



ENTAKSI SOLUTIONS

SISTEMA DI GESTIONE CERTIFICATO

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001

ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035

SERVIZI FIDUCIARI QUALIFICATI

ETSI 319 401 | ETSI 319 411-1 e 2 | ETSI 319 421 | ETSI 119 511

FIRME E SIGILLI ELETTRONICI - MARCHE TEMPORALI

CONSERVAZIONE A LUNGO TERMINE

User Manual

UM eSIGN en 20230516 User manual

Entaksi Solutions SpA

Index

Document information.	1
Document approval	1
Revisions	1
1. Introduction.	3
1.1. eSIGN service features	3
2. Roles and responsibilities	5
2.1. Service Delivery Operational Support (SDOS)	6
2.2. Information System Operational Support (ISOS)	6
2.3. eSIGN Manager tasks	7
2.4. Service management responsibilities	7
3. Entaksi Console registration procedure	9
3.1. Single Sign-on access	11
3.2. Resend registration link and password recovery	11
3.3. How to access the Service	11
3.4. User settings management.	11
4. eSIGN Console	13
4.1. Dashboard.	13
4.2. Console tables	14
4.3. Console Menu	15
5. Configuration	16
5.1. Company master data	16
5.2. Access management	16
5.3. Notification	19
5.4. Classification scheme	19
5.5. Organizational areas	22
6. eSIGN signing processes.	24
6.1. Configurations	25
6.2. Signatures report	34
6.3. Signatory users	34
6.4. Signatory groups	43
6.5. Signing process.	46
6.6. Process template	58
6.7. Signing process workflow.	64
6.8. Signature pages	65
6.9. Markers	72
7. Entaksi Token	80
7.1. Management.	81
7.2. Sign local documents through Acrobat	82
8. eSIGN Desktop.	83
8.1. eSIGN Desktop Installation	84
8.2. File Menu	84
8.3. Help menu.	86
8.4. Launch eSIGN Desktop.	86
8.5. Connecting eSIGN Desktop to the eSIGN service.	88
8.6. Signing documents with eSIGN Desktop.	89
9. Entaksi app	91
9.1. Installing Entaksi app.	91

9.2. App access and signing documents.	93
10. Terminology	95
10.1. Glossary.	95
10.2. Acronyms	102
11. Regulations, reference standards and certifications	103
11.1. Company certifications	103
11.2. Regulations.	103
11.3. Standards	104
12. Periodic check of system accessibility.	106
13. Localization of stored data.	107
14. Backup copies management policy	108
15. Maintenance of the application software	109
16. Malfunctions management	110
16.1. Service reports.	110
16.2. Claims	110
16.3. Emergency changes	110
17. Data protection management	111
17.1. Data Breach	111
18. Service Level Agreement	112
19. Service reporting	113

Document information

Project	User Manuals
Type	User Manual
Document ID	UM eSIGN en 20230516 User manual
Version	1.11.0
Creation Date	16/05/2023
Last Revision	15/04/2025
Author	Erica Negri
Status	Released
Classification	Public



Paper reproductions of this document are to be considered working copies not registered by the Integrated Management System.

Document approval

Date	Employee	Mansion	Signature
15/04/2025	Paola Caioli	DeIM	Digital signed

Revisions

Date	Version	Name	Mansion	Action	Distribution
16/05/2023	0.0.1	Erica Negri	ICT Team	Draft creation.	Internal
16/05/2023	1.0.0	Erica Negri	ICT Team	Release.	Internal
20/07/2023	1.1.0	Erica Negri	ICT Team	New template and configuration functionalities.	Public
08/09/2023	1.2.0	Erica Negri	ICT Team	Described the new features of printing and duplication of the classification scheme, the definition of the author of the FEA processes via link, the association of metadata to additional data. Added the section dedicated to the Entaksi signature application	Public

Date	Version	Name	Mansion	Action	Distribution
21/09/2023	1.3.0	Erica Negri	ICT Team	The new feature of additional data "rules" has been added. The new template feature to add or modify signatory users registry during the signature phase different from the process signer's one has been introduced.	Public
03/11/2023	1.4.0	Erica Negri	ICT Team	The new functionalities for rejecting a signature process and the mandatory attachments in the signing phase are added.	Public
20/01/2024	1.5.0	Erica Negri	Quality Assurance Manager	The new functionalities of import and export of additional data via .csv file and the new detail page of the signing processes are added.	Public
08/04/2024	1.6.0	Erica Negri	Quality Assurance Manager	The new feature for defining fonts and sizes of the editable field and the new features of the application of the Classification Scheme has been added.	Public
10/06/2024	1.7.0	Erica Negri	Quality Assurance Manager	The Entaksi Token and the new methodologies for signing local documents via eSIGN Desktop are been added.	Public
11/09/2024	1.8.0	Erica Negri	Quality Assurance Manager	New management of AdES agreement acceptance; definition of signatories in the templates; new features of eSIGN Desktop.	Public
20/11/2024	1.9.0	Anna Mazzotta	ICT Team	New features of eSIGN Desktop, new management of signatory users in groups and templates with parameters.	Public
28/02/2025	1.10.0	Anna Mazzotta	ICT Team	The new functionality for sending notifications to multiple third-party users in the signature processes has been added	Public
15/04/2025	1.11.0	Anna Mazzotta	ICT Team	The new file renaming feature to templates and signing processes has been added.	Public

Copyright © 2025 Entaksi Solutions SpA

Information contained in this document is property of Entaksi Solutions SpA. It is provided privately and confidentially to the intended recipient(s) and it must not be used for production purposes, nor communicated to third parties or reproduced, partially or integrally, published or redistributed without the prior written consent of Entaksi.

1. Introduction

This user manual describes the **eSIGN** service which is provided by Entaksi Solutions SpA, hereinafter referred to as "Entaksi". The service **eSIGN** is used to manage the definition and the digital signature process of your documents.

eCON Digital Preservation Service is the system on which eSIGN is based. It is provided by Entaksi.

Entaksi is listed among the **Qualified Preservation Service Providers** according to the requirements defined by Agenzia per l'Italia Digitale (AgID) and the service is included in the catalogue of Cloud services established and managed by Agenzia per la Cybersicurezza Nazionale (ACN).

The Preservation System complies with the AgID directives on reliability, security and data protection. It has the following features:

- **Completeness** - presence of any uploaded document.
- **Robustness** - consistency guarantee of the data entered.
- **Scalability** - ability to manage an increasing number of users and documents.
- **Security** - protection from unauthorized access and manipulation of data.
- **Reliability** - independence from hardware failures.
- **Clarity** - easy consultation according to various search criteria.

Digital preservation is based on supports with characteristics of high reliability and high permanence of data, and its duration is established in the service contract.

Entaksi is registered, through its branch Entaksi Solutions SpA Irish Branch, as a **Trust Service Provider (QTSP)** under the European Regulation EU 910/2014 - eIDAS by the DCCAE - Department of Communications, Climate Action and Environment, Ireland.

Entaksi is a trust service provider for:

- **Issuing qualified certificates for electronic signatures and seals.**
- **Creating electronic time-stamps.**
- **Long-term preservation of electronic signatures and seals.**

Entaksi issues qualified certificates for the following uses:

- **Qualified certificates for electronic signatures.**
- **Qualified certificates for electronic seals.**
- **Qualified certificates for time-stamping units that issue qualified time-stamps.**

This qualified certificates are also used within the service eSIGN. For a detailed description of all the features of the qualified services offered by Entaksi, you can consult the [page "Documentation" within the corporate website](#).

This manual describes:

- how to access the service and how to use it;
- all the functions provided by the service;
- information security procedures.

This manual represents the main reference for the description and regulation of each aspect of the service, including the management of communication between Entaksi and the Customer.

eSIGN is available in SaaS (Software as a Service) mode, and it can be reached through the web interface hosted on the **Console** provided by the Entaksi. It is therefore not necessary to install any software to use the service, just use a browser compatible with modern standards.

Entaksi reserves the right to make changes and updates to the document necessary for the adaptation of the service to regulatory and organizational changes, reporting the extremes in the initial block "Revisions".

[Back to top.](#)

1.1. eSIGN service features

eSIGN is the Entaksi service that allows you to manage the electronic signature process: configuration of master data and templates, definition of the digital signature workflow, application of the signature process to your documents, preservation of your documents in compliance with law.

The service includes:

- the definition of the signatory users' personal data;
- configuration of standard templates to define signature processes;
- the definition of signature processes based on standard templates or configured on the specific document type;
- check, control and management of the entire signature workflow from its start to its end;
- the preservation in compliance with the law of the managed and signed documents.

The digital preservation phase is managed through **eCON** service by Entaksi, which uses technological infrastructures that meet the high reliability requirements required by law (in particular: the OAIS Reference Model ISO 14721, the Information Security Management Standard ISO/IEC 27001, the EU legislation about data protection, Italian laws on digital preservation such as DPCM 3 December 2013 concerning the technical rules on the preservation system).

Through eCON service you can upload digital documents into the preservation system, you can digitally sign them and you can ensure their preservation in compliant with law. Thanks to the service interface, it is possible to know the status of the documents, to access the consultation function, to search for the data of interest and to obtain DIP for the required documents.

The **eSIGN Service** is structured as follows:



Figure 1. eSIGN service.

All operational phases of eSIGN service are described in the following chapters.

[Back to top.](#)

2. Roles and responsibilities

In this chapter is defined the designated community of the preservation system, as characterized in the Standard ISO/IEC 14721:2012 OAIS (Open Archival Information System). This standard provides an open information system model for the management and long-term preservation of information content, and it is applicable to any type of archive. The chapter also defines roles and activities for each service manager.

The eCON Digital Preservation Service provided by Entaksi labels the roles defined below, in accordance with the document "List of professional profiles for digital preservation" published by AgID on the basis of Circular no. 65/2014 (G.U.n.89 of 16/04/2014). The role of Preservation Manager is also specified in the D.P.C.M. 3 December 2013, articles 6-7.

The legislation defines "**Producer**" people or client systems who provide the information to be preserved, responsible for creating the Submission Information Package (SIP) and its sending to the preservation system. The Producer receives a confirmation of the SIP reception or an error resulting from the SIP submission.

The legislation defines "**Preservation manager**" as the natural person who defines and implements policies necessary for document storage, and he is responsible for documents preservation. The Preservation Manager entrusts Entaksi with the digital preservation service in accordance with IT documents, as well as defined in the contract. In Public Administrations, the role of the Preservation Manager is played by an internal manager or a formally appointed internal official.

As specified by the AgID Guidelines, Chapter 4.5 - Preservation Manager, "Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore, al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione."

A "**Consumer**" or "**User**" is defined as people, or client systems, who interact with the Preservation System, within the limits indicated in the General Conditions of the Service and permitted by law, to find preserved information of interest and to access them in detail.

The Entaksi Digital Preservation Service is made up of various "**Managers**", each of whom covers a very specific role in the company and in particular in the service, in order to better guarantee the reliability of the system without overlapping activities and with compartmentalization of roles:

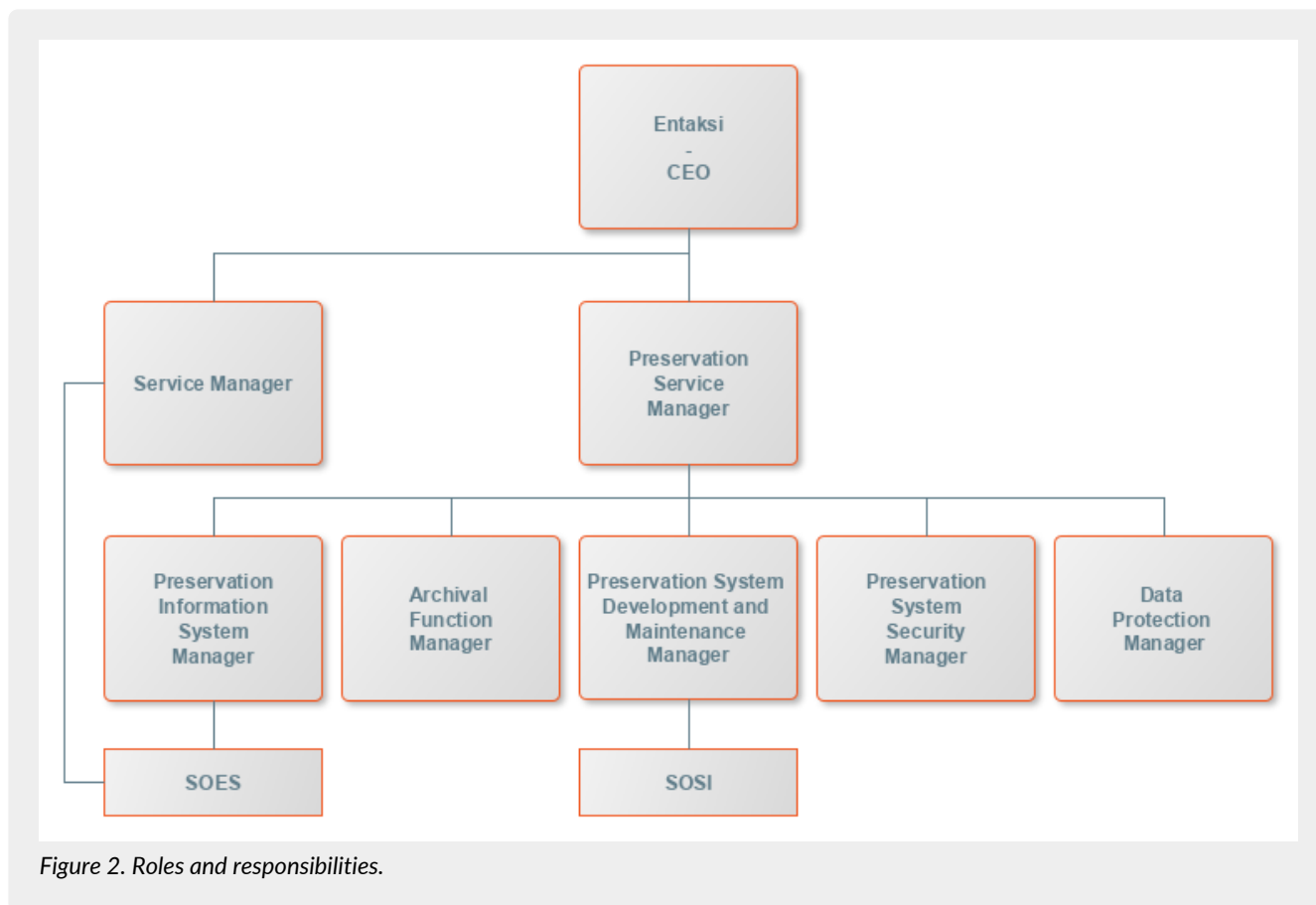
- **Preservation Service Manager.**
- **Archival Function Manager.**
- **Data Protection Manager.**
- **Preservation System Security Manager.**
- **Preservation Information System Manager.**
- **Preservation System Development and Maintenance Manager.**

eSIGN is based on the eCON Storage System, and therefore provides the same roles and responsibilities.

