POLIMI GRADUATE SCHOOL OF MANAGEMENT

Advanced Electronic Signature Operating Manual

DOCUMENT CODE MO-FEA-OTP

VERSION 1.0

DATE dd/mm/yyyy

CONTENTS

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document contains all the technical and organisational information required for full compliance with the advanced electronic signature technical rules.

This document is intended for use with the "AES OTP Registration Form" (hereinafter also referred to as AES Registration Form) and summarises the technical characteristics of the electronic signature service.

1.2 REGULATORY AND TECHNICAL REFERENCES

Regulatory references

[1] Regulation (EU) No 910/2014 (eIDAS) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] Italian Legislative Decree 82 of 7 March 2005 (Official Journal 112 of 16 May 2005) – Digital Administration Code as amended and supplemented

[3] Italian Prime Ministerial Decree of 22 February 2013 (Official Journal 117 of 21 May 2013) – Technical rules on the generation, affixing and verification of advanced, qualified and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3), 32(3b), 35(2), 36(2), and (71)

[4] Italian Prime Ministerial Decree of 13 November 2014 (Official Journal 8 of 12 January 2015) – Technical rules on the creation, transmission, copying, duplication, reproduction and time stamping of electronic documents and on the formation and storage of public administration electronic documents pursuant to Articles 20, 22, 23-bis, 23-ter, 40(1), 41, and 71(1), of the Digital Administration Code referred to in Legislative Decree 82 of 2005

[5] Italian Prime Ministerial Decree of 3 December 2013 (Official Journal 59 of 12 March 2014) – Technical rules on the system of storage pursuant to Articles 20(3) and (5-bis), 23-ter(4), 43(1) and (3), 44, 44-bis, and 71(1), of the Digital Administration Code referred to in Legislative Decree 82 of 2005.

[6] Italian Presidential Decree 445 of 28 December 2000 (Official Journal 42 of 20 February 2001) – Consolidation Act of laws and regulations on administrative documentation

1.3 DEFINITIONS

The following definitions are used in this document. For the terms defined by the Digital Administration Code and the Italian Prime Ministerial Decree, please refer to the definitions set out therein.

Term	Definition
Electronic signature certificate	An electronic certificate linking the validation data of an electronic signature to a natural person and confirming at least that person's name or pseudonym.
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.
Private key	A key in the pair of asymmetric keys that is used by the Signatory to affix the electronic signature to the electronic document.
Public key	A key in the pair of asymmetric keys that is intended to be made public to verify the electronic signature affixed to the electronic document by the Signatory.
Validation	The process of verifying and confirming the validity of a signature.
Storage	A process of long-term secure storage of computer documents or image copies of analogue documents, which ensures their integrity, security, non-modifiability, availability and preservation of legal value.
Validation data	Data used to validate an electronic signature.
Personal identification data	A set of data establishing the identity of a natural or legal person, or of a natural person representing a legal person.
Electronic signature creation data	The unique data used by the Signatory to create an electronic signature.
Electronic signature creation device	A configured piece of software or hardware used to create an electronic signature.

