.it/pdf/ICERT-INDI-PDSFEA-ENG.pdf

2. SERVICE DESCRIPTION – INTRODUCTION

Tinexta Infocert operates as a provider of qualified and non-qualified trust services. The Service described in this Technical Annex is an advanced electronic signature service using a non-qualified certificate (hereinafter also referred to as **the** "Service"), in accordance with the ICERT-INDI-FEA policy and practice statement (hereinafter also referred to as the "CPS") and the ICERT-INDI-PDSFEA *PKI Disclosure Statement* (hereinafter referred to as the "PDS"). For this Service, Tinexta Infocert has obtained a conformity assessment carried out by the Conformity Assessment Body CSQA Certificazioni S.r.l., in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 (hereinafter referred to as **the "eIDAS** Regulation") and the standards ETSI EN 319 401, ETSI EN 319 411-1**,** in accordance with the eIDAS assessment scheme defined by ACCREDIA against the standards ETSI EN 319 403 and UNI CEI-ISO/IEC 17065:2012 (collectively, hereinafter, **the 'Applicable** Regulations').

The Advanced Electronic Signature (hereinafter also referred to as 'AES' or **'AES** Service') is the tool that allows you to sign documents directly from a PC or smartphone. It is the result of a cryptographic transformation of data that provides a mechanism for verifying the origin and integrity of the data, as well as the non-repudiation of the signature. The cryptographic keys used for this operation are stored on a remote device. The keys are linked to an individual via a non-qualified digital certificate (hereinafter also referred to as the "Certificate"), which contains their identifying details.
The encryption keys are generated, stored and used via a secure device known as a 'Signature Creation Device' (hereinafter also referred to as 'SSCD').
The key pair is generated on a cryptographic device known as an 'HSM' (Hardware Security Module) at Tinexta Infocert's premises.
The type of Certificate is identified by a number called an "O.I.D." (Object Identifier), which is a code that identifies the Certification Authority Tinexta Infocert, the purpose of the Certificate and the *"policy and procedure"* with which it complies. The full definition and description of O.I.D.s can be found in the CPS (Certificate Practice Statement).
The issued certificate is signed by a Certification Authority ("CA"), in this case Tinexta Infocert, which has been recognised by Adobe and is therefore included in the trusted certificate store known as the "AATL" (Adobe Approved Trusted List).
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

Subject/Holder: The Subject, also referred to as **the Holder**, refers to the natural or legal person who holds the non-qualified certificate. This subject is the user of the services offered and has their key identifying details included in the certificate.

Subscriber: The Subscriber is the natural or legal person who requests Tinexta Infocert to issue digital certificates for a Subject. **The Subscriber may be the same as the Subject/Certificate Holder** when a natural person applies for a Certificate for themselves. In other situations, the Subscriber may be an entity or organisation acting on behalf of natural persons linked by commercial relationships or within the framework of an organisational structure.

Interested third party: a natural or legal person who is interested in and/or responsible for the information included in the certificate relating to the Role and/or the Organisation.

3. TECHNICAL AND REGULATORY SPECIFICATIONS

3.1 Provision and Use of the FEA Service

The FEA Service is provided by Tinexta Infocert to the Party, pursuant to this Technical Annex and the Agreement entered into with the Party.
The Subscriber must request Tinexta Infocert to register and issue the Certificate in accordance with the procedures set out in the policy and practice statement, using the specific Activation Request provided by Tinexta Infocert (hereinafter **the "Activation** Request").
The issue of the Certificate by Tinexta Infocert to the Subject is subject to the successful completion of the prior and necessary identification procedure for the Subject, as set out in paragraph 3.2.3 of the CPS and in paragraph 3.1.3 of this document.
Therefore, should the identification process fail, the Certificate will not be issued; whereas, should the identification process be successful, the Certificate is issued to the Subject in accordance with the CPS.
The issued Certificate may be used to sign documents using tools made available by Tinexta Infocert or by the Non-Subject Subscriber, to unlock the signing keys and, after completing an authentication process using dedicated tools, the CA will retain information relating to the subject's true identity for at least twenty (20) years from the expiry of the certificate, up to a maximum of 23 (twenty-three) years from the date of issue.
In the event that Tinexta Infocert ceases trading, it shall arrange for the transfer of such information to third parties, under the same conditions set out herein, as specified in the policy and practice statement.