The service is managed by the Preservation Service Manager. His tasks are described in the paragraph [eSIGN Manager tasks](#).

Data relating to the identifiers and specific roles covered by the various managers of the Preservation Service eCON are available in the eCON preservation manual, published both on the [Agenzia per l'Italia Digitale website](#) and on the [Entaksi Website](#).

The roles are represented in the following diagram.



Entaksi Solution SpA is responsible for the provision of the service, and the Preservation Service Manager is the role appointed for the service delivery tasks. Preservation Service Manager can rely on the structures described in the following paragraphs to carry out his duties.

[Back to top.](#)

2.1. Service Delivery Operational Support (SDOS)

Service Delivery Operational Support (SDOS), **Service Delivery Operational Support**, is a Entaksi's department with the aim of **collecting information and problem reports from customers** (Producer and Users) and from the internal structures involved in the provision of the eSIGN Service.

The SOES is managed by the Preservation Service Manager and the Preservation Information System Manager, and it is responsible for the collection and handling of reports coming from users of the service. Reports are entered in Entaksi's ticketing system, and are categorized by type into one of the following classes:

- incident;
- service request.



Customers can send reports and requests to the eCON Service by e-mail at helpdesk@entaksi.eu.
SDOS is active from Monday to Friday from 09:00 to 18:00.

[Back to top.](#)

2.2. Information System Operational Support (ISOS)

Information System Operational Support (ISOS), **IT Development Operational Support** is managed by the Entaksi ICT Manager (also Preservation Information System Manager), and it aims to **ensure the correct functioning of Entaksi's technological and software infrastructure** and the preservation system supported by it.

Upon indication of the eSIGN Manager, SOSI keeps the IT infrastructure and application up to date according to Entaksi's preservation policies and customers needs, in compliance with current legislation and international standards.

It works closely with SDOS to manage any malfunction report.

SOSI is active from Monday to Friday from 09:00 to 18:00.

[Back to top.](#)

2.3. eSIGN Manager tasks

The following table shows the Preservation Service Manager's tasks and how these tasks are performed:

Table 1. Tasks.

Preservation Service Manager	How is performed
Management tasks: defines the requirements for the provision of the Service, organizes the content of the storage media and manages the security and traceability procedures that guarantee the correct delivery of the Service.	These tasks are performed by Entaksi's ICT staff, through the functions made available by the system software.
Activities monitoring task: archives and keeps available the access using system processing procedures and processing logs.	These tasks are performed by Entaksi's ICT staff, through the functions made available by the system software.
Maintenance and control tasks: checks the correct execution of the application software procedures and updates the service after the bug fixing or the change request.	These tasks are performed by Entaksi's ICT staff, through the use of a software management system with which maintain the software versioning.
System check tasks: verifies the correct functionality of the system and the software managed.	These tasks are carried out by Entaksi's ICT staff, who periodically check system's functionalities.
System safety tasks: guarantees the mandatory measures for the physical and logical security of the Service and for the creation of security copies.	Physical and logical security refers to the Entaksi systems and networks security. It is in compliance with the Entaksi Security Plan policies. Safety copy creation activities are carried out by Entaksi's ICT staff.
Periodic check of system accessibility: periodically verifies the accessibility of the Service, and guarantees assistance to users and staff.	These tasks are performed by Entaksi's ICT staff, through the functions made available by the system software.
SLA compliance check: periodically checks the compliance with the SLA guaranteed to the Customer.	These tasks are performed by Entaksi's ICT staff, through the functions made available by the system software.



NOTE: The Service Manager is not responsible for the content of the individual documents, which are inserted and managed directly by customers.

2.4. Service management responsibilities

Table 2. Responsibilities

Service Manager	Customer	eSIGN Manager
Generation of data necessary for the Service provision	R	
Data and documents entry	R	
System's availability to receipt and process the data sent		R
Data consistency check	R	

Service Manager	Customer	eSIGN Manager
Management and periodic update of system software and DB		R
Execution of application management activities	R	
Check of elaborated data	R	
Search and browse of documents managed via web interface	R	
Use of elaborated data	R	
Errors or malfunctions reporting	R	
Backup generation and safe storage		R
Periodic check of system accessibility		R
SLA compliance check	C	R

R indicates the manager responsible, C who collaborates in carrying out the activity.

[Back to top.](#)

3. Entaksi Console registration procedure

eSIGN service can be accessed after a **user registration to the Entaksi system Console**, which is reachable at the address <https://entaksi.eu/console/#/>

The web interface allows you to access all Entaksi's services. All the different services can be used combined or individually from this interface. Entaksi's services are described on [our site](#).

In order to access to the chosen service, each user must be **registered on the Entaksi Console platform**. He can log into the desired service using his registered credentials (username and password). Credentials are unique for every service provided by Entaksi.

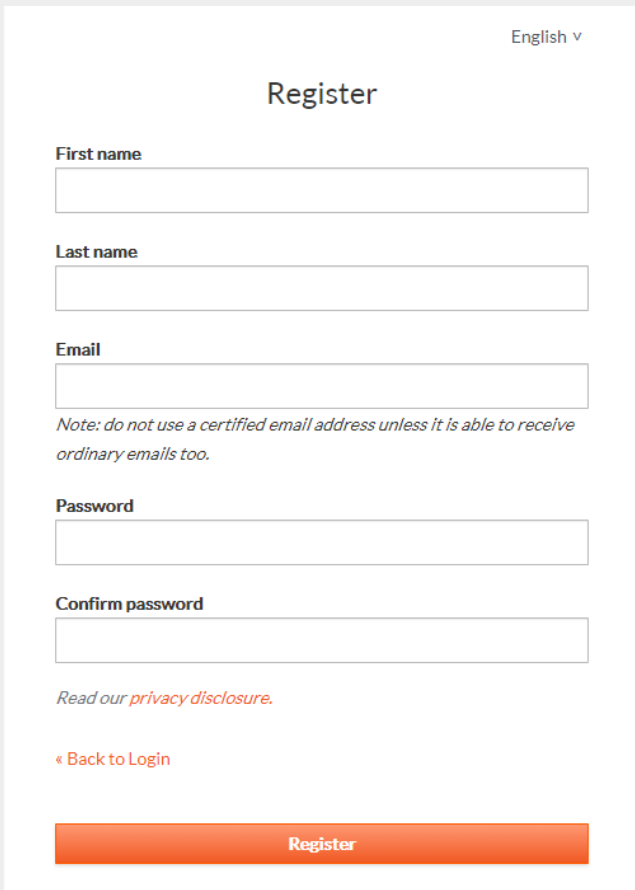
The registration platform complies with the OAuth2 standard which guarantees high levels of access and credential protection.

The access to services' functionalities is subject to the completion of the contract.

In order to register himself, the user must therefore access the Entaksi Console and click on the link "**Register**" placed next to the question "New User?".

Figure 3. Sign in.

Into the following form the user must enter his personal data: name, surname, **NOT PEC email if not enabled to receive non-certified email**, username and password.



English v

Register

First name

Last name

Email

Note: do not use a certified email address unless it is able to receive ordinary emails too.

Password

Confirm password

[Read our *privacy disclosure*.](#)

[« Back to Login](#)

[Register](#)

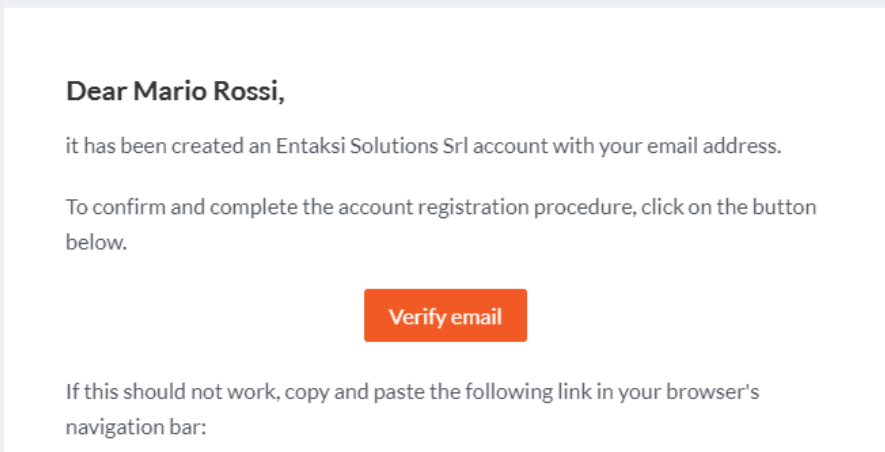
Figure 4. Inserimento dati.



ATTENTION: in order to be able to send the verification email it is required that **the email address indicated in the registration form is NOT a PEC address** as not all PEC mailboxes are enabled to receive non-certified email, and so the verification message should not reach its destination.

Once the information has been entered and the "Register" button is clicked, the data is stored but **the user is not yet active as the verification of the entered email address has yet to be performed.**

The system automatically sends an **email to the address indicated during registration, containing a link that the user must click to complete the registration procedure.**



Dear Mario Rossi,

it has been created an Entaksi Solutions Srl account with your email address.

To confirm and complete the account registration procedure, click on the button below.

[Verify email](#)

If this should not work, copy and paste the following link in your browser's navigation bar:

Figure 5. Email confirmation.

For security reasons, this link is valid and active for 360 minutes (6 hours) from the sending. After this time it will no longer be usable. If necessary, see the paragraph [Resend registration link and password recovery](#). If the registration is not completed, the data will be deleted from the systems within 7 days.

Once confirmed by clicking on the email link, the user is directly redirected to the activated service. From this moment it is possible to access the service entering the name and password previously chosen.

3.1. Single Sign-on access

Single Sign-on access is also available by **Google**, **Apple** or **Microsoft** account.

In this case, the user has to click on the appropriate button of the desired service on the right part of the screen to log in.

Once the account has been selected and logged in, the system acquires the user data directly from the external service, proposing the email verification message again and sending the email to the selected address.

The email confirmation procedure is the same as for standard registration.

[Back to top.](#)

3.2. Resend registration link and password recovery

In the event that the verification email has not arrived or more than 360 minutes have elapsed since receipt, the user can **get a new message containing the confirmation link** by logging back to the page of the service and entering username and password chosen during registration.

The system will not allow access yet, but will send a new confirmation email.

In case of **loss of the password** the recovery is possible by accessing the login page and clicking on "**Forgot Password?**".

On the proposed form the user must indicate username or registration email, and the system will send a message to the registered email address containing a link to start the password recovery procedure.

3.3. How to access the Service

The Service is available using the following browsers:

- **Google Chrome**
- **Mozilla Firefox**
- **Safari**
- **Internet Explorer**
- **Microsoft Edge**

To ensure security during the transfer of information, the connection involves the use of TLS protocols.

[Back to top.](#)

3.4. User settings management

From the eSIGN service access link <https://entaksi.eu/console> it is possible to view the user profile settings by clicking on the user name at the top right.

By clicking on **User settings** in the menu, it is possible to view the user data and make changes related to:

- **Account:** it is possible to change the name and the surname of the user displayed and the login email (it will require a new confirmation via email).
- **Password:** the user can enter a new password.
- **Authenticator:** a QR code is available for mobile applications such as FreeOTP and Google Authenticator in order to activate two-factor verification. This will add an additional security code generated by these applications after each access. On first use, the user has to scan the QR with the smartphone and to enter the verification code.
- **Related accounts:** here it is possible to connect a Google, Apple or Microsoft account.
- **Sessions:** from this tab it is possible to check the sessions currently active for the user, with the referred IP address, starting time, last access and type of open application. If unauthorized sessions are detected, it is possible to interrupt them by clicking on "Log out all sessions", log back in, and set a new password.

- **Log:** the list of all the sessions opened by the user in the last two months is available here.

[Back to top.](#)

4. eSIGN Console

The eSIGN service is available on **Entaksi Console**, the web application that allows you to **manage signing process, to preserve signed documents in compliance with law, to search them in the system and to download Dissemination Information Packages (DIP), which contains legally-compliant documents to show in case of inspections and controls.**

Through the Console you can access the eSIGN service in SaaS mode.

The Entaksi Console is a flexible and configurable application. Through the configuration tools, each user can be set on different roles and different levels of data visibility.

The interface has a left side menu from which you can access your reference company or a list of companies if you are associated with more than one.

4.1. Dashboard

The page is divided into **"My services"** and **"Preservation system"**.

All contracted services are displayed in **"My services"** section.

By clicking on each service button, the main page opens.