Term	Definition
Electronic document	Any content stored in electronic form, in particular text or a sound, visual or audiovisual recordings.
Provider	Entity providing an Advanced Electronic Signature service in accordance with Article 55 of Italian Prime Ministerial Decree of 22 February 2013.
Automatic signature	A particular electronic signature process carried out with the authorisation of the Signatory who retains exclusive control of their signature keys, in the absence of their strict and continuous supervision.
Qualified signature	A particular type of advanced electronic signature based on a qualified certificate and a system of encryption keys, one public and one private, that are connected to each other, in which the Signatory uses the private key and the recipient uses the public key to express and verify the origin and integrity of an electronic document or a set of electronic documents.
Electronic signature	Data in electronic form that are attached or linked by a logical association with other electronic data that the Signatory uses to sign.
Advanced Electronic Signature	An electronic signature that fulfils the requirements of Article 26 of the eIDAS Regulation.
Qualified Electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device and is based on a qualified electronic signature certificate.
Signatory	A natural person who creates an electronic signature.
Hash	The string of binary symbols (bits) of a predefined length generated by applying a suitable hash function to digital evidence (Article 1(1)(h) of Italian Prime Ministerial Decree of 22 February 2013).
Hash function	A mathematical function that uses digital evidence to generate a hash to ensure that it is impossible to use the hash to reconstruct the original digital evidence and generate an identical hash based on different digital evidence (Article 1(1)(g) of Italian Prime Ministerial Decree of 22 February 2013).
Electronic identification	The process using electronic personal identification data representing a single natural or legal person, or a single natural person representing a legal person.
Means of electronic identification	A piece of hardware and/or software containing personal identification data and used to authenticate an on-line service.
Registration form	A contractual document prepared by the Provider to obtain the Client's consent to the use of the electronic signature system, which shall be signed by the Client only once, at the beginning of the relationship or at a later time.
OTP	A One-Time Password is a password that is valid for one transaction only. The OTP is generated and provided to the Signatory immediately before they affix the electronic signature. It can be based on hardware devices or software processes.
Trust service provider	A natural or legal person providing one or more trust services, either as a qualified trust service provider or as an unqualified trust provider.
Qualified trust service provider	A trust service provider providing one or more qualified trust services and to which the supervisory body assigns the status of qualified trust service provider.
Trust service	An electronic service normally provided against payment and consisting of the following elements: creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, registered electronic delivery services and certificates for such services; creation, verification and validation of web site authentication certificates; or storage of electronic signatures, seals or certificates relating to such services.
Qualified trust service	A trust service that fulfils the requirements set out in the Regulation.
Signature tool	A process for the creation of an advanced electronic signature that guarantees the Signatory's identity, uniqueness between the signature and the document, and the origin and integrity of the document itself.
Electronic time stamp	Data in electronic format that link other data in electronic form to a given date and time so as to prove that the latter existed at that time.
Qualified electronic time stamp	An electronic time stamp that fulfils the requirements of Article 42 of the eIDAS Regulation.

2 PARTIES INVOLVED

2.1 PROVIDER

The Provider is the entity that provides Advanced Electronic Signature solutions for use in relations with third parties for institutional, corporate or commercial reasons, implementing them on its own behalf or availing itself of solutions implemented by entities whose corporate purpose includes the implementation of advanced electronic signature solutions for Providers.

The Provider's full details are as follows:

Company name	**MIP Politecnico di Milano Graduate School of Business S.c.p.a**
Registered office	**Via** Lambruschini 4c
Phone number	0223992820
Corporate register number	**08591680155**
VAT number	**08591680155**
Website	https://www.gsom.polimi.it

2.2 IMPLEMENTER

The Implementer is the entity whose corporate purpose includes the implementation of advanced electronic signature solutions for Providers.

The Issuer's full details are as follows:

Company name	**InfoCert S.p.A.** **Company managed and coordinated by Tinexta S.p.A.**
Registered office	**Piazza Sallustio 9, 00187 Rome (RM)**
Operating headquarters	**Via Marco e Marcelliano 45, 00147 Rome (RM)**
Phone number	**06 836691**
Corporate register number	**Tax number 07945211006**
VAT number	**07945211006**
Website	**www.infocert.it**

InfoCert is the Trust Service Provider that issues the signature certificates and other signature tools in accordance with the technical rules issued by the Supervisory Authority and in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (also referred to as the eIDAS Regulation), and with Legislative Decree 82 of 7 March 2005 (Official Journal 112 of 16 May 2005) – Digital Administration Code as amended and supplemented.

2.3 USER / SIGNATORY

The User/Signatory is the natural person who uses the Advanced Electronic Signature tool to complete, modify or terminate contractual relations with the Provider, and/or to perform related operations and/or communications.

