



AdES Operational Manual

Version	1
Document Date	10/08/2025

1. Introduction	2
1.1 Glossary	2
1.2 Normative	3
1.3 Process stakeholders	4
2. eSignAnyWhere	5
2.1 Creation and management of signature practices	6
2.2 Signature Experience	8
2.3 Compliant storage	9
2.4 Sharing signed documentation	9
3. Termination of service	9
3.1 Revocation of consent by the Signatory	10
3.2 Dismissal of AdES service	10

1. Introduction

This document aims to describe the characteristics, operational methods, procedures, and technologies adopted by Firstance Group for the provision of the Advanced Electronic Signature (AdES) service, in accordance with the technical and regulatory requirements applicable to those who intend to use this solution for the execution of documents.

The electronic signature service is enabled through the partner Namirial S.p.A., with whom Firstance Group has entered into an agreement for the provision of the service.

The “**Advanced Electronic Signature**” (AdES) was introduced into the Italian legal system by Legislative Decree No. 235 of 30 December 2010, amending the Digital Administration Code (CAD), and is currently defined by Article 3, paragraph 1, point 11 of the eIDAS Regulation as an electronic signature which meets the requirements set out in Article 26, namely:

- a) it is uniquely linked to the signatory;
- b) it is capable of identifying the signatory;
- c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control;
- d) it is linked to the signed data in a way that allows the identification of any subsequent modification of such data.

From an evidentiary standpoint, Legislative Decree No. 235/2010, as subsequently amended by Legislative Decree No. 179 of 26 August 2016, further established, by integrating Article 20 of the Digital Administration Code (CAD), that: “The electronic document satisfies the requirement of written form and has the legal effect provided for under Article 2702 of the Civil Code when it bears a digital signature, another type of qualified electronic signature, or an advanced electronic signature, or, in any case, when it is created, following the electronic identification of its author, through a process that meets the requirements established by AgID pursuant to Article 71, using methods that ensure the security, integrity, and immutability of the document and, in a clear and unequivocal manner, its attribution to the author. In all other cases, the suitability of an electronic document to meet the requirement of written form and its evidentiary value shall be freely assessed in court, taking into account its characteristics of security, integrity, and immutability. The date and time of creation of the electronic document are enforceable against third parties if affixed in accordance with the applicable Guidelines.” In order to effectively implement an AdES in practice, it is necessary to comply with the technical rules set out in the Prime Ministerial Decree (DPCM) of 22 February 2013, published in the Official Gazette No. 117 of 21 May 2013, as well as with the Guidelines issued by AgID pursuant to Article 71 of the Digital Administration Code (CAD).

1.1 Glossary

Termine	Descrizione
Namirial	Electronic Signature Service Provider and Certification Authority
CA	Certification Authority
Certifier	The public or private entity authorized to issue digital certificates following a specific certification procedure in compliance with national and European standards
Recipient	The individual who receives the invitation to access an eSaw envelope
eSaw	<i>eSignAnyWhere</i> is the platform used for managing document workflows that end with a simple, advanced, or qualified electronic signature

AdES	Advanced Electronic Signature. A set of data in electronic form attached to or logically associated with an electronic document, which allows the identification of the Signatory and ensures a unique link to the Signatory, created using means that the Signatory can maintain under his or her sole control, and linked to the data to which the signature refers to the data in a way that enables detection of any subsequent modification
Automatic Signature	A type of remote signature designed for unattended use
Signatory	The individual for whom the advanced electronic signature solution is made available in order to sign electronic documents
Registration form	The contractual document that collects the Signatory's consents regarding the use of the advanced electronic signature system, executed by the Signatory once, either at the beginning of the relationship or at a later stage
Namirial Archive	The Namirial Long Term Archiving platform (compliant digital preservation)
Operator	The person who initiates the digital signature process, who may be either a Firstance collaborator or a member of the co-distributors' network with whom Firstance has entered into a co-intermediation agreement
Signature Provider	The entity providing electronic signature services, ensuring document integrity and compliance with applicable regulations on security and legal validity. The electronic signature provider supplies the tools and technological infrastructure required to create, manage, and verify electronic, qualified, or digital signatures