3.1.2 Digital Certificate

A digital certificate is an electronic document, signed by Tinexta Infocert, which certifies the association between the Subject and their pair of cryptographic keys (public and private).
The keys are generated and managed in a secure cryptographic device under the control of Tinexta Infocert.
Tinexta Infocert guarantees the correct association of the keys with the Subject by issuing the Certificate in accordance with the Applicable Regulations and the policy and practice statement.

3.1.3 Identity verification process

Only the documents listed in the "CPS Addendum – Acceptable Identity Documents" available on the Tinexta Infocert website at the following link are acceptable: https://qtsp.infocert.it/pdf/CPS_identity_docs.pdf.
The identification methods listed below are described in detail in section 3.2.3 of the CPS:

- LiveID
- AMLID
- SignID
- AutID
- VideoID
- SelfID

Where required, before proceeding with identification, the subject must ensure they are in possession of the original identity documents and their tax code or equivalent unique identifier.
The documents must be originals, in good condition and valid.

3.1.4 Certificate Renewal

The Data Subject may renew the Certificate, prior to its expiry, using the tools made available by Tinexta Infocert. The renewal request is signed with the private key corresponding to the public key contained in the Certificate to be renewed.
The outcome of the renewal is, in effect, the issue of a new Certificate.
Renewal is not possible if the attributes specified in the Certificate are no longer valid.
Once the Certificate has been revoked or has expired, it cannot be renewed and a new identification process is therefore required.
With regard to the provisions on duration and renewal set out in the Agreement, should the Subject give notice of termination prior to the automatic annual renewal of the said Agreement, the ability to use the Certificate will be blocked and, at the request of the Subject and/or, where applicable, the subscriber, the Certificate will be revoked.

3.1.5 Suspension or Revocation of the Certificate

The certificate may be revoked or suspended upon a certified request from the Subject or the non-Subject subscriber (an Interested Third Party where the latter has given their consent to the inclusion of the Role), or on the initiative of the CA.
Further details on this matter are set out in the policy and practice statement.

3.2 SERVICES

3.2.1 Non-qualified advanced remote signature certificates

The advanced remote signature certificates referred to in the following paragraphs are identified by the following Object Identifiers (OIDs):

Service	OID
Issuance of a non-qualified certificate for advanced remote signature	1.3.76.36.1.1.8.3
Issuance of a non-qualified certificate for automated advanced remote signature	1.3.76.36.1.1.8.5

3.2.2. Remote signature

The Service involves the generation of a pair of cryptographic keys, the issue of a non-qualified certificate for advanced electronic signatures with a three-year validity period, subject to any different validity period that may be established by current legislation, and the signature service.
Remote signing enables the subject to apply digital signatures without the need to use personal physical devices, such as USB tokens or smart cards.
Non-qualified certificates for advanced remote signing procedures, issued by Tinexta Infocert, are used via specific IT procedures that connect securely to the signing service provided by Tinexta Infocert.
The Service provides that the Subject is given access to an IT procedure, implemented on the systems of Tinexta Infocert or the non-Subject subscriber, where applicable, through which the Subject can manage their own Certificate.

The cryptographic keys required for signing are stored in an SSCD, managed by Tinexta Infocert.

The subject retains exclusive control over the application of the signature through a substantial or high-level authentication process, which typically involves the combined use of a PIN and an OTP.
Where applicable, authentication may be delegated to the subscriber.
Each signing session requires a new authentication to ensure the security of the process, and operations can be carried out on both desktop and mobile devices.
Remote signing can be carried out using signing applications provided by Tinexta Infocert, or integrated via an API (Application Programming Interface) into the application provided by the non-subject subscriber.