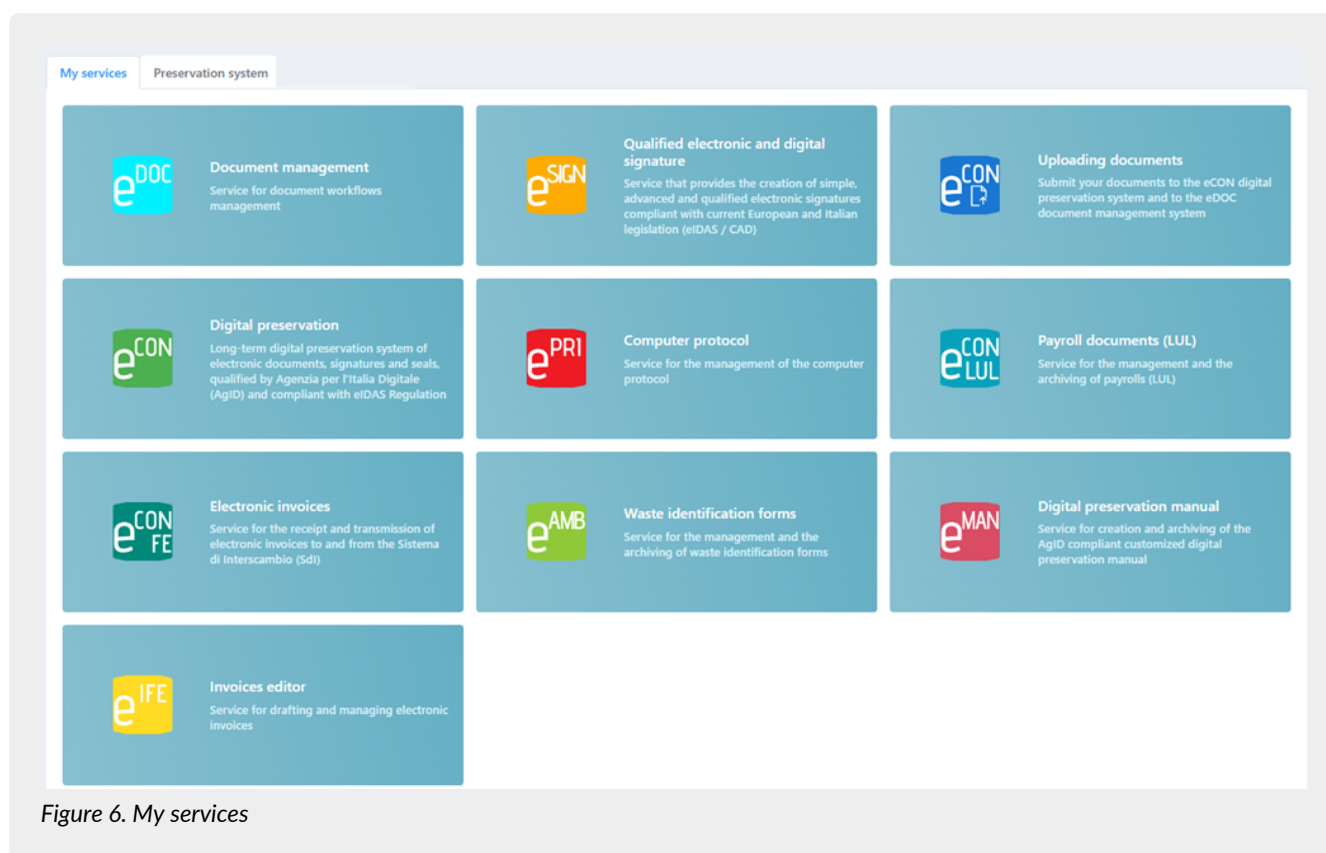


Figure 6. My services

The **"Preservation system"** section presents a summary of the archive status, with the quantity of space disk occupied, number of documents and files uploaded.

Below there is a summary of the latest uploaded documents divided into three sections Submission Information Packages, Archival Information Packages and Dissemination Information Packages.

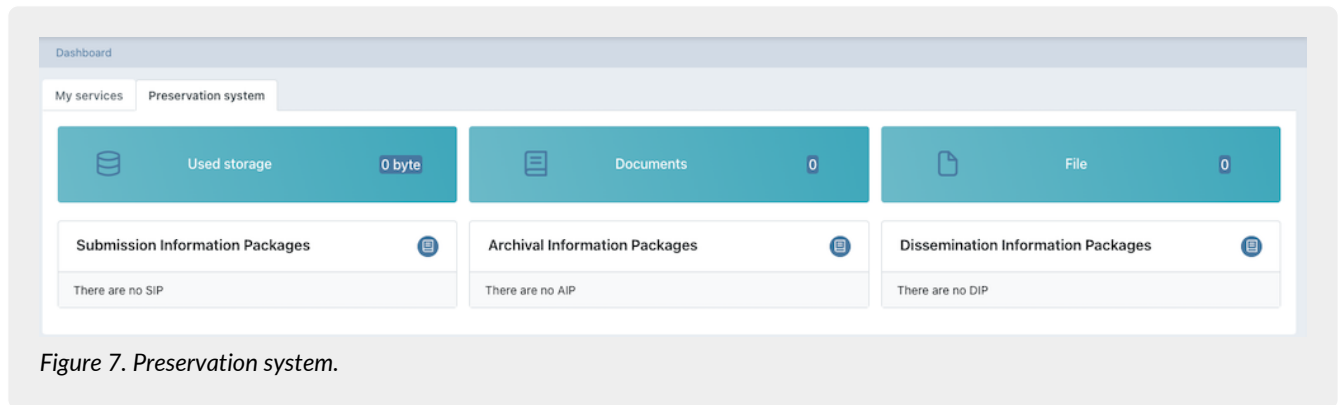



Figure 7. Preservation system.

By clicking on the  button the eSIGN service page opens where all the packages in the system are listed, not just the last ones.

By clicking on the single package, its detail page opens.

4.2. Console tables

Entaksi Console contains several tables that **allow you to navigate and to search data quickly**.

By clicking once the row, it is highlighted, and **it is possible to scroll the list with the keyboard directional arrows**, both on rows and columns. The selected row can be opened by pressing the enter key or by clicking on it.

Thanks to the breadcrumb on the top left of the page, you can go back to the previous table and the selection stays kept. In case the table has many rows, this function is particularly useful and it allows you to **navigate the contents** without losing the sign on the list.

For all system tables, two functions are particularly useful to have an immediate search within the list: the **Filters** and the **Sorts**.

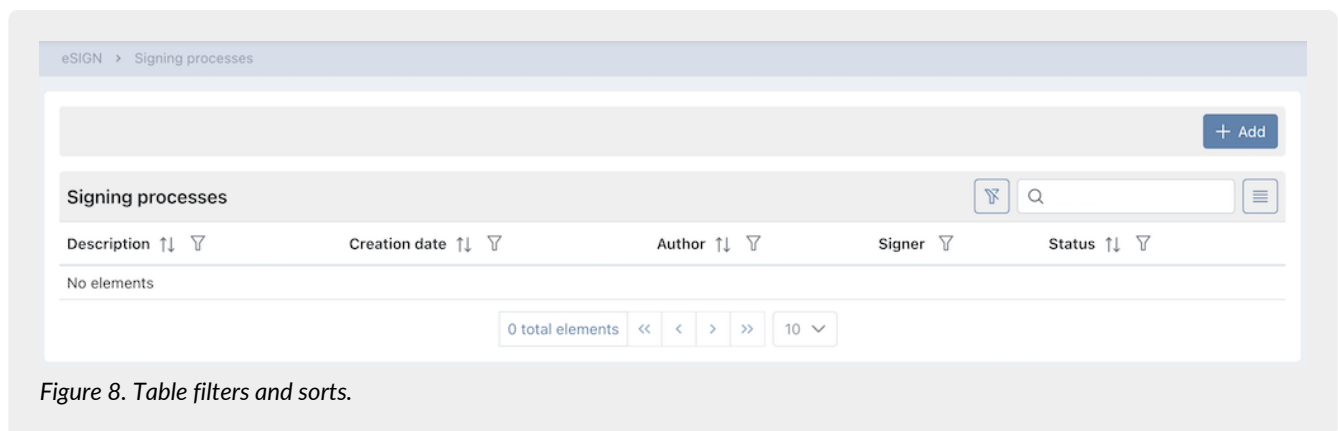






Figure 8. Table filters and sorts.

By clicking on the column header on the  icon you can sort the list in ascending order (and in this case the icon becomes ) or in descending order (and in this case the icon becomes .

There are several types of available sorting:

- **By date:** data will sort with respect to the date.
- **By number:** data will sort with respect to the numerical value.
- **By text:** data will sort alphabetically.
- **By list:** data will sort with respect to the order of the list elements.

In order to filter data, you have to click on the icon  on the desired column. A form opens and you can enter the desired filter.

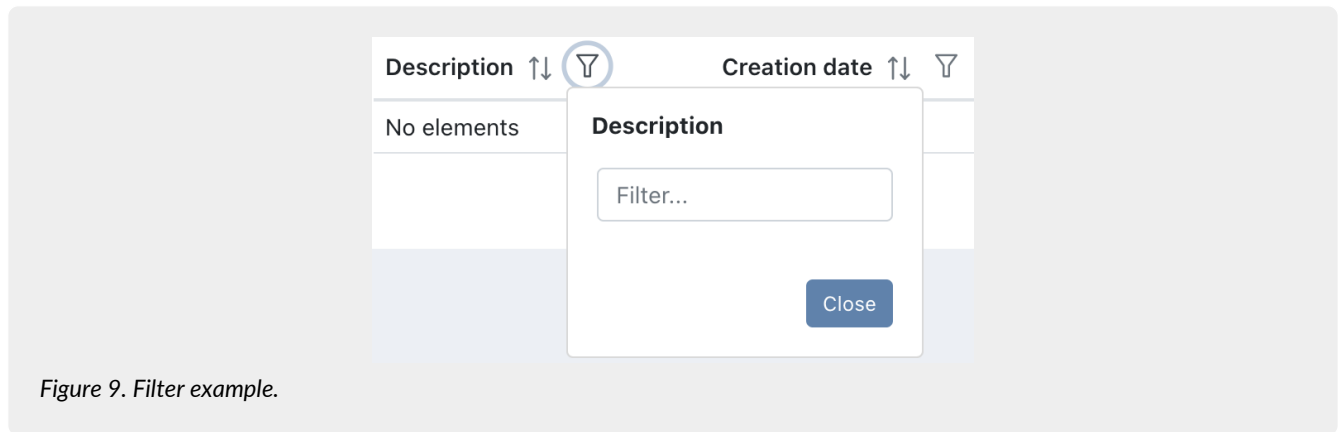




Figure 9. Filter example.

By entering the criterion and clicking the "Close" button, the list filters and the icon turns colored (). It indicates the presence of a criterion.

Hovering with the mouse over the icon a tooltip displays the criterion without entering in the form again.

By clicking on the delete filter button () placed at the top right next to the box search, you can massively eliminate all the filters and orders of the list.

On the other hand, if you have several filters set but you need to delete a single one, you have just to click on the "filter" icon again, enter the form, delete the criterion and click the "Close" button.

Various filter types are available:


- **By date:** you have to enter a valid date or choose it directly from the calendar by clicking on the right icon.
- **By text:** you have to enter the text inside the box.
- **By list:** they are filters that are applied by choosing an option from those in the list.

At the top right, there is an additional filter "Search" box which allows you to perform a selection with respect to the entered value not on a specific column, but on all columns in the table.

This function is available only for text and number data, it is **not** available for date and list data.


The search keys also **filter the counts of the buttons on the bottom of the page** (eg: if the company has a total of 100 SIPs and the you search in the "Status" item only those rejected, finding 2, also the count at the bottom of the page will show only the total number of rejected SIP, namely 2).

The **made searches** are recorded in the browser cache: so, the search key will preserve.

In order to have all the available data, it is necessary to clean all the search keys by clicking on the delete filter button () or by cleaning each search key.



WARNING: this useful feature of preserving search keys during site navigation by saving them in the browser cache implies that, in case of service updates, saved information may not be consistent with the new version of the console.
We therefore recommend **to clear your browser's cache with each update**, in order to avoid any malfunctions.

With  button it is possible to include or to omit the displayed columns in the list. In fact, by clicking on it, the list of available columns is displayed. By clicking on the column of interest, if it is displayed, it will hide. Otherwise, if it is hidden, it will display.

Any column view changes are logged in the browser's cache, therefore they are preserved.


4.3. Console Menu


The Entaksi Console Menu is located on the left side of the page.


The menu is dynamic: **exclusively** the items relating to the contracted services and functions appear.

The side menu display is minimized by default: only the icons identifying the service and features are visible.

To view the fully open menu with the description of the main items, it is necessary move to the sidebar with the mouse.

If you wish to block the side menu in full view, click on  icon.

To view the sub-items of each menu, click on the scroll arrow  : a drop-down menu opens and by clicking on each item the respective page is displayed.

To unlock the menu and close it laterally, click on .

By clicking on each single menu item, the page is displayed on the right side.



WARNING: For quick access to Entaksi services, it is recommended to bookmark the main page link <https://entaksi.eu/console> rather than links to other pages of the service.

This is because if internal links are reorganized for technical reasons, a "404 page Not Found" would be returned, and in such cases, you will need to start from the main link.

5. Configuration

The configuration section of the eSIGN service displays company master data and allows you to configure the general properties of the preservation service such as user's roles or notifications.

The menu contains:

- **Company master data:** section where it is possible to view the company master data entered in the service contract ([Company master data](#))
- **Access management:** section where it is possible to view the list of users connected to the selected company ([Access management](#)).
- **Notification:** section where it is possible to configure the email notifications sent from the system ([Notification](#)).
- **Classification scheme:** section where it is possible to configure and manage the classification scheme of the company ([Classification scheme](#)).
- **Organizational areas:** section where it is possible to configure and manage the company organizational areas ([Organizational areas](#)).

5.1. Company master data

In the **Company master data** section it is possible to view the data submitted by the company during the service registration.

The data cannot be changed directly, because it refers to the service contract. For any changes it is necessary to contact helpdesk@entaksi.eu.

5.2. Access management

In the **Access Management** section, the list of users related to the company and to the contracted services is shown. The association with the company and the service allows users to access all the various functions.

The page contains several sections dedicated to a specific service.



The display of these sections is dynamic: only the sections of the contracted services are shown.

In each section, users are listed and their role is shown.

Below there is a brief description of the items and filters in the list.

- **Name:** it is the user's name.
- **Surname:** it is the user's surname.
- **Username:** it is the user's username.
- **Email:** it is the user's email.
- **Role:** it is the user's role in the service.
- **Date of acceptance:** it is the date the user was entered.
- **Data of revocation:** it is the revocation date, when the user is revoked.
- **Additional data groups:** it shows the visibility of additional data management.
- **Status:** user's role status.

From this section it is possible:

- to sort the columns and filter the elements in the table as described in [Console tables](#);
- to modify the user by clicking on , only if the status of the role is "Activated";
- to delete the user by clicking on , only if the status of the role is "Activated".

The table below lists the possible values for the "Status" of the user role:

Value	Description
TO ACTIVATE	The user is inserted, but the role is not yet active: the user can't access to the eSIGN service.
ACTIVATED	The user is inserted and the role is active: the user can access to the eSIGN service.
TO REVOKE	A role revocation is requested for the user.
REVOKED	The revocation requested for the user is definitive (also confirmed by the value of the revocation date): the user can't longer access to the eSIGN service.

To insert a new user, click on the "Add" button. A new form opens where you have to enter the user's name, surname and email. You have also to select a profile among those available.

Each service has roles and dedicated configuration possibilities.

Mandatory fields are shown in red and you'll save only if they are correctly filled in.