1.2 Normative

Riferimento	Descrizione
EU Regulation No. 910/2014	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
Presidential Decree No. 445/2000	Decree of the President of the Republic of 28 December 2000, No. 445 (Official Gazette No. 42 of 20 February 2001) – Consolidated text of legislative and regulatory provisions on administrative documentation
Regulation (EU) No. 679/2016	Regulation (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
Legislative Decree No. 82/2005	Legislative Decree of 7 March 2005, No. 82 "Digital Administration Code"
Prime Ministerial Decree of 22 February 2013	Decree of the President of the Council of Ministers of 22 February 2013 (Official Gazette No. 117 of 21 May 2013) – Technical rules concerning the generation, affixing, and verification of advanced, qualified, and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3), 32(3)(b), 35(2), 36(2), and 71
AgID Determination No. 121/2019	AgID Determination No. 121/2019 containing the "Guidelines setting forth the Technical Rules and Recommendations concerning the generation of qualified electronic certificates, qualified electronic signatures and seals, and qualified electronic time validations"
Legislative Decree No. 231/2007	Legislative Decree No. 231 of 21 November 2007 (Official Gazette No. 290 of 14 December 2007) and subsequent amendments and integrations – "Implementation of Directive 2005/60/EC on the prevention of the use of

	the financial system for the purpose of money laundering and terrorist financing, as well as of Directive 2006/70/EC laying down implementing measures thereof"
Bank of Italy Measure of 30 July 2019	Measure containing "Provisions on customer due diligence for the prevention of money laundering and terrorist financing," pursuant to Article 7(2) of Legislative Decree No. 231 of 21 November 2007
CNIPA Resolution No. 11 of 19 February 2004	Technical rules for the reproduction and preservation of documents on optical media suitable to ensure the conformity of documents to the originals, pursuant to Article 6(1) and (2) of the consolidated text of legislative and regulatory provisions on administrative documentation, as set out in Presidential Decree of 28 December 2000, No. 445
AgID Determination No. 407/2020	AgID Determination No. 407/2020 containing the "Guidelines on the creation, management, and preservation of electronic documents," as amended by AgID Determination No. 371/2021

1.3 Process stakeholders

Issuer

Firstance Group (hereinafter "FIRST" or the "Issuer") assumes, with respect to each of its Signatories, the role of Issuer of the AdES solution as defined in Article 55, paragraph 2, letter a) of the Prime Ministerial Decree. Pursuant to Article 57, paragraph 1, letter a) of the same Decree, the issuers of the AdES solution must reliably identify the user by means of a valid identification document in order to configure an AdES.

The reliable identification of the Signatory of the document is carried out by FIRST through its own Operators or through its co-distributors, in compliance with the validated and agreed identification procedures. In the cases provided for by law, the identification procedure for AdES purposes coincides with the identification procedure required under anti-money laundering regulations, performed pursuant to Legislative Decree No. 231/2007, on the basis of documents, data, or information obtained from a reliable and independent source.

FIRST undertakes, in compliance with the provisions of the Prime Ministerial Decree, to carry out the following activities:

- To reliably identify (either directly by FIRST or through its co-distributors) the user by means of a valid identification document;
- To inform the user of the exact terms and conditions of use of the service, including any possible limitations thereof;
- To make the activation of the service conditional upon the acceptance of the Registration Form, which includes the user's declaration of acceptance of the service terms and conditions;
- To retain, for at least 20 years, a copy of the identification document, the Registration Form, and the privacy notice;
- To ensure the availability, integrity, legibility, and authenticity of the document confirming acceptance of the service;
- To disclose the features of the system implemented to ensure compliance with the provisions set forth in the Technical Rules, Article 56, paragraph 1;
- To specify the characteristics of the technologies employed and how they ensure compliance with the prescribed requirements;
- To provide the possibility for the Signatory/user to revoke the service.

Signature Provider

Namirial S.p.A. is the Signature Provider of the AdES solution, as defined under Article 55, paragraph 2, letter b) of the DPCM, providing OTP services through its proprietary platform. Namirial is an IT company specializing in software and digital services. It acts as a Qualified Trust Service Provider and Certification Authority, offering trust services such as Electronic Signatures, Advanced Electronic Signatures (AdES), Qualified Electronic Signatures, Certified Electronic Mail (PEC), Electronic Invoicing, and Long-Term Archiving compliant with applicable regulations.

For further information, please refer to the website: <https://www.namirial.it/>

Applicant

The Applicant is the Signatory who executes the contractual documentation by means of electronic signatures. The Applicant is required to ensure:

- the accuracy and completeness of the personal data provided to the Issuer, including the correct telephone number to be used for the OTP signature;
- the delivery or upload to the Operator of a valid identity document;
- that they have reviewed the descriptive documentation of the AdES service prior to subscribing to the service.

2. eSignAnyWhere

eSignAnyWhere (eSaw) is Namirial's platform designed for the digitalization of business transactions that include electronic signatures and serves as the solution underlying the signature service provided by FIRST.