3.2.3. Automatic remote signing

Automatic signing is a specific application of electronic signatures, used remotely. The subject must use a pair of cryptographic keys dedicated exclusively to this function, distinct from those used for other purposes, ensuring compliance with the security and integrity requirements set out for advanced signatures.

In addition to the provisions of paragraph 3.2.1 of this Technical Annex, the Service allows for the automatic generation of signatures on documents sent via automated IT procedures. In such cases, it is not necessary for the subject to confirm their intention to sign, as they are aware of the documents generated by the aforementioned IT procedure.
The management of the automated 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 automated signature certificate containing the following restriction on use:
"This certificate is valid only for signatures applied via an automated procedure".
Documents are automatically signed 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 PIN and OTP, which are 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.
Each digital certificate for an automatic signing procedure may be associated with only one IT procedure for the transmission of documents.

3.2.4 One-shot remote signature

The One Shot Advanced Electronic Signature (hereinafter **'FEA** OS') is a remote signature whose keys, once generated, are available solely and exclusively for the signing transaction for which they were generated. Immediately after their use, the private key is destroyed.

The FEA OS allows the subject, subject to verification of their identity and confirmation via an OTP code, to authenticate themselves and use the FEA OS linked to the Certificate, within the Certificate's validity period – which is 60 minutes or 30/45/60 days – for the purpose of signing electronic documents. Certificates with a validity period of 60 minutes are valid for less than the maximum time required to process a revocation request; therefore, these certificates cannot be revoked.

The issue of the Certificate by Tinexta 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 3.1.3 of this Technical Annex.
Notwithstanding the provisions of the Agreement regarding withdrawal, since the FEA OS, by its very nature, requires immediate execution, the Subject, if a Consumer, expressly accepts the loss of the right of withdrawal pursuant to Article 16(a) of Directive 2011/83/EU on consumer rights and subsequent amendments and additions, provided that this provision is applicable to the specific context.
Where the Certificate has a duration of 60 minutes, by way of derogation from the provisions of paragraph 3.1.5 of this document, given that the duration of the Certificate is less than or equal to the minimum time (60 minutes) required to make public the information regarding its subsequent invalidity, no provision is made for the revocation or suspension of such certificates.
Where the Certificate has a validity period of 30/45/60 days, the contract relating to the FEA OS Service is
subject to the condition precedent of the successful completion of the identification process, which must take place no later than
30/45/60 days.

3.3 Obligations and Responsibilities

3.3.1. Obligations and Responsibilities of the Data Subject and the Non-Subject Subscriber

The obligations and liabilities of the Subject and, where applicable, of the Non-Holder Subscriber are determined by the Applicable Regulations, this Technical Annex, the relevant policy and practice statement, and the Agreement in the version in force on the date of the Activation Request.
If, at the time of identification, the Subject conceals their true identity, or if the Non-Subscriber subscriber or the Subject themselves act in a manner that compromises the identification process and the related findings set out in the Certificate, they shall be held liable for any damages incurred by Tinexta Infocert and/or third parties arising from the inaccuracy of the information contained in the Certificate.
The Non-Subject Subscriber and/or the Data Subject are obliged to indemnify and hold Tinexta Infocert harmless against any claims for damages. The Non-Holder Subscriber and/or the Data Subject are also liable for any damages incurred by Tinexta Infocert and/or third parties in the event of a delay in initiating the procedures for the revocation or suspension of the Certificate, as set out in the policy and practice statement. Furthermore, they must ensure compliance with the hardware and software requirements necessary for the correct use of the certificates.
The Subject and the Non-Holder Subscriber are solely responsible for the documents which, via Tinexta Infocert's applications or those of the Subscriber himself, are transmitted for the purposes of signing; they therefore assume full and absolute responsibility for the functioning of the relevant IT procedure and for the content, validity and ownership of such documents, thereby relieving the Certification Authority of any and all liability in this regard.