5.2.1. eCON service access management

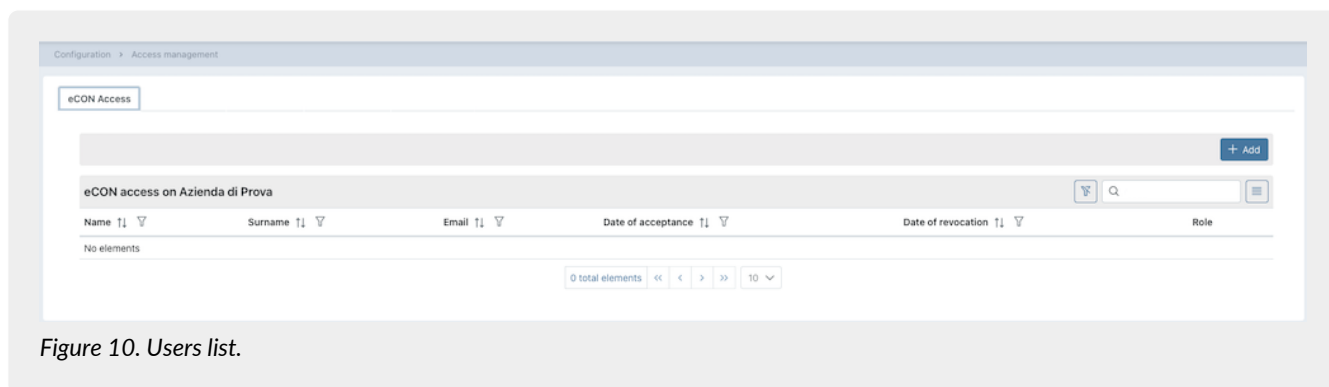


Figure 10. Users list.

The table below shows the available roles for the eSIGN service:

Description	Enabling
Amministratore del servizio (service manager).	The user with this profile can access all the features of the service, including enabling new users.
Utente del servizio (service user).	The user with this profile can access all the features of the service, excluding enabling new users.

If the enabling of document visibility segregation on eCON has been requested, it can be entered when entering the user. In fact, when you are entering the user, you can choose one of the listed segregation possibilities. So, the user can manage **only** the eCON documents for which he has been enabled.

In case an user must have no restrictions (he can manage all documents), just do not select any item.

The system assumes the email from the service contract as service manager, which has privileges over all functions of the service.

When the email address registers and connects to the Console, the personal data will be automatically enhanced with those entered during registration.

5.2.2. eSIGN service access management

In the "eSIGN Accesses" section, in addition to the data listed above, the information relating to the additional data groups is shown.

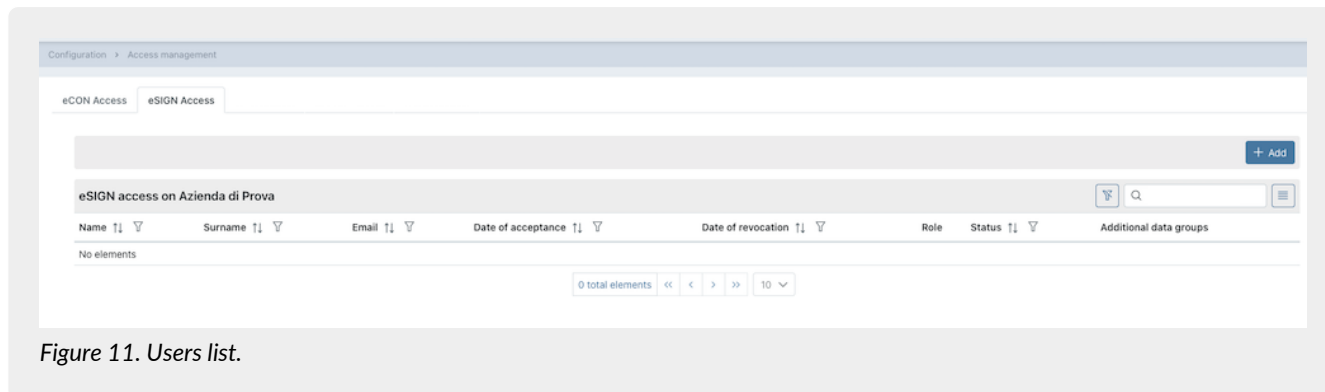


Figure 11. Users list.

The table below shows the available roles for the eSIGN service:

Description	Enabling
eSIGN Administrator	The user with this profile can access to all the functions of SIGN service, including the change of the service configuration, enabling of new users and assigning their profile. He can also view, modify or cancel all processes including those created by other users.
eSIGN Administrator who cannot view signature processes created by other users	The user with this profile can access to all the functions of eSIGN service, including the change of the service configuration, enabling a new users and assigning their profile. He can view, modify or cancel only the signature processes created by himself.
User of eSIGN service	The user with this profile can access to all the functions of the SIGN service with some limitations: he will have access to the service configurations excluding additional data configuration and the additional data group and he will not be able to enable new users. He cannot enable new users. He can view, modify or cancel all the signature processes, including those created by other users.
User enabled to monitor and to create signature processes	The user with this profile can access only to the functions strictly connected to the creation of processes signature and their monitoring. He can view, edit or cancel all signature processes, including those created by other users. He will not have access to the service configuration page and signature reporting page.
User enabled to monitor signature processes created by himself	The user with this profile can access only to the creation of signature processes and their monitoring. He can view, modify or cancel only the signature processes created by himself.
User enabled to monitor signature processes	The user with this profile can access only to the monitoring of signing processes. He can exclusively view all signature processes, including those created by other users.

In the user entry form, after entering the name, surname, email and role, a further section will appear through which the user's additional data segregation can be managed.

☐ The user has visibility into all additional data

Select one or more additional data groups

Figure 12. Additional data segregation.

By default, "The user has visibility into all additional data" option is checked: the user can view and manage all additional data. By deselecting this item, you can choose one or more visibility groups from the list below. The user will enable to manage and view the additional data belonging to the selected groups.

If one of the previous visibility options is not selected, the user can't view and/or manage additional data in any context.

By clicking on the "Save" button, the new user is entered with his role.

5.3. Notification

Entaksi Console provides a tool to configure email notifications automatically sent by the system after some functions.

You can configure your notification settings on the company to which you are associated through the "Notification" link in the "Configuration" menu. If multiple companies are present, you can set different configurations for each one.

At first all the notifications are disabled: you can activate them by selecting the desired sending from the corresponding dropdown for each company.

Notifications can be set to "Do not send" or "Always send", and at the conclusion SIP validation process also "Only in case of error".

5.4. Classification scheme




The classification scheme is a tool to divide documents into sectors and categories, schematizing their competences and functions in a logical way.

In this section, present **only** on some modules and visible **exclusively** for users authorized to manage, it is possible to view all the Classification scheme present in the system, to insert a new ones and to modify those not yet active.

In this page, all the classification schemes entered in the system are listed.

Configuration > Classification scheme

+ Add

Code ↑↓	Description ↑↓	Start date ↑↓	End date ↑↓	Status ↑↓	
2023-xxx	Titolario v.0.2	30/10/2023		DRAFT	 
2023-001	Titolario v.0.1	12/06/2023		CONFIRMED	

2 total elements << < 1 > >> 10

Figure 13. Classification scheme

Below is a brief description of fields preset in the grid.



- **Code:** code automatically assigned by the system in order to uniquely identify the classification scheme;
- **Description:** description entered when saving the classification scheme;

- **Start date:** effective date of the classification scheme;
- **End date:** end date of classification scheme. If empty, the classification scheme is active;
- **Status:** status of the classification scheme.

The table below lists the possible values for the "Status" of the classification scheme:

Value	Description
DRAFT	The classification scheme entered is in Draft. You can modify and / or delete it. This scheme cannot be used for document classification as it is not active.
CONFIRMED	The classification scheme is in confirmed status. You can use it for the classification of documents up to its end date.

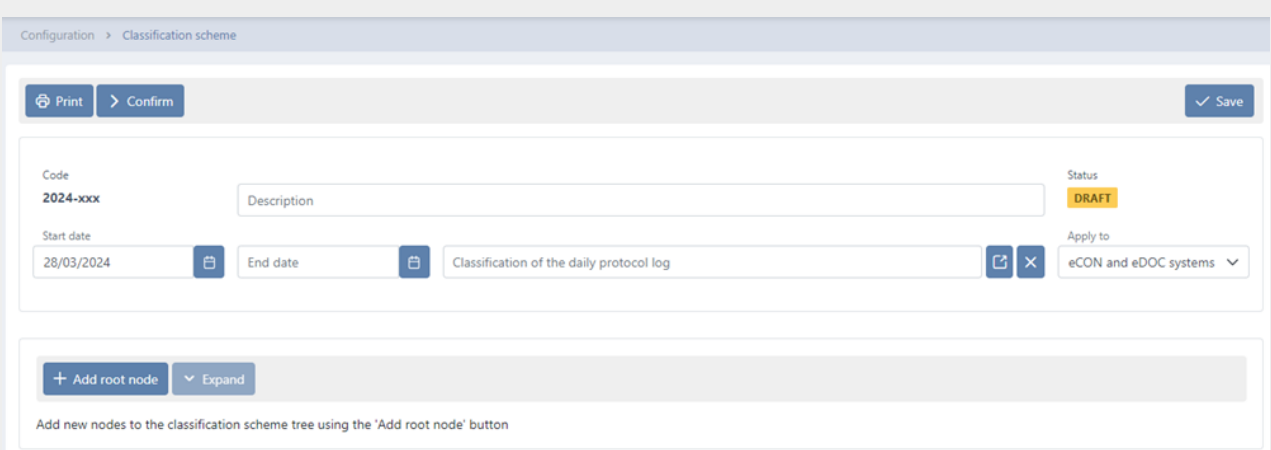
From this section it is possible:

- to sort the columns and filter the elements in the table as described in [Console tables](#);
- to delete the classification scheme by clicking on  only if its status is "Draft";
- to duplicate the classification scheme by clicking on . A new classification scheme will be created with the same tree and same header data except the code which will be aaaa-xxx (see [Adding a classification scheme](#)) and the start date which will be equal to the day after the duplication date;
- to enter in the classification scheme detail page by clicking on the row. If it is in "Draft" status, you can modify it. If it is in "Confirmed" status, you can put it back in draft status only if its start date is after the current one. In any other case, you can only see its structure or apply it only on eDOC, only on eCON or both on eDOC and eCON (see [Adding a classification scheme](#)) by clicking the "Apply" button at the top right;
- to add a new classification scheme by clicking on "Add".

Even if there are more classification schemes (confirmed or not), **only one can be active**. It is the one in confirmed status with an absent (not entered) end date or with an end date greater than the current one.

5.4.1. Adding a classification scheme

By clicking on the "Add" button, a new page opens where you can insert a new classification scheme or modify an existing one.



Configuration > Classification scheme

Print Confirm Save

Code: 2024-xxxx Description: Status: DRAFT

Start date: 28/03/2024 End date: Classification of the daily protocol log Apply to: eCON and eDOC systems

+ Add root node Expand

Add new nodes to the classification scheme tree using the 'Add root node' button

Figure 14. Adding a classification scheme.

During the creation phase, the service assigns an identification code to the classification scheme.

This code will be composed as follows: yyyy-xxx where yyyy indicates the creation year and xxx the unique progressive creation number.

The creation year is assigned immediately, therefore it will be visible even if the title is in draft status.

The unique progressive creation number, on the other hand, it will be assigned only in the confirmation phase of the classification scheme.

In order to insert and to uniquely identify a classification scheme, you have to enter the description and a start date (the date from which the classification is valid).

It should be noted that the start date must **not** overlap with any start date of classifications previously entered in the system. The service proposes the day following the date of creation as the default start date in order to prevent any error.

The expiry date may also not be entered: the system will automatically enter this date upon confirmation of a new classification by reporting in this field the day before its start date.

To enter the classification of the daily protocol log you have to enter the classification tree first, and then to select a node among those in the list.

The selected classification will be automatically reported in the generation of daily protocol logs until the Classification scheme is valid.

This field is mandatory to confirm the classification scheme.

It will also be necessary to specify the scope of the Classification scheme by choosing one of the options in the list:

- only on the eDOC document service: the application of the Classification scheme **exclusively** concerns the display of documents on the document service, the display of the archival register remains unchanged.
- only on the eCON preservation service: the archival register is automatically configured in accordance with the Classification scheme **exclusively** for documents preservation: the display on the eDOC service remains unchanged.
- both on the eDOC document service and on the eCON preservation system: the archival register of documents is automatically configured according to the structure of the applied Classification scheme: documents are preserved in eCON and displayed on eDOC in accordance with the Classification scheme structure.

To change the classification of the daily protocol log is possible only in the draft status.

To cancel a previously entered value, click on .

To save the entered data, but not confirm classification, click on the **"Save"** button placed at the top right.

In addition to the description and the validity dates, it is necessary to define a document organization scheme of the company. The service prevents you from confirming a classification without a saved scheme.

This classification scheme has a tree structure.

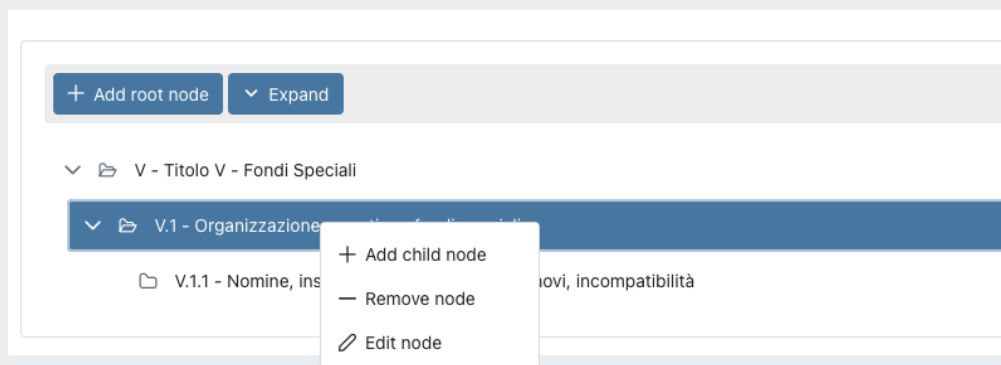


Figure 15. Example of classification scheme structure

To insert the top-level parent node (the "root" node), click on the **"Add root node"** button.

To insert / edit / remove a "child" node, click with the right button of the mouse on the "parent" node: a menu drop-down appears with the three options.

To delete a node, select the **"Remove node"** option. In addition to the selected node, all child elements will be removed.

To edit a node, in the code, description or retention rule, select the **"Edit node"** option, make the desired changes and click on the **"Save"** button.

To insert a node click on the **"Add node"** option: a form will be displayed.