3 GENERAL RULES

3.1 PROVIDER'S OBLIGATIONS

In relation to the Advanced Electronic Signature process, the Provider shall ensure that:

- The technical rules set out in the Prime Ministerial Decree **[3]** are respected.
- The Signatory has been identified beforehand using a valid identity document.
- The Signatory has been informed beforehand of the exact terms and conditions relating to the use of the AES service, including the limitation of use.
- The Signatory signs an acceptance declaration of the terms and conditions of service to activate the AES service.
- A copy of the identity document and the declaration referred to in the previous point are stored for at least 20 years, ensuring their availability, integrity, legibility and authenticity.
- The Signatory may obtain, upon request and free of charge, a copy of the declaration and all information on the solution from the Provider.
- All information defined by the Italian Prime Ministerial Decree **[3]** is present on its website, including this document.
- A service for withdrawing consent to use the Advanced Electronic Signature solution is made available to the Signatory, where possible.
- The Signatory is provided a support service.
- The Advanced Electronic Signature may be affixed by the Signatory only.
- The Signatory has full knowledge of the document they are signing, and their signature cannot be affixed to any document other than the one being displayed.
- It is not possible to reuse the signature affixed by the Signatory on a different electronic document.

3.2 IMPLEMENTER'S OBLIGATIONS

The Implementer shall ensure that:

- The technological solution developed allows the signature to be linked unambiguously to the Signatory.
- The electronic document cannot be modified once the Signature has been affixed.

3.3 SIGNATORY'S OBLIGATIONS

The Signatory shall:

- Ensure the truthfulness, accuracy and completeness of the personal data provided to the Provider
- Deliver to the Provider an identity document that is valid at the time of registration
- Read the AES service descriptive documentation before registering for the service

3.4 INSURANCE

Pursuant to Article 57(2), the Provider has taken out appropriate third-party liability insurance cover to protect advanced electronic signature holders and third parties against any damage caused by inadequate technical solutions. The coverage limits are those provided for in the Italian Prime Ministerial Decree **[3],** i.e. not less than €500,000.

4 IDENTIFICATION AND REGISTRATION PROCESS

4.1 SIGNATORY IDENTIFICATION

Pursuant to Article 57(1)(a) of the Italian Prime Ministerial Decree **[3]**, Providers supplying the AES solution shall unambiguously identify the Signatory by means of a valid identity document.
The unambiguous identification of the document Signatory is done in person or remotely by the Provider, which may use its own network of agents/employees or other personnel for this purpose.

The Signatory's identity is verified by means of a valid and non-expired identity document, as required by the provisions of Article 35 of Italian Presidential Decree 445 of 28 December 2000; a copy of the identity document is kept.

4.2 LIMITATIONS OF USE AND SCOPE OF THE SOLUTION

Pursuant to Article 60 of the Italian Prime Ministerial Decree **[3]**, and as detailed in the Registration Form, the Advanced Electronic Signature may be used exclusively in relations between the Signatory and the Provider.

4.3 SIGNING OF THE REGISTRATION FORM

The Registration Form, including both the declaration of registration for the Advanced Electronic Signature services and consent to personal data processing, shall be signed by the Signatory using a "simple" electronic signature.

4.4 SIGNING OF DOCUMENTS

Once registration is complete, the User will be able to sign all documents proposed by the Provider using an AES with OTP.

The signing process can only be activated by the Signatory using One-Time Password authentication.

The OTP is generated and provided to the Signatory immediately before they affix the electronic signature.

Once the Signatory's identity has been established, the Provider makes the signed documents available to the Signatory.

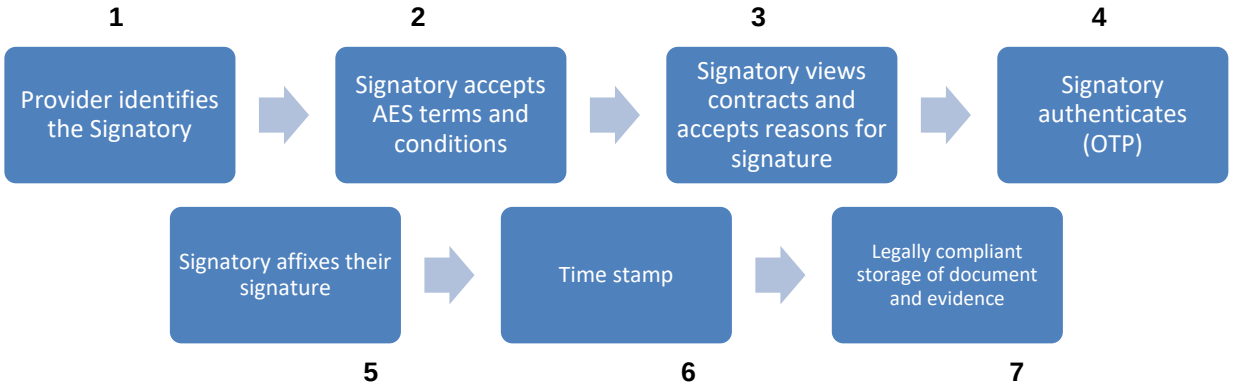
5 TECHNOLOGICAL SOLUTION USED

5.1 AES WITH OTP

5.1.1 PROCESS

The Advanced Electronic Signature with OTP solution involves the following steps:

1. The Signatory identifies the Signatory.
2. The Signatory agrees to the terms and conditions of the Advanced Electronic Signature service.
3. The Signatory views the contracts to be signed and accepts the reasons for signature.
4. The Signatory authenticates to the Advanced Electronic Signature (OTP) process.
5. The signature with the private key of the unqualified OneShot certificate issued to the Signatory is entered in the contract signature fields.
6. When identification is complete, the signing process is complete and the resulting document is time stamped.
7. The Provider sends the resulting document to a legally compliant storage service along with the evidence collected during the registration process.



5.1.2 SOLUTION CHARACTERISTICS

Article 56 of the Italian Prime Ministerial Decree of 22 February 2013, entitled “Characteristics of advanced electronic signature solutions”, breaks down and clarifies the requirements contained in the definition in Article 26 of Regulation (EU) 910/2014 (eIDAS), and defines the characteristics of AES solutions.

Below are the characteristics of the technology used and the manner in which it enables compliance with the requirements laid down in those regulatory references:

Requirements (pursuant to Article 56 of Italian Prime Ministerial Decree of 22 February 2013)	
Is linked solely to the Signatory	The signing process can only be activated by the Signatory by entering the One-Time Password received on their mobile phone number. The mobile phone number is certified by the Provider and is linked only to the Signatory during the identification phase.
Is suitable for identifying the Signatory	The unqualified signature certificate contains the Signatory’s personal identification data collected by the Provider when verifying the Signatory’s identity.
Is created using data for the creation of an electronic signature that the Signatory can, with a high level of security, use under their sole control	In the proposed solution, the following data are used to create the signature: 1) OTP sent via SMS for Signatory authentication, and 2) private key of the unqualified electronic certificate that can only be invoked upon successful authentication of the Signatory.
Is linked to the data provided at the time of registration in such a way that any subsequent changes to these data can be identified.	The use of cryptographic signature mechanisms ensures the integrity of the data provided at the time of registration.
Allows the Signatory to obtain evidence of what they have signed	The Provider makes the signed contracts available to the Signatory.
Identifies the entity referred to in Article 55(2)(a) of Italian Prime Ministerial Decree of 22 February 2013 (Provider)	References to the Provider are indicated in this Operating Manual and in the Registration Form made available to the Signatory.
Ensures absence of any element in the document to be signed capable of modifying the acts, facts or data represented therein	The documents to be signed are produced in such a way as to ensure compliance with the requirements laid down in the Digital Administration Code and the Italian Prime Ministerial Decree of 13 November 2014 on the “creation, transmission, copying, duplication, reproduction and time stamping of electronic documents” (no macros or functions).
Is linked unambiguously to the signed document	The Client's authentication transaction with OTP and affixing of the Signatory's electronic signatures are unambiguous moments.

6 CONTACTS

6.1 INFORMATION ABOUT THE AES SERVICE

Any communication, request for support and complaint (including requests pursuant to Article 57 of the Italian Prime Ministerial Decree [3]) may be sent to the Provider using the contact details provided in the Service Registration Form.

This document is published on the Provider's website at the address indicated in the Service Registration Form.

6.2 HOW TO REQUEST DOCUMENTS

The Signatory may, at any time, obtain a copy of all the documentation relating to the Advanced Electronic Signature service or signed with it.

In particular, the Signatory may obtain a copy or duplicate of:

- the Registration Form signed at the time of registration for the service
- the Personal Data Processing Consent Form signed at the time of registration for the service
- the identity document attached to the Registration Form
- the documents signed using the AES

The documentation shall be requested directly from the Provider using the contact details provided in the Service Registration Form.