3.3.2. Specific Obligations of the Subject

The authentication tools (for example, the PIN, the OTP or the device that generates it) used for the Certificate activation procedure are strictly personal. Consequently, the subject is required to safeguard the confidentiality of these tools, refraining from communicating or disclosing them to third parties, even in part, and keeping them in a secure place.

The Certificate Holder, being aware that the use of a Certificate is attributable solely to them, is obliged to exercise the utmost care in the identification, use, storage and protection of the authentication tools made available by Tinexta Infocert or by the non-Certificate subscriber.
They must exercise the utmost care when using the digital signature certificate, verifying the content of the documents to be signed and ensuring that they reflect their intentions.
They are also required not to use the Certificate after it has expired, been revoked or suspended.
They are responsible for the accuracy of the information provided during identification and in the Activation Request.

3.3.3 Obligations of the Non-Subject Subscriber

The Non-Subject Subscriber is responsible for applying for the Certificate from the Certification Authority and is responsible for its management, in accordance with the PDS and the policy and practice statement. They must take appropriate measures to prevent damage arising from the use of the asymmetric key system or the Certificate. If they manage the authentication process, they must ensure authentication with a substantial or high level of security as required by Implementing Regulation (EU) 2015/1502 and subsequent amendments and additions, and in accordance with the procedures agreed with Tinexta Infocert.
It is also required to prevent the use of the Certificate after its expiry, revocation or suspension and to indemnify Tinexta Infocert against any liability arising from the misuse of the Certificate.

3.3.4 Obligations of Tinexta Infocert

Tinexta Infocert's obligations are exclusively those set out in the Applicable Regulations, this Technical Annex, the policy and practice statement and the Agreement.
In particular, Tinexta Infocert undertakes to store all certificates issued, their activation *logs* and authentication records in a dedicated, non-modifiable digital archive for 20 (twenty) years, in accordance with the policy and practice statement.
In particular, Tinexta Infocert gives no warranty whatsoever in respect of:

- the proper functioning and security of the *hardware* and *software* used by the subject;
- any use of the private key and the Certificate other than that provided for by current Italian legislation and the policy and practice statement;
- the regular and uninterrupted operation of national and/or international electricity and telephone lines;
- the validity and relevance, including as evidence, of the signature in relation to parties and for acts and documents subject to legislation other than Italian law;
- the confidentiality of any signed message, deed or document (therefore, any breaches of confidentiality are, as a rule, detectable by the subject or the recipient through the appropriate verification procedure).

Tinexta Infocert guarantees solely the operation of the Service, in accordance with the service levels set out for the subject in the policy and practice statement.

3.3.5 Role and Organisation

In accordance with the policy and practice statement and applicable regulations, the non-Holder subscriber or the subject themselves may request the inclusion in the Certificate of specific information relating to the subject's role.
This information may include:

- professional qualifications and/or licences;
- powers of representation on behalf of natural persons or private or public law bodies;
- membership of such bodies;
- the exercise of public functions.

This entry must be made in accordance with the procedures set out in the relevant policy and practice statement.
To request the inclusion of the role, the consent of **the Interested Third Party** is required; this party may be the same as the subscriber, and may also request the revocation or suspension of the Certificate at any time.
If the Subscriber (who is not the Subject) wishes the Certificate to reflect the Subject's membership of their organisation, it is the Subscriber's responsibility, in their capacity as the Interested Third Party, to notify Tinexta Infocert of any changes relating to the Subject's membership of the organisation.
Applications for certificates indicating membership of the organisation are accepted only if they come from entities with a defined legal form that can be verified with the Companies Register.
The organisation's registered name, trade name and identification code will be included in the Certificate only if the organisation has expressly authorised the issue of the Certificate, even without a specific indication of role.

4. SLA

4.1 Service Level Agreements (SLAs)

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