OPERATIONAL MANUAL
OF THE AES SOLUTION
– Advanced Electronic Signature –

Summary

1. DEFINITION AND VALUE OF THE ADVANCED ELECTRONIC SIGNATURE

The electronic signature or subscription of a digital document serves to ensure the certain identification of the source, i.e., the authorship of the document, as well as to guarantee its immutability and integrity.

In the case of the advanced electronic signature, commonly referred to in abbreviated form as “AES”, the subscription occurs through a strict IT procedure aimed at ensuring that the electronic document to which it is associated meets the requirement of written form and has full legal validity as per art. 2702 of the Civil Code, pursuant to art. 20 paragraph 1-bis of the CAD.

The AES solution must comply with the provisions of Legislative Decree 82/2005 and subsequent amendments (Digital Administration Code, hereinafter “CAD”), the technical rules on AES provided by the Prime Ministerial Decree of 22.02.2013 and subsequent amendments (hereinafter “DPCM”), and the AgID Guidelines on the formation, management, and preservation of electronic documents.

2. PURPOSE OF THE OPERATIONAL MANUAL

The AES operational manual aims to provide users/signatories with a descriptive illustration of the specific features of the advanced electronic signature solution adopted by the Provider COMACCHIO S.p.A.

3. FEATURES OF THE AES SOLUTION

The REMOTE AES solution adopted by the Provider, in compliance with art. 56 paragraph 1 of the DPCM, guarantees:

A. the identification of the Signatory of the document (requirement of the Provider);

B. the unique connection of the signature to the Signatory;

C. the exclusive control by the Signatory over the signature generation system;

D. the ability to verify that the signed electronic document has not been altered after the signature was affixed;

E. the possibility for the Signatory to obtain evidence of what was signed;

F. the identification of the Provider of the REMOTE AES solution;

G. the absence in the subject of the subscription of any element capable of altering the acts, facts, or data represented therein;

H. the unique connection of the signature to the signed document.

The REMOTE AES solution also exclusively uses encrypted transmission channels and security measures compliant with Regulation (EU) 679/2016 and subsequent amendments ("GDPR").

3.1 Adhesion to and revocation of the use of the AES solution

To use the AES solution, the Signatory must mandatorily be identified and must first provide their consent by signing the specific adhesion form provided by the Service Provider (declaration of acceptance), pursuant to Article 57, paragraph 1, letter a) of the DPCM, by signing through the portal using the electronic signature solution based on OTP. By doing so, the Signatory expresses their intention to adhere to the AES solution and to accept the method of processing of personal data.

Adhesion to the AES solution is optional and may be revoked by the Signatory at any time. Should the Signatory choose not to adhere to the AES solution or subsequently revoke their adhesion, the document signing process will in any case be carried out using the traditional paper-based method or another method agreed upon.

The Signatory may revoke the AES service freely at any time by selecting the revocation button on the signing portal and signing the revocation using an electronic signature solution based on OTP.

3.2 Identification of the Signatory of the document

The Service Provider has the operational responsibility to reliably identify the Signatory by requesting a valid identification document, of which a copy is obtained during the AES service enrollment process. The copy of the identification document and the adhesion form to the service, signed by the Signatory, are digitally stored for at least 20 years.

3.3 Unique connection of the signature to the Signatory

The uniqueness of the connection between the signature and the Signatory, a mandatory requirement for the signing of the electronic document, is ensured by the unambiguous software correlation of the Signatory to the signing process, as well as by the use of a “One Time Password” (OTP) received from the solution and entered by the Signatory specifically to create a unique and indissoluble link between the signature transaction, the document, and the Signatory.

At the end of the AES signing process, in order to further strengthen its evidentiary effectiveness, the AES solution automatically generates a Signature Dossier document, digitally signed by the Service Provider, which is intended to record all the steps taken, the events, and the data of the signing transaction (the Signatory's personal details, etc.), uniquely associating the signature with both the Signatory and the document.

3.4 Exclusive control of the Signatory over the AES generation system

The Signatory, after being identified and having adhered to the REMOTE AES solution, can sign electronic documents while maintaining exclusive control over the AES solution used, through the following procedure:

1. The Signatory may receive a notification of documents to be signed through various channels: mobile app, email, SMS, or certified email (PEC). By accessing the web platform, the Signatory will find the document to be signed, being able to independently verify the content of the document, their personal data, and every detail concerning the terms and/or clauses to be signed, before initiating the REMOTE AES process.
2. The activation of REMOTE AES on the document takes place through the following steps:

   ➢ The Signatory confirms the content of the document by clicking the "For acknowledgement" button;

   ➢ The Signatory chooses to sign by selecting the "sign" option in relation to the document; the system generates a One Time Password (OTP) with a limited validity period and uniquely associated with the signature transaction;

   ➢ The Signatory receives the OTP through various possible methods (e.g., SMS, mobile app, email, etc.) and must input the received OTP into the online platform;

   ➢ By associating the OTP with the signature transaction, the Signatory expresses their intent to sign the document and retains exclusive control over the document and the signature.
3. The document is then digitally signed using a qualified digital certificate issued to the Service Provider.
4. The Signature Dossier, generated at the end of the signature transaction and digitally signed with a qualified electronic signature by the Service Provider, is intended to record all the steps taken, as well as the events and data of the signature transaction (such as the Signatory's personal details), uniquely associating the signature with both the Signatory and the document.
5. The signed document and the Signature Dossier are then sent to the legally compliant digital preservation service.