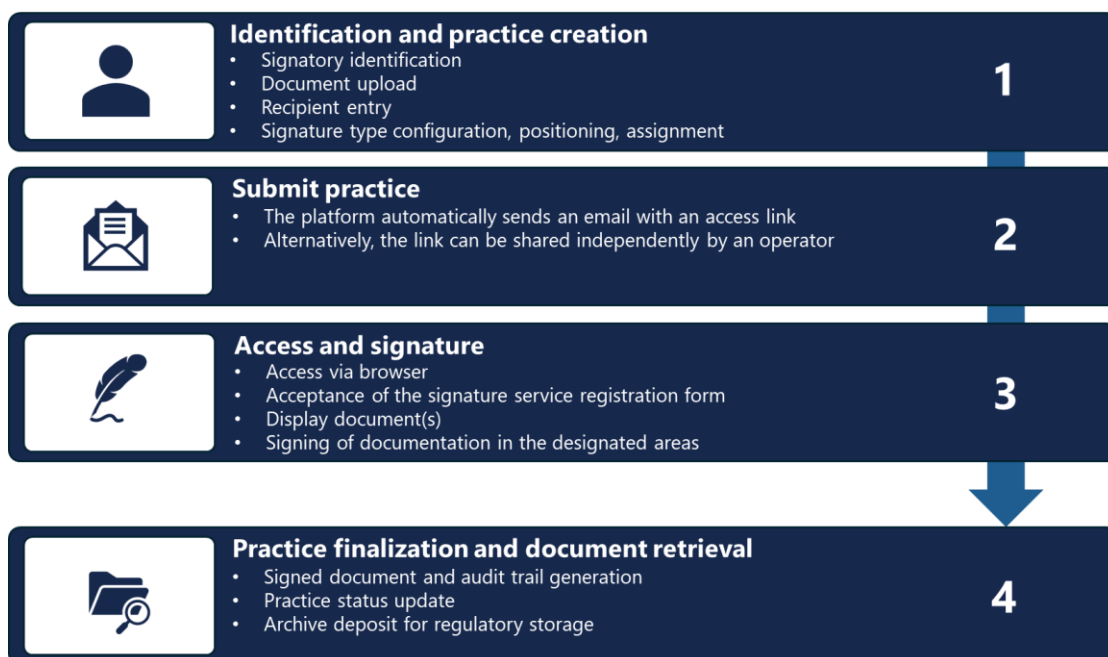
The platform allows the management of document workflows, with particular reference to the signing phase, successfully consolidating numerous use cases within a single solution and supporting any type of electronic signature. eSaw provides simple integration tools and offers a high degree of customization through the use of tailored graphical interfaces, customizable communications, and pre-configured templates.

With eSaw, it is possible to manage complex signing transactions, accessed via multiple channels (e-mail, web, mobile...) and by multiple users. The platform can be employed in any application context that requires the execution of signing processes, including those offered by FIRST through its own application solutions. Indeed, the eSaw platform can be used for the implementation of AdES in compliance with Article 57 of the Prime Ministerial Decree of 22 February 2013 through the use of OTP SMS or graphometry.

Specifically, regarding the signing process, the eSaw platform interacts with FIRST's applications, ensuring a complete and intuitive user experience. Communications to the recipients, such as the e-mail invitation to sign, are independently managed by the Issuer, retrieving the access link to the case from eSaw and providing it to the Applicant through its own tools – e-mail, FA Lounge web app/app, etc. Notwithstanding the integration with FIRST's various applications, the eSaw platform remains the solution responsible for the signing process, ensuring that, upon completion, digitally signed PDF documents are produced with either a PAdES (PDF signature) or CAdES (p7m) encrypted envelope. In addition, for each signing case, eSaw automatically generates a specific Audit Trail, i.e., the document that tracks and collects all logs, information, and data related to the completed case and the actors involved.

2.1 Creation and management of signature practices

The following summarizes the workflow of a signing case, from its creation to the retrieval of the signed documents. The case is managed directly through the Operator panel (e.g., FA Suite, Firstance internal IT systems), which communicates with the eSignAnyWhere electronic signature platform via application integration.