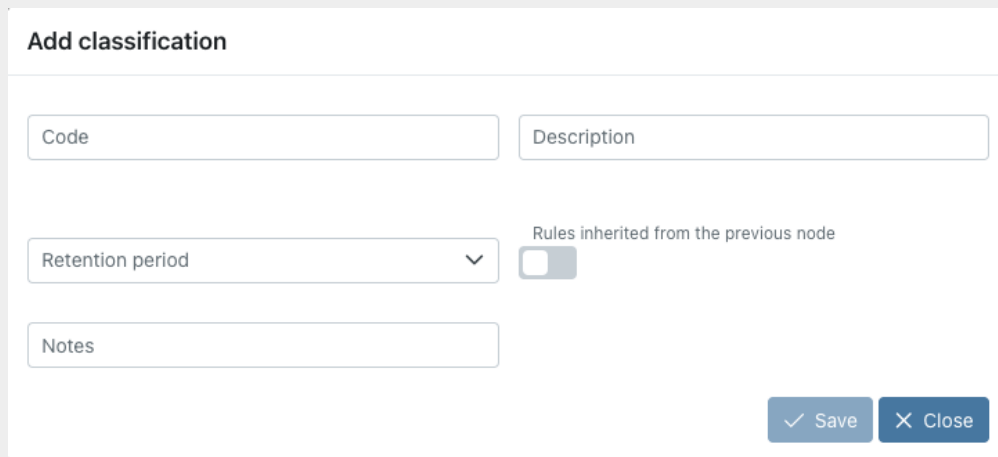


Figure 16. Entering a node.

To complete the entry, it is necessary to enter the code and description of the node, any additional notes, define a conservation rule, choosing an element from those proposed in the list or inherit the rule of the "parent" node by ticking the relevant item, and click the **"Save"** button.

You can choose to inherit the retention rule from the parent node only for child nodes. On the root nodes, this option is not visible.

If you insert nodes without specifying any conservation rule, an alert icon is displayed next to the node in order to help you to quickly identify the node with this missing data.

All actions on the node are automatically saved: it isn't necessary clicking the top right global save key.

By clicking on **"Expand"**, all nodes of the tree will expand showing the whole structure of the tree.

By clicking on **"Collapse"**, all nodes of the tree will compress showing only the "root" nodes.

By clicking on the **"Print"** button, it is possible to print the classification scheme with its retention period.

By clicking on the **"Confirm"** button, the classification passes from the "Draft" status to the "Confirmed" one and, the system automatically sets the end date of the current classification equal to the day prior to the start date of the newly confirmed classification.

In the event that the classification is not active yet, you can make further changes by returning the status to draft click on the **"Modify"** button.

In case of confirmed classification, it is possible to apply its structure both on eDOC service and eCON service by clicking on the "Apply" button on the top right of the page.

5.5. Organizational areas

As defined in Article 50 TUDA, within the context of its legal system, each administration identifies the offices to be considered to coordinate document management in large homogeneous organizational areas, ensuring uniform classification and archiving criteria, as well as internal communication between the same areas.

This section is present only on some services and it is visible only to authorized users. In this section, the homogeneous organizational areas are listed.

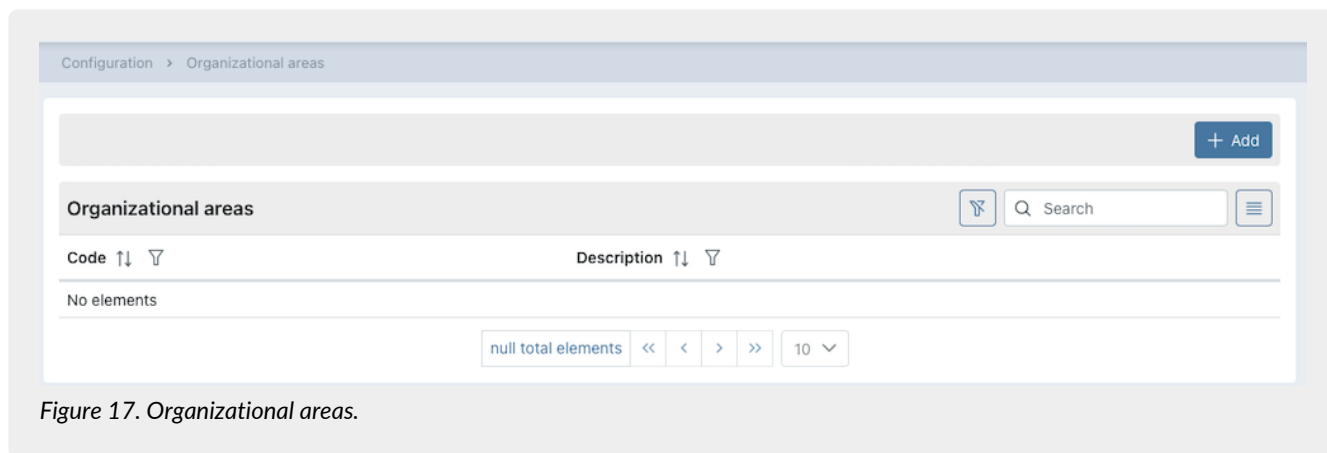


Figure 17. Organizational areas.

- **Code:** it is the code of the homogeneous organizational area entered during insertion;
- **Description:** it is the description of the homogeneous organizational area entered during insertion.

From this section it is possible:

- to sort the columns and filter the elements in the table as described in [Console tables](#);
- to enter in the organizational area detail page to modify it by clicking on the row;
- to add a new organizational area by clicking on "Add".

5.5.1. Entering organizational areas

By clicking on the "Add" button a new page opens where you can insert a new organizational areas.

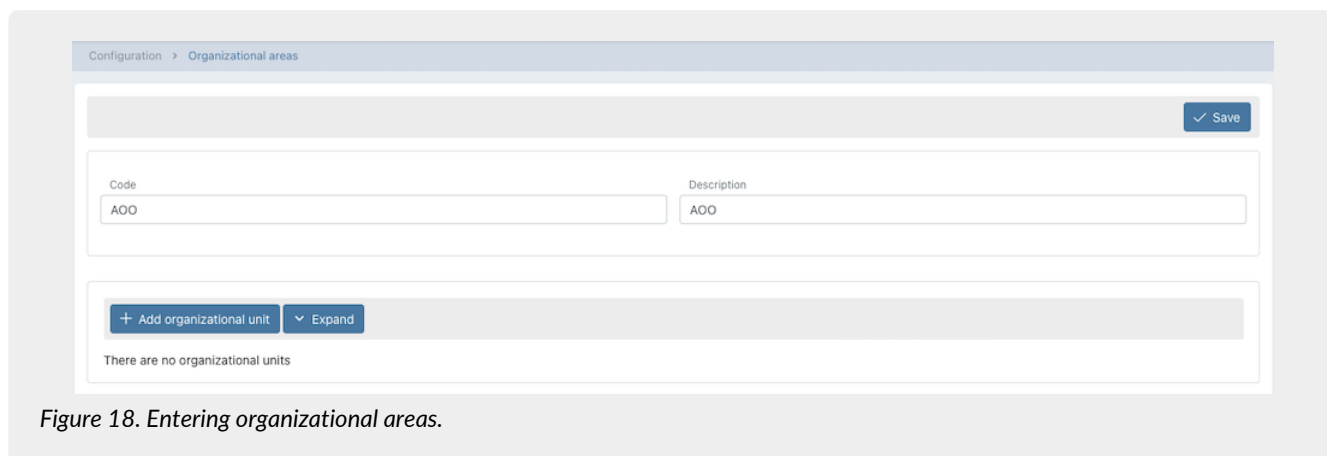


Figure 18. Entering organizational areas.

In order to uniquely identify an organizational area, you have to enter a code and a description.

To save the entered data, click on the top right "Save" button.

To enter a new organizational area click on the "Add organizational unit" button. The inserted organizational units have a tree structure.



Figure 19. Example of organizational area structure.

To insert / edit / remove a "child" node, click with the right button of the mouse on the "parent" node: a menu drop-down appears with the three options.

To delete a node, select the **"Remove node"** option. In addition to the selected node, all child elements will be removed.

To edit a node, in the code, description or retention rule, select the **"Edit node"** option, make the desired changes and click on the **"Save"** button.

To insert a node click on the **"Add node"** option: a form will be displayed.

Figure 20. Entering organizational area units.

To complete the entry, it is necessary to enter the code and description of the node and click the **"Save"** button.

By clicking on **"Expand"**, all nodes of the tree will expand showing the whole structure of the tree.

By clicking on **"Collapse"**, all nodes of the tree will compress showing only the "root" nodes.

6. eSIGN signing processes

The eSIGN service allows the correct management of electronic signature processes on documents previously uploaded to the system.

You can upload:

- templates (models in .odt or .docx format) through which, thanks to special markers, you can create PDF files to be signed containing predefined data from the system;
- PDF files to be signed in a process;
- PDF templates previously loaded and suitably configured. So, at the start of the process, an automatic recognition of the signatures takes place and you have not to choose the signatory user for each signature phase.

Once logged in to the Entaksi Console, in order to access to the eSIGN service, you can click on the dashboard button **"Qualified electronic and digital signature"**, which links to the **Signature Processes** page, or you can use the **"eSIGN"** main menu: each item opens the respective page.

The menu **"eSIGN"** includes:

- **Signing processes**: a list of all signing processes created through the eSIGN service (see [\[signing processes\]](#));
- **Process template**: a list of all templates created to standardize signing processes (see [Process template](#));

- **Signatory user:** a list of all signatory users registered in the eSIGN service (see [Signatory users](#));
- **Signatory group:** a list of signatory user groups for the bulk sending of signing processes (see [Signatory groups](#));
- **Configurations:** the general configurations of the eSIGN service;
- **eSIGN Desktop:** the page for downloading the eSIGN Desktop application and the drivers necessary for the proper use of signing devices ([eSIGN Desktop](#));
- **Signatures report:** display the number of signatures used in the various signing processes entered ([Signatures report](#)).

6.1. Configurations

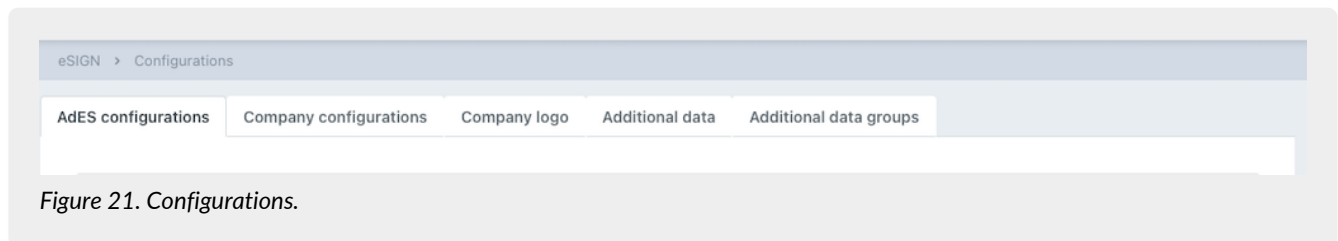


Figure 21. Configurations.

"Configurations" page is divided in five sections.

- **"AdES configuration"**, where it is possible to request an AdES agreement signature acceptance process for the signatory user;
- **"Company configurations"**, where it is possible to configure notifications of the signing process and actions to submit documents to the preservation system or to the document management system;
- **"Company logo"**, where it is possible to upload the company logo that is shown in the sent emails;
- **"Additional data"**, where it is possible to configure additional data and its properties;
- **"Additional data groups"**, where it is possible to aggregate additional data.

Any visibility segregation can be defined at the user role level (see [Access management](#)).

6.1.1. Link for starting AdES agreement signature acceptance process by the user

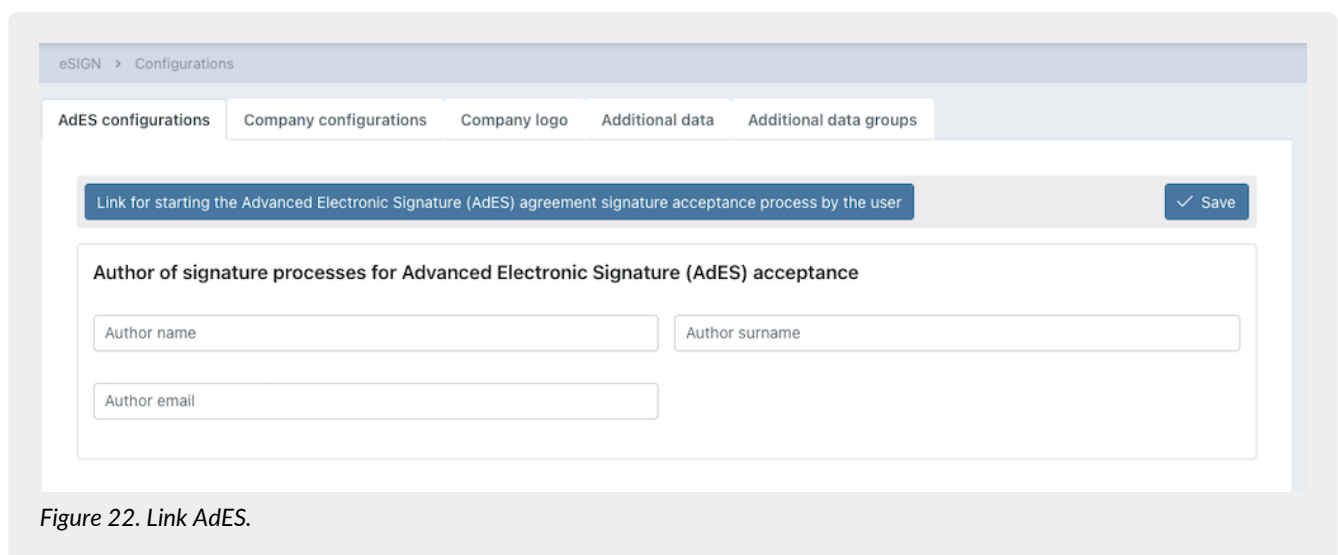


Figure 22. Link AdES.

Through this link, it is possible to request an AdES agreement even if the user's personal data is not entered.

First of all, you have to configure an AdES template with editable fields, in order to enter signer's personal data as described in [Adding signature process template](#) and [Markers](#).

Once the template is configured, by clicking on the button, a new AdES process starts. When the document is signed with the required data, the new signatory is added to the service.

The process is visible in the process list, so you can download the AdES document.

In the event that no author is specified in the "Author of signature processes for AdES acceptance" section, the process author

is one of the users enabled for the service.

In the event that, on the other hand, in the "Author of the signature processes for AdES acceptance" section an author is specified, he is the author of the AdES acceptance process from link.

To save an author, enter the name, surname, email and click on the top right button "Save".

If you do not want to specify a precise author, having previously saved one, cancel all three fields and click the "Save" button to confirm the operation.

6.1.2. Company configurations

Configurations saved on this page are proposed automatically in each new process. It is also possible to modify this configuration as you want (see paragraphs [Adding a signature process](#) and [Adding signature process template](#)).