3.5 Possibility to verify that the signed electronic document has not been altered after the signature was affixed

At the end of the signing process using AES, the electronic document is digitally signed with the qualified certificate of the Service Provider, issued by a Qualified Trust Service Provider or an Accredited Certifier registered with the Agency for Digital Italy (AgID).

The Signature Dossier, generated at the end of the signature transaction and digitally signed with a qualified electronic signature by the Service Provider, is also intended to record all steps taken, along with the events and data of the signature transaction, including the hash (digital fingerprint) of the signed document.

The above ensures the integrity and immutability over time of the electronic document signed by the Signatory.

3.6 Possibility for the Signatory to obtain evidence of what was signed

The document signed using the REMOTE AES solution and the Signature Dossier are made available to the Signatory, who can therefore access evidence of what has been signed.

3.7 Identification of the AES solution Provider

The AES subscription form explicitly indicates, with the relevant identification data, the entity providing the AES solution pursuant to Article 55, paragraph 2, letter a), of the DPCM.

3.8 Absence in the subject of the subscription of any element capable of altering the acts, facts, and data represented therein

The documents produced within the AES solution exclusively use formats designed to ensure the absence of any element capable of altering the acts, facts, and data represented therein, in accordance with Annex 2 of the AgID Guidelines on the creation, management, and preservation of electronic documents.

The documents produced are exclusively in ISO-standard PDF/A format (containing no scripts, macros, fillable fields, or other elements that could alter their content after generation).

3.9 Unique connection of the signature to the signed document

The data from the AES signature transaction, integrated with additional information, are included in the Signature Dossier document, which indissolubly links them to the digital fingerprint (hash) of the signed document.

4. INFORMATION TO DATA SUBJECTS PURSUANT TO ART. 13 GDPR

COMACCHIO S.p.A., in its capacity as data Owner (hereinafter the “Owner”), issues this information notice to the data subject (the “Signatory”), in relation to the processing of their personal data for purposes connected to the provision of the Advanced Electronic Signature

Service, following subscription to the Service, in compliance with European and Italian regulations on personal data protection.

Purpose and legal basis of the processing

The activation of the Advanced Electronic Signature Service involves the processing of the Signatory's personal identification data (for example, first and last name, mobile phone number, email address, etc.), in accordance with the provisions of the Prime Minister's Decree of 22/02/2013 "Technical rules on the generation, affixing and verification of advanced, qualified and digital electronic signatures." In particular, the processing is carried out for the identification, activation, management of the Service, and compliance with the requirements of the Decree (DPCM) of 22/02/2013.

The legal basis for processing for the aforementioned purposes is compliance with a legal obligation to which the Owner is subject as the Provider of the Advanced Electronic Signature service, as well as the legitimate interest of the Owner to establish, exercise or defend a right.

Data retention period

Personal data will be retained for the time necessary to manage the Advanced Electronic Signature Service, as well as to fulfill specific obligations imposed by current regulations (at least 20 years, in accordance with Article 57 of the Prime Minister's Decree (DPCM) of 22/02/2013). Further retention is reserved for the time necessary to settle (by any means) any disputes that may arise.

Nature of data provision and consequences of refusal

The provision of data is necessary; therefore, any refusal to provide such data, in whole or in part, may result in the impossibility for the Owner to pursue the above-mentioned purposes.

Categories of recipients

The Owner will not disclose the data but intends to communicate them to internal personnel authorized to process them according to their respective duties, as well as to professionals or service companies used for the provision of the Advanced Electronic Signature service and to public and private entities, also following inspections and audits.

These recipients, if they process data on behalf of the Owner, will be appointed as data processors by means of a specific contract or other legal act.

Transfer of data to a third country and/or an international organization

The data of the data subject will not be transferred to third countries or international organizations.

Data subject's rights

The data subject has the right to request from the Owner access to their personal data and to have them rectified if inaccurate, erased, or to have their processing restricted if the conditions are met, to object to their processing based on legitimate interests pursued by the Owner, and to obtain the portability of the data personally provided only if subject to

automated processing based on consent or contract. To exercise their rights, the data subject may use the form available at the link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924 and send it to the following address: privacy@comacchio.com.

The data subject also has the right to lodge a complaint with the competent supervisory authority for data protection matters: Italian Data Protection Authority (www.garanteprivacy.it).

5. INSURANCE COVERAGE

The Provider declares to have taken out suitable insurance coverage in accordance with Article 57 of the DPCM of 22 February 2013, to cover any damages caused to third parties due to malfunctions of the AES system or due to non-compliance with applicable regulations.

The details of the insurance policy are available upon request.