1. Identification is carried out by the FIRST Operator (or by the network of co-distributors with whom FIRST has entered into a co-brokerage agreement) and varies depending on the sales methods adopted. This activity is preparatory to the collection of the dataset necessary for the creation of the signing case.
Once this activity is completed, the Operator proceeds to select the documents to be included in the practice, insert the signature fields within the relevant documents, and configure them as required, if not already pre-configured through IT systems. Subsequently, the Operator specifies the recipient users of the practice, whose dataset will consist of the identifying data of the respective Applicants: first name, last name, e-mail address, and telephone number (for One Time Password – OTP – signature).
2. The confirmation of the creation of the practice triggers the sending of communications to the recipients via e-mail, with the documentation to be signed accessible through a specific link included in the message. Alternatively, if otherwise provided, the Operator may share the access link (from the Operator panel) and send it to the recipients via different communication channels (e-mail, FA Lounge web app/app, etc.). The status of the practice can always be monitored by the Operator through their interface.
3. The recipients will therefore have the possibility to access the practice through the access link to the electronic signing process, expressing their intention to proceed with the process. Before being able to sign the documents, the Applicant must:

- Enter the OTP code received via message on the verified telephone number for the respective authentication.
- Accept the Registration Form for the electronic signature service proposed within the process. Acceptance of the form certifies the Applicant's intention to access the signature service. In the event of refusal of the form, the process is interrupted and the Applicant cannot proceed with the digital signing of the documents.

Once the preparatory activities are completed, the Applicant accesses the document signing screen, where all signature fields must be signed to complete the process. On the signing screen, accessible via their own device, the Applicant can personally verify their data and all details regarding the conditions or clauses to be signed, and can independently select the individual signature fields on which they are required to manually express their intention to sign (a "point and click" process).

Through the procedure described above, the Applicant is therefore ensured exclusive availability of the device and full control over the signing process, always having the possibility, for each individual signature applied, to: view the contents of the documents at the moment of signing so as to have full awareness of what is being signed, zoom in/out on the document text, easily locate every part of the document where a signature is required, and confirm the signature applied or cancel the operation.

For more details on the electronic signing procedure, see paragraph 2.2 – Signing Experience.

4. The completion of the actions required from each Applicant triggers a change in the status of the practice, followed by the corresponding notification (visible from the Operator panel). Upon completion of the practice, the platform provides the Applicant(s) with the possibility to directly download the documentation with their digitally applied signatures. Optionally, the Operator may be requested to share the signed documentation via e-mail. Once the process is concluded, the signed documentation is automatically deposited in a dedicated archive of the Namirial Issuer for its long-term legal retention.

The retrievable documentation consists of:

A) Signed document(s)

TEST DOCUMENT

The undersigned:

- Name: Lorenzo
- Surname: Raimondi

DECLARES

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam eaque ipsa, quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt, explicabo. Nemo enim ipsam voluptatem, quia voluptas sit, aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos, qui ratione voluptatem sequi nesciunt, neque porro quisquam est, qui dolorem ipsum, quia dolor sit, amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt, ut labore et dolore magnam aliquam quaerat voluptatem.

DATE
13/10/2024

SIGNATURE

Firmato da: RAIMONDI LORENZO
Firma da: Namirial CA Firma Qualificata
Ora/Minuto/Secondo: 13-10-2024 09:02:57
Indirizzo IP: 161.89.33.64

AND ACCEPTS

Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit, qui in ea voluptate velit esse, quam nihil molestiae consequatur, vel illum, qui dolorem eum fugiat, quo voluptas nulla pariatur? [33] At vero eos et accusamus et iusto odio dignissimos ducimus, qui blanditiis praesentium voluptatum deleniti atque corrupti, quos dolores et quas molestias excepturi sint, obcaecati cupiditate non provident, similique sunt in culpa, qui officia deserunt mollitia animi, id est laborum et dolorum fuga.

DATE
13/10/2024

SIGNATURE

Firmato da: RAIMONDI LORENZO
Firma da: Namirial CA Firma Qualificata
Ora/Minuto/Secondo: 13-10-2024 09:02:57
Indirizzo IP: 161.89.33.64

The signed document is returned in PDF format and contains all the signatures applied by the various recipients within the designated areas, as well as any additional elements provided. Each signature is visible through the graphical appearance applied at the relevant point, including the Applicant's first and last name and any supporting data (signing time, IP address, etc.). The document is digitally signed with the Namirial seal, guaranteeing the origin and authenticity of the process. In the case of a qualified signature (remote, automatic, disposable, or via physical device), the name of the relevant Certification Authority is also reported, while retaining the possibility to verify the digital signature directly using the Adobe feature or through third-party verification tools available to the user. In the case of multiple documents included in the same practice, they will be returned within a zip folder.