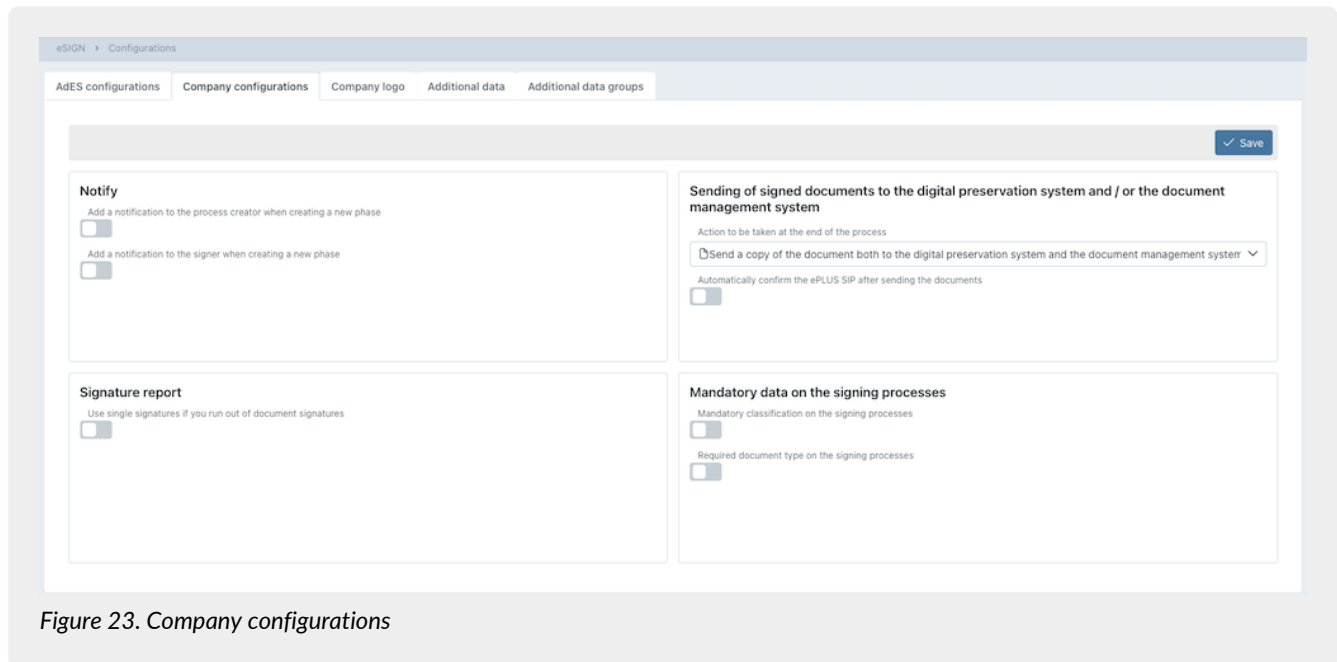


Figure 23. Company configurations

In the "Notify" section, it is possible to configure notification emails both for the process author and for its signatory (see paragraph [Signing process workflow](#)).

By checking the "Add notification to process creator when creating a new phase" item, this configuration is proposed when adding new phase in a process. So, when the document is signed, a notification email is sent to the process creator with the signed document as attachment.

By checking the "Add a notification to the signer when creating a new phase" item, when the document is signed, a notification email is sent to the signer with the signed document as attachment.

In the "Sending of signed documents to the digital preservation system and / or the document management system" section, it is possible to configure the signed documents submission to the document management system and/or the preservation one.

In the list, you can choose from the following options:

- "send a copy of the document to the digital preservation system at the end of this phase". By selecting this option, at the end of the process, the signed document is sent to the ePLUS service to create a SIP. Then, the SIP is submitted to the preservation system. It will be **only** in the preservation system and **not** in the document management system;
- "send a copy of the document to the document management system at the end of this phase". By selecting this option, at the end of the process, the signed document is sent to the document management system. Then, documents are **only** in the document management system and **not** in the preservation one;
- "send a copy of the document both to the document management system and the digital preservation system at the end of this phase". By selecting this option, at the end of the process, the signed document is sent both to the document management system and the digital preservation system. The signed document is sent to the ePLUS service to create a SIP. Then, the document is **in both** systems, in the document management system and in the preservation one.

The chosen option is automatically proposed when creating a process or a template phase. If more phases are entered, the option is present **exclusively** on the last one.

By checking "**Automatically confirm the ePLUS SIP after sending the documents**", the created SIP in the ePLUS service is automatically closed and submitted. By not checking this item, the SIP will remain open in the ePLUS system and you have to close it manually to submit documents.

In the "**Signature report**" section, by clicking on "**Use single signatures if you run out of document signatures**", it is possible to decide to consume the purchased single signatures when the purchased document signatures are finished.

In the "**Mandatory data on the signing processes**" section, it is possible to configure mandatory fields when creating a signing process.

- **Mandatory classification on the signing processes.** This option is only visible if there is an active classification scheme in the Company and the user is authorized to select the classification.
By checking this item, you cannot start processes without having valued this field.
- **Required document type on the signing processes.** This option is always visible.
By checking this item, you cannot start processes without having valued this field.

The mandatory nature of these two fields is independent of each other: you can request the mandatory of both, of only one or neither.

To save the entered configurations, click on the "**Save**" button.

6.1.3. Company logo

In this section it is possible to insert the company logo which appears in the header of the email sent from the eSIGN service .

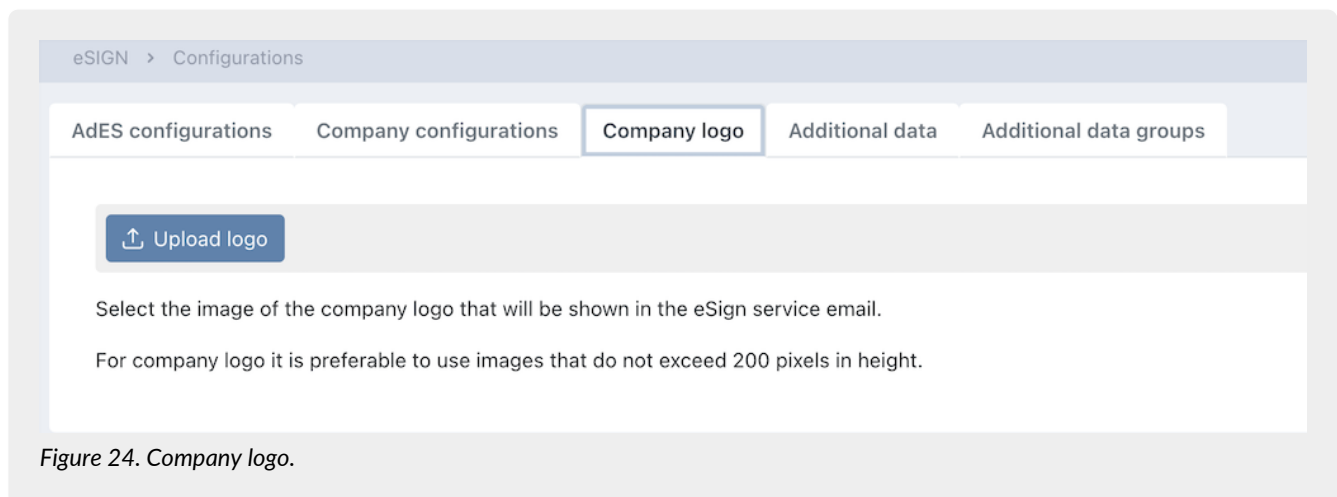


Figure 24. Company logo.

By clicking on the "**Upload logo**" button, you can choose the desired image.

In order to obtain an optimal display of the company logo in emails, it is better to use images that do not exceed 200 pixels in height.

Once having selected the image, a preview is shown.

By clicking on the "**Delete**" button, it is possible to delete the inserted image and to select another one.

If no image is saved, the emails are without the company logo. The eSIGN logo is visible on the right side of the emails.

6.1.4. Additional data

This type of data can be customized and configured by the company.

Except for the label which has a purely internal and descriptive value, additional data are markers linked to the signer. The code is the element and the description the value (see paragraph [Markers](#)).

Through this type of data suitably inserted in the .docx or .odt file with the "extra" type markers, the company can manage generalized templates for all signatories (see [Process template](#)). The value of data is linked to the signer of the signature phase. In fact, the values displayed during the signing phase are those entered in the signer's personal data section in the service (see [Signatory users](#)).



The additional data entered in this section is automatically reported in all personal data of the signatory users.

This type of data can contain sensitive information. So, its visualization and management can be suitably segregated (see [Access management](#)).

In this section all the entered additional data is listed. This section is visible only to the service administrator user (see [Access management](#)).

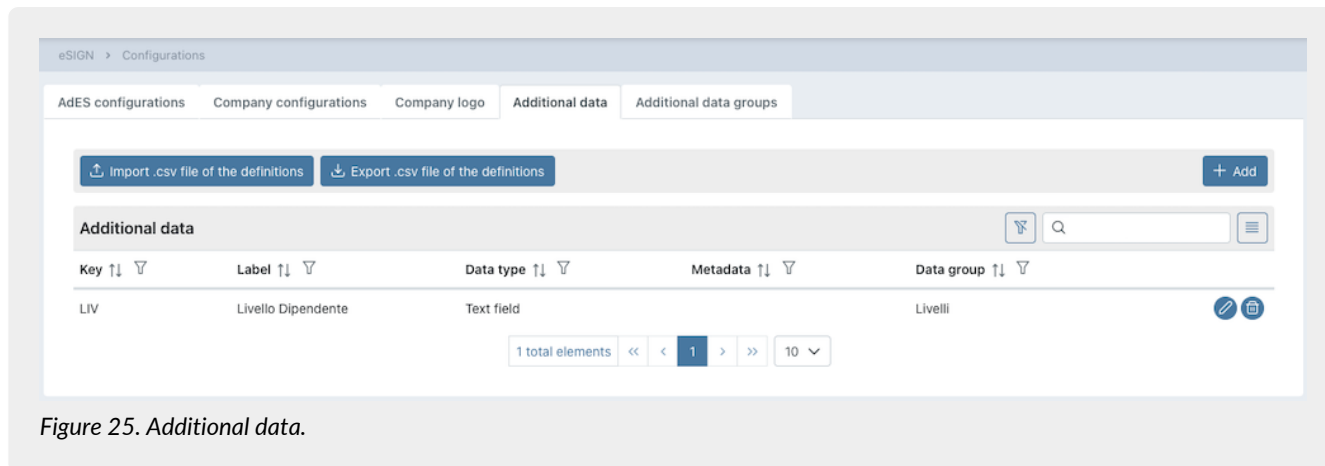




Figure 25. Additional data.

Below there is a brief description of the items and filters on the list.

- **Label:** further description relating to the additional data;
- **Key:** unique key that identifies the additional data;
- **Metadata:** metadata linked to the additional data. This metadata will be present in the SIP of the eSIGN documents. It will be filled with the value of the additional data in the signatory's personal data.
For this reason it is **not** possible to associate a metadata with multiple additional data: each metadata must be associated with one and only one additional data;
- **Data group:** group to which the additional data belongs. Its management is described in the next paragraph [Additional data groups](#).

From this section it is possible:

- to order the columns and filter the elements as described in the [Console tables](#) chapter;
- to modify or delete additional data by clicking on  and  respectively placed at the bottom right.
To change the values click the "Save" button on the edit form.
You cannot delete an additional data if it is present in templates or processes.

To enter new additional data, there are the following ways:

- to create a template with a file containing new additional data (see [Process template](#));
- to upload a personal data .csv file containing a new additional data (see [Integration of personal data by file](#));
- to click on "Add" in this section;
- to import a .csv file with new additional data in this section.

By clicking the "Add" button, a further form opens. You can enter the identifying information of the additional data, such as the key, the label, the field type and the metadata link.

Additional data

Key Label

Field type Field min length

Field max length Pattern for validating the value of additional data

Mandatory ☐

Metadata

Figure 26. Manual entry of Additional Data.

After having entered the key and the label fields, you can choose type of the additional data. The insertion options are displayed. By default the system proposes the "Text field" as field type.

The mandatory options are highlighted in red when saving.

The table below shows the options for each field type.

Field type	Description	Options
Text field	The additional data could be filled only with a text. The imputable characters will be free, respecting, however, the length maximum and/or minimum if entered.	Mandatory: if checked, the field is mandatory in the signing phase; Field min length: it is the minimum length of the field; Field max length: it is the maximum length of the field; Validation pattern: it is the validation criterion that you want to adopt to verify the correctness of the entered text by the signer. Since validation patterns have a complicated and non-standard construct, please search online the correct string according to your needs and check it on the site regex101.com .
Numeric field	The additional data could be filled only with a numerical value.	Mandatory: if checked, the field is mandatory in the signing phase; Digits: they are the decimal digits of the numeric field.
Date field	The additional data could be filled only with a date type field.	Mandatory: if checked, the field is mandatory in the signing phase.
Date-time field	The additional data could be filled only with a date-time type field.	Mandatory: if checked, the field is mandatory in the signing phase.


Field type	Description	Options
Values list field	The additional data could be filled only with a item in a list. The list items are configurable in the options.	Mandatory: if checked, the field is mandatory in the signing phase; Values list: it is the list of values that can be chosen during the signing phase. List values must be entered with the following construct: Value1#Value2#Value3#.
Yes/NO field	The additional data could be filled only with a Yes/NO or empty value. It can assume the values "YES", "NO" or empty (if it is not mandatory).	Mandatory: if checked, the field is mandatory in the signing phase.

To associate a metadata with additional data, you have to select the desired value in the metadata list.

If you want to delete a previously saved association, click on the button  in the right side of the metadata list.

By clicking on the **"Save"** button, the additional data is saved.

By clicking on the **"Close"** button, the additional data is not saved.

To change the type of additional data, i.e. from text to list, simply edit the additional data by clicking on the  button, change the field type, enter any values in the optional fields for the chosen type and click the "Save" button.

In the event that the selected field type is consistent with any additional data filled in the register of signatory users, the change is saved immediately.

Otherwise, a message is displayed reporting all the found anomalies and if you approve the modification, the non-compliant additional data in the register of the signatory users will be deleted.

By clicking on the buttons on the top left of the section, it is possible to export or import CSV files for the management of additional data.

By clicking on the buttons on the top left of the section, it is possible to export or import CSV files for the management of additional data.

To export all additional data of the registry, click on the **"Export .csv file of the definitions"** button.

To export only a set of additional data, filter the list in order to obtain the desired data and then click on **"Export .csv file of the definitions"**: only the additional data listed will be exported.

To import a CSV file click on the **"Import .csv file of the definitions"** button and upload it from the file upload form.

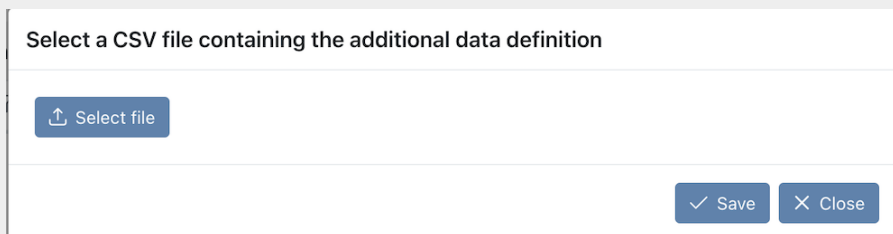


Figure 27. Upload file form.

By clicking on **"Select file"**, you can select the CSV file to upload. By clicking on **"Close"**, the upload is canceled; while clicking on **"Save"** the upload is confirmed.

By confirming the upload, the import procedure will:

- **Overwrite** the data previously recorded in the registry with the data present in the CSV file if the key of the additional data entered in the file is already present in the database;
- **Insert** the new additional data with the information contained in the file if the key of the additional data in the CSV file is not already present in the database.

The upload result is displayed in the central part of the form. In the form are displayed the total number of lines processed, the total number of master data that have been updated or inserted and the number of rows that have problems that have

produced neither insertions nor updates.

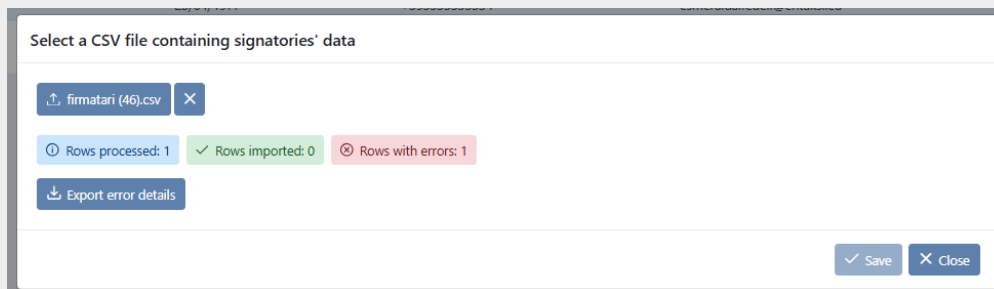


Figure 28. File upload result.

By clicking on "**Export error details**", a file is downloaded. In this file you can find all anomalies and the reason of rejection. By clicking on the "**Close**" button you return to the additional data section. All changes or entries of the additional data are visible.

Below are the rules for the correct construction of the CSV file.

The CSV file must have:

- as column headers the names of the fields for the additional data entry, i.e. the fields in the input form for each selectable field type; the master data or additional data fields name as column headers;
- the values to be entered or modified in the registry as rows ;
- as separator the semicolon character (;);
- as string delimiter the double quote character (").

In order to make a correct file, in the table below you can find the names of the heading columns, the relative descriptions and if it is mandatory.

Field Name	Description	Mandatory
KEY	"Key" field of the additional data.	YES
LABEL	"Label" field of the additional data.	YES
TYPE	"Field type" of the additional data. It can be: TEXT: for the text field; NUMBER: for the numeric field; DATE: for the date field; DATETIME: for the date-time field; LIST: for the values list field; BOOLEAN: for the Yes/No field. In the event that no type is filled, during the import phase the additional data will be defined as TEXT by default.	NO
MANDATORY	"Mandatory" field of the additional data. It can be: true: to make the additional data mandatory; false: to make the additional data not mandatory;	NO
MIN_LENGTH	"Min length" field of the additional data. To be filled exclusively with integer values if the field TYPE takes the value TEXT.	NO

Field Name	Description	Mandatory
MAX_LENGTH	"Max length" field of the additional data. To be filled exclusively with integer values if the field TYPE takes the value TEXT.	NO
DECIMAL_DIGITS	Campo "Cifre decimali" del dato aggiuntivo. To be filled exclusively with integer values if the field TYPE takes the value NUMBER.	NO
VALIDATION_PATTERN	"Pattern for the validating the value of additional data" field. To be filled exclusively with integer values if the field TYPE takes the value TEXT. It is the validation criterion to verify the correctness of the filled text. Since validation patterns have a complicated and non-standard construct, please search online the correct string according to your needs and check it on the site regex101.com .	NO
VALUES	"Values list (separated by)" field of the additional data. To be enhanced with the list of values separated by the character .	YES only if the field TYPE takes the value LIST.

To modify additional data, export the CSV file, modify the values of the additional data and import the modified file.

In case the type of additional data is modified, i.e. from text to list, and it is consistent with any values filled in the register of signatory users, the change is saved immediately.

Otherwise, a message is displayed reporting all the found anomalies and if you approve the modification, the non-compliant values of additional data in the register of the signatory users will be deleted.

To enter one or more new additional data in the registry, simply add a new line for each additional data in the .csv file, valuing the column "KEY" with a value not already existing in the registry and entering mandatory or optional values with respect to the type field.

By importing the file, new additional data will be added in the list.

6.1.5. Additional data groups

The additional data group is an aggregator (precisely group) of additional data. A group can consist of several additional data, but an additional data can belong only to a group.

Through the groups it is possible to segregate the visibility of the additional data contained in it with an appropriate configuration of the user's role (see [Access management](#)).

In this section all the entered groups are listed. This section will be visible only to the service administrator user (see [Access management](#)).

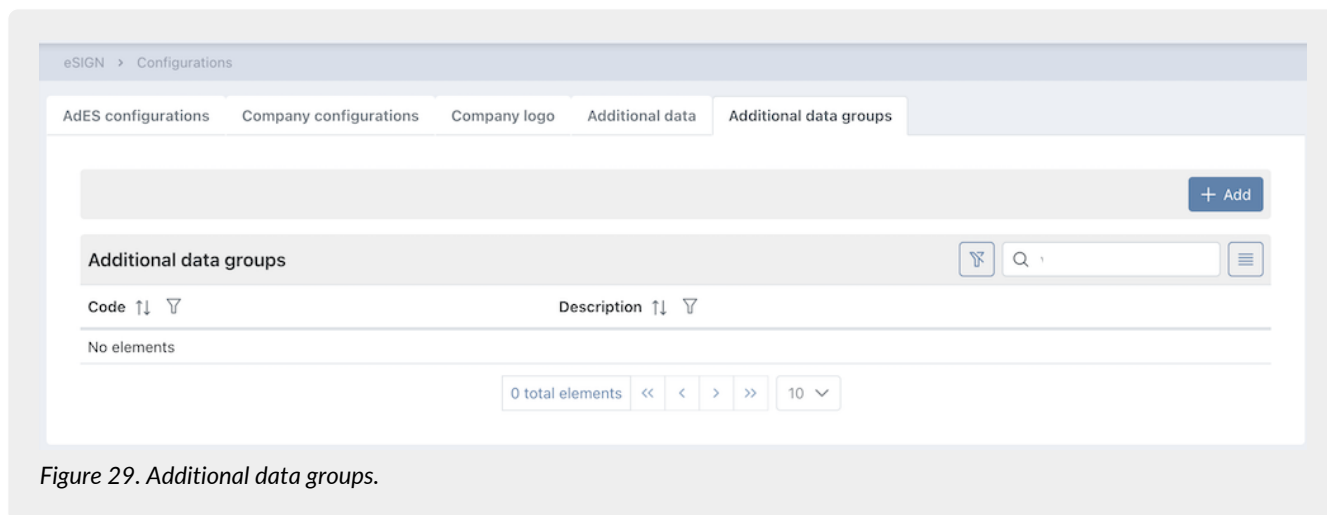




Figure 29. Additional data groups.

Below there is a brief description of the items and filters on the list.

- **Code:** it is the group code;
- **Description:** it is the group description;

From this section it is possible:

- to order the columns and filter the elements as described in the [Console tables](#) chapter;
- to modify or delete groups by clicking on  and  respectively placed at the bottom right. To change the value of the group code or the group description, you have to click the "Save" button on the edit form. You can always delete a group. Once deleted, the group will no longer be visible either in the list of additional data (see paragraph [Additional data](#)) and nor in the role configuration (see [Access management](#)).

To add a new group, you have to click on the "Add" button. A new form opens and you can enter the group.

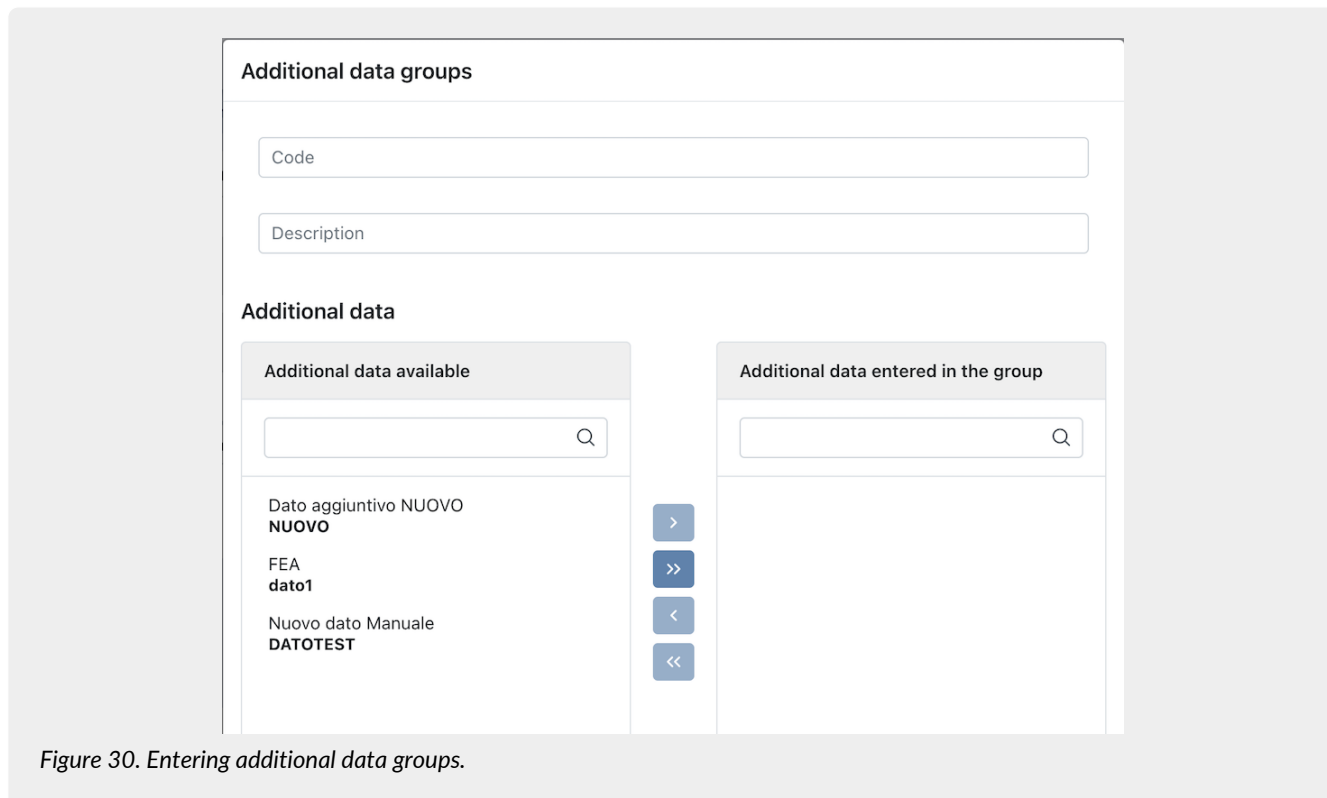






Figure 30. Entering additional data groups.

The code and description of the group can be entered in the upper section of the form.

The lower section is divided into two subsections: on the left side there is all additional data available to include in the group, on the right side there is all the additional data included in the group.

By selecting the desired additional data and by clicking on the buttons in the center of the two sections, data will move from

one section to another:

- : the selected additional data moves from the left section to the right one. It is included in the group;
- : all additional data move from the left section to the right one. They are included in the group;
- : the selected additional data moves from the right section to the left one. It is excluded from the group;
- : all additional data move from the right section to the left one. They are excluded from the group;

By clicking on the "Save" button, the new additional data group is saved and it is viewable in the list. By clicking on the "Close" button, the additional data group is not saved.

6.2. Signatures report

The number of signatures used with the eSIGN service has to be agreed commercially.

There are currently two types of consumption: single signatures or document signatures.

On the **Signatures report** page it is possible to monitor the consumption of the purchased signatures number.

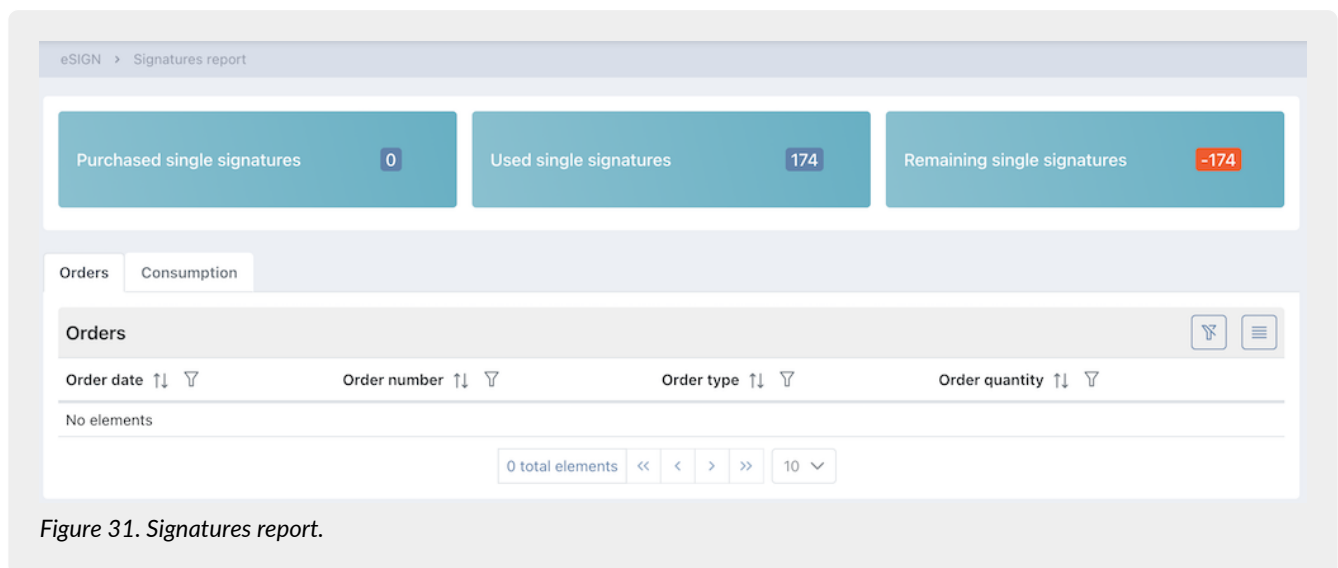


Figure 31. Signatures report.