B) Audit-trail (Certificate of completion of practice)

Audit Log per 'Contratto_demo'
generato su 2024-10-19 | 12:43:58 nella versione 24.40.1.172-8d99178491

Informazioni Generali

Envelope ID: 1ac7d73-c100-4d1e-a8b5-0d0d0e0f4c7
Nome Profilo: Contratto_demo
Mittente: Lorenzo Raimondi (l.raimondi@namirial.com)
Stato: Completato
Sequenza di Firma: SI
Divulgazione Elettronica Abilitata: No
Invia Pratiche Completate: SI

Informazioni sul Documento

Riferimento Documento: 01
Nome: Test_document_1.pdf
Numero di pagine: 1
Hash del PDF (calcolato prima della pre-elaborazione del flusso di lavoro (SHA256): E94B7137B1403E9A243D17B7D4D50B63D64F6D6E6A1738CD10C47279A2
Hash della Pratica Completata (SHA256): 87359FCAC1348F3E354E09B8430079C7D0D303D54E8EA3460B0C91DFD0A1

Destinatari

Sequenza	Nome	E-mail	Numero di telefono	Tipo	Autenticazione
1	Lorenzo Raimondi	l.raimondi@namirial.com		Neutro	Firmatario
2	Lorenzo Raimondi	l.raimondi@namirial.com		Neutro	Destinatario in
					Copia

The document, signed with the Issuer's seal, contains all the information and technical details related to the practice and its completion, divided into the following main sections:

- General information
- Document information
- Recipients
- Recipient details
- Notification messages
- Electronic consent
- Transaction status
- Detailed tracking of actions performed
- Acceptance of the Registration Form for the digital signature service

2.2 Signature Experience

Applicant Signature

Each signature field within the document must be selected by the Applicant using the "point & click" method (Namirial Click2Sign solution) in order to apply the signature. For each selected signature field, the platform requires the user to confirm their intention to sign the document. Following the confirmation, the system inserts the corresponding timestamp, which certifies the Applicant's first and last name, email, date and time of the signature, and IP address.

Automatic Signature

Additionally, if required by the documentation, FIRST's signature is applied through an Automatic Signature certificate recognized by Namirial.

The application of this type of signature does not require any further actions from the certificate holder, as it is automatically applied by the platform within the created signature workflow.

2.3 Compliant storage

FIRST has entered into an agreement with Namirial for the delegation of compliant long-term archiving of digitally signed documents, an activity managed through the specific solutions provided by the same Issuer. The archiving process involves storing all documents signed by the Applicants, together with the corresponding audit trails, within the Provider's IT systems, while ensuring that FIRST retains full access for consultation and retrieval of the documentation.

2.4 Sharing signed documentation

If the Applicant needs to obtain the signed documentation at a later stage after the signing, FIRST provides the following contact procedures based on the type of distribution adopted:

- In the case of co-distribution (Co-distributor – FIRST – Insurer), the Applicant requests the digitally signed documentation directly from the operator belonging to the co-distributor network with whom they interacted for the subscription of the documents. The co-distributor network may, according to the processes defined with FIRST, independently retrieve the documentation from the FIRST application or contact FIRST for the sharing of the documentation.
- In the case of direct intermediation with FIRST (FIRST – Insurer), the Applicant may request the digitally signed documentation from a FIRST operator at the following addresses:
 - o for FA Italy: italia@firstance.com ; estero@firstance.com
 - o for FA International (Luxembourg, Liechtenstein, Monaco, Spain, Finland): middleoffice.lu@firstance.com

3. Termination of service

The provision of the Advanced Electronic Signature service may be interrupted either due to the revocation of consent by the Applicant or due to the discontinuation of the service by FIRST. The effects of both termination scenarios are outlined below.

3.1 Revocation of consent by the Signatory

If the Applicant chooses to revoke their consent to the use of the Advanced Electronic Signature service, the documents governing the relationship between the Applicant and FIRST (including any other parties possibly involved) must be signed manually on paper. Documents previously signed with an Advanced Electronic Signature remain valid. The revocation of consent must be submitted via written communication with the subject line "REVOCATION OF ADES SERVICE REGISTRATION" to Firstance at the following address: firstance@legalmail.it

3.2 Dismissal of AdES service

Should FIRST decide to discontinue the AdES service, the documents governing the relationship between the Applicant and FIRST (including any other parties possibly involved) will be signed manually on paper or by other methods subsequently identified. Documents previously signed with an Advanced Electronic Signature will remain valid and will continue to be preserved in compliance for the entire retention period required. FIRST will also continue to retain the audit trail certifying the completion of the Advanced Electronic Signature until the expiry date established by DPCM regulations for the Issuer.