The page is divided into two sections.

At the top, the first section shows the total consumption by signature type:

- the total number of signatures purchased through orders;
- the total number of signatures used in the various processes;
- the total number of remaining signatures (purchased signatures - used signatures)

The second section is divided into two parts:

- in the **Orders** section, all orders are listed with the quantity of the purchased signatures;
- in the **Consumption** section, all processes are listed, regardless of their status, with their consumption in the last column.

It is possible to sort the columns and filter the elements as described in the chapter [Console tables](#).



The consumption displayed is "real time". Also new processes are included in the count, and not only those started or concluded. So, the numerical indicators are updated simultaneously with the insertion of the processes and the definition of its signatures.

6.3. Signatory users

The first section, **Signatory users**, shows the list of all subjects previously entered in the system.

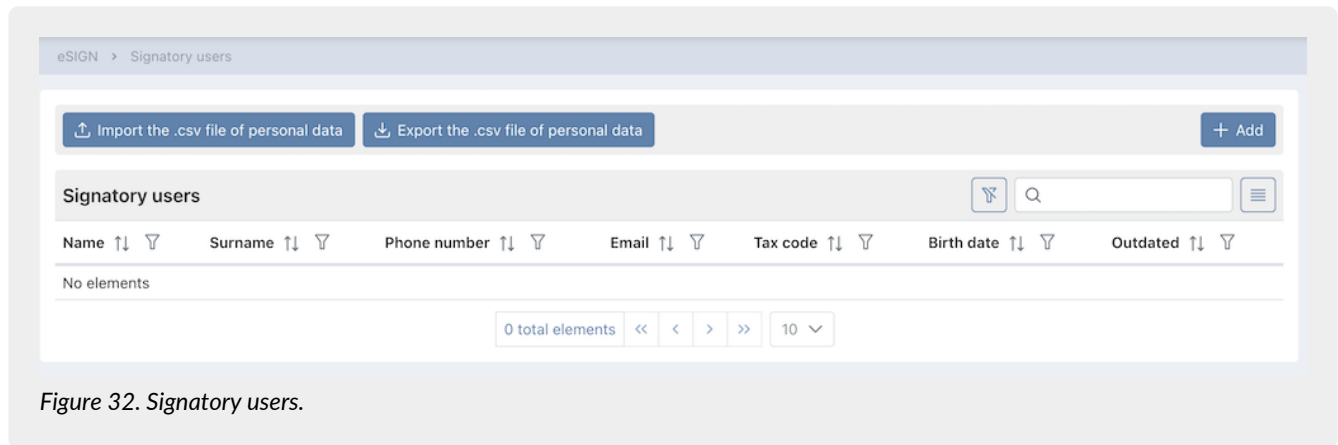



Figure 32. Signatory users.

The grid shows for each subject:

- **Name.**
- **Surname.**
- **Phone number.**
- **Email.**
- **Tax code.**
- **Birth date.**
- **Outdated:** it indicates whether the signatory user is obsolete ("Yes" value) or he is still active ("No" value).
- **Exportable:** it indicates whether the signatory user has been made exportable ("Yes" value) or not ("No" value). The column is not visible by default: it must be enabled by clicking the function button .

From this section it is possible:

- to order the columns and filter the elements as described in the [Console tables](#) chapter;
- to modify data entering in the detail page by clicking on the row;
- to add a new subject by clicking on the **"Add"** button and entering the required data.

By clicking on **"Export .csv file of personal data"**, it is possible to export the data in a CSV format. You can export all or part of the personal data, using the filters in the table. In addition to the personal data, in the exported file there are the additional data and the first attachment or document, too.

By clicking on **"Import .csv file of personal data"**, it is possible to import a CSV file to modify or to integrate the signatory users' personal data (see [Integration of personal data by file](#)).

6.3.1. Enter signatory users

On the **Signatory users** detail page it is possible to enter a new personal data or to modify a previously inserted one or to disable it (see [Management of outdated signatory user](#)).

In order to save a user, you have to enter the mandatory fields which are: name, surname, email, tax code.

If not entered and/or incorrect, the mandatory fields are in red after saving.

It is not possible to save until all mandatory fields are correctly entered.

There is also a uniqueness check on the tax code, telephone number and email: it is not possible to enter duplicate personal data with respect to this information.

In case you want (*exclusively in the case of template processes*) to exclude a signatory from the digital signature and send an email with the document attached for acknowledgment, check **"The signatory user is not enabled to use the digital signature"**.

In the event that the signatory user's identity documents have not been saved in the registry but are in the possession of the company, check the option "The identity document was acquired externally."

In case there is a need to "mark" a user as exportable directly from the registry without the aid of additional dedicated data or a personalized import procedure, check the option "The user is exportable".

After entering all the mandatory data, click on **Save**.

The entered data is correctly saved and inserted in the signatory users' list as described in the [Signatory users](#) paragraph.

After the user's first saving, other sections appear on the page. The personal data section has as its title the main references of

the user just entered (name, surname and tax code).



Figure 33. Signatory users entry detail.

6.3.2. Advanced Electronic Signature (AdES) agreement acceptance

In the "Advanced Electronic Signature (AdES) agreement acceptance" section, the agreement acceptance is sent to users.

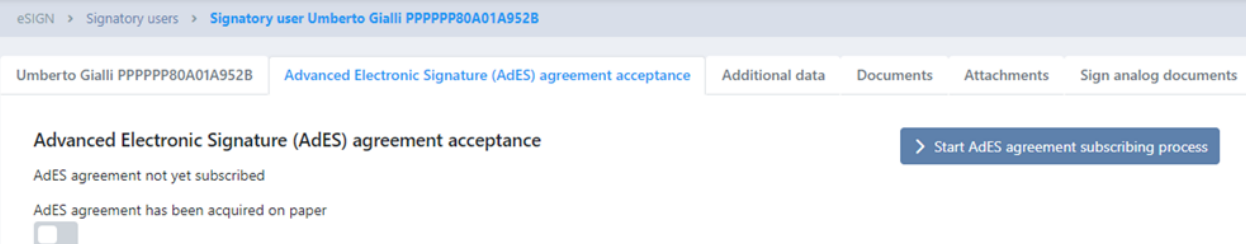


Figure 34. Advanced Electronic Signature (AdES) agreement acceptance.

If the AdES agreement acceptance has been made in paper form, it is necessary tick the relevant item. In this case, the request button will disappear.

To start the AdES agreement acceptance signing process click on the relative blue button. In order to start this process, it is essential to have previously entered into the system an AdES agreement acceptance signature template as described in the paragraph [Adding signature process template](#).

In the absence AdES agreement acceptance, the user **could not** affix an advanced electronic signature. So, he can only be included in processes with simple or digital signatures.

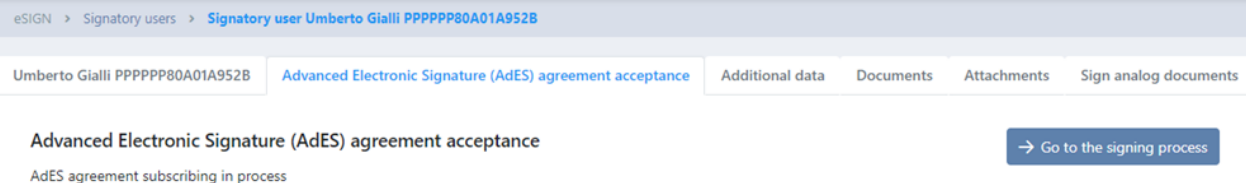


Figure 35. AdES signature process

After starting the subscription you can view the generated signature process by clicking on the "Go to the signing process" button: the detail page of the process will be opened. If the generated process is canceled, the "Start AdES agreement subscribing process" button will appear again. Once the AdES agreement acceptance process is completed, it is possible to revoke the acceptance by clicking on the "Revoke Acceptance" button: the revocation date information will be displayed on the left side, under the acceptance date information.

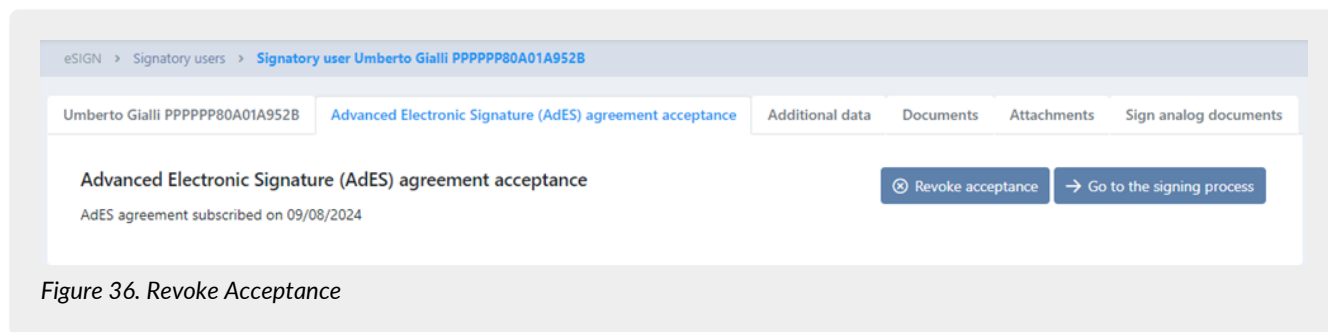


Figure 36. Revoke Acceptance

In case of a revoked acceptance, it is still possible to initiate another AdES agreement acceptance process for the signing user at any time.

By clicking the "Go to the signing process" button, you can view the details of the completed process for the first revoked acceptance.

By clicking the "Start AdES agreement subscribing process" button, you can start a second process to obtain another AdES acceptance.

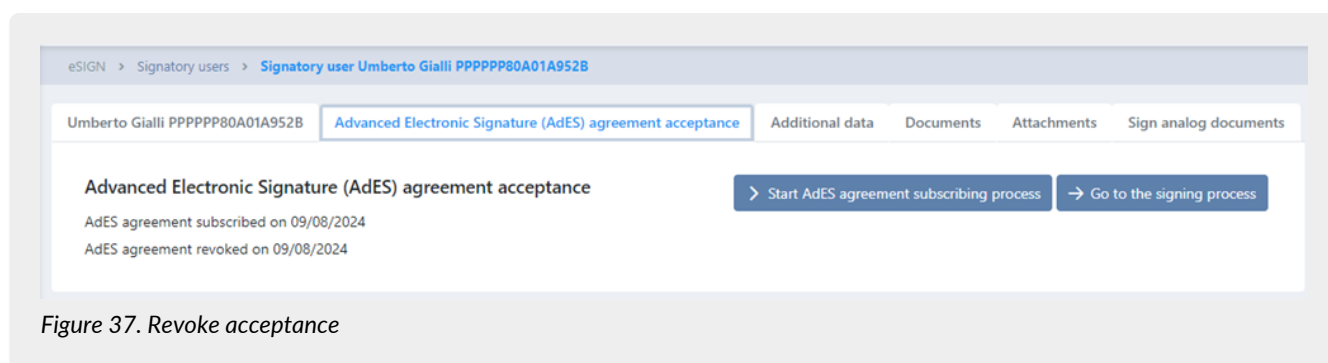


Figure 37. Revoke acceptance

If the process started for AdES agreement acceptance is rejected by the signatory user, the information will be displayed on the left side of the page. By clicking the "Go to the signing process" button, the details of the rejected process will be shown.

In this case, it is not possible to restart the AdES agreement acceptance from this page; the rejected process must be restarted. (see. [Restarting a rejected signature process](#))

6.3.3. Additional data

In the "Additional data" section, it is possible to enter the additional data values for the automatic valorisation of the templates linked to the signatory user (see paragraph [Markers](#)).

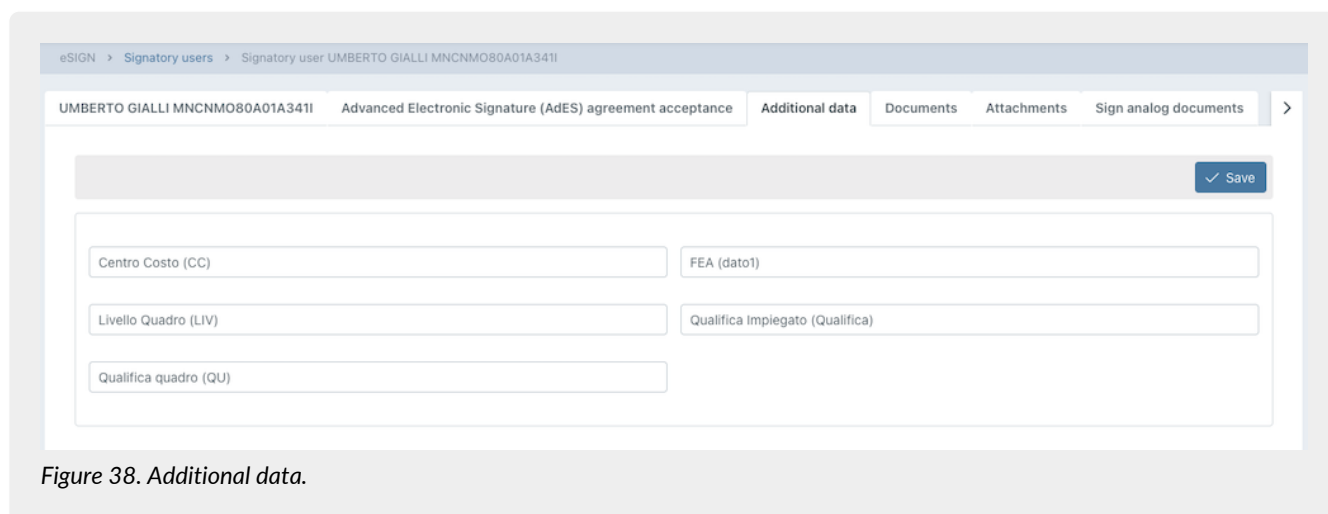


Figure 38. Additional data.

The additional data listed is strictly bound to the segregation defined in the definition of the user's role (see [Access management](#)). You can view and manage only the additional data you are enabled.

To fill a value to an additional data, simply enter the value in the field and click the **"Save"** button at the top right. During saving, a consistency check is carried out on the value entered and the additional data definition (see [Additional data](#)). If the value entered does not comply, the field will be highlighted in red and saving is inhibited.

6.3.4. Identity documents and attachments

In the **"Documents"** section, it is possible to enter the identity documents data and to attach a scan of the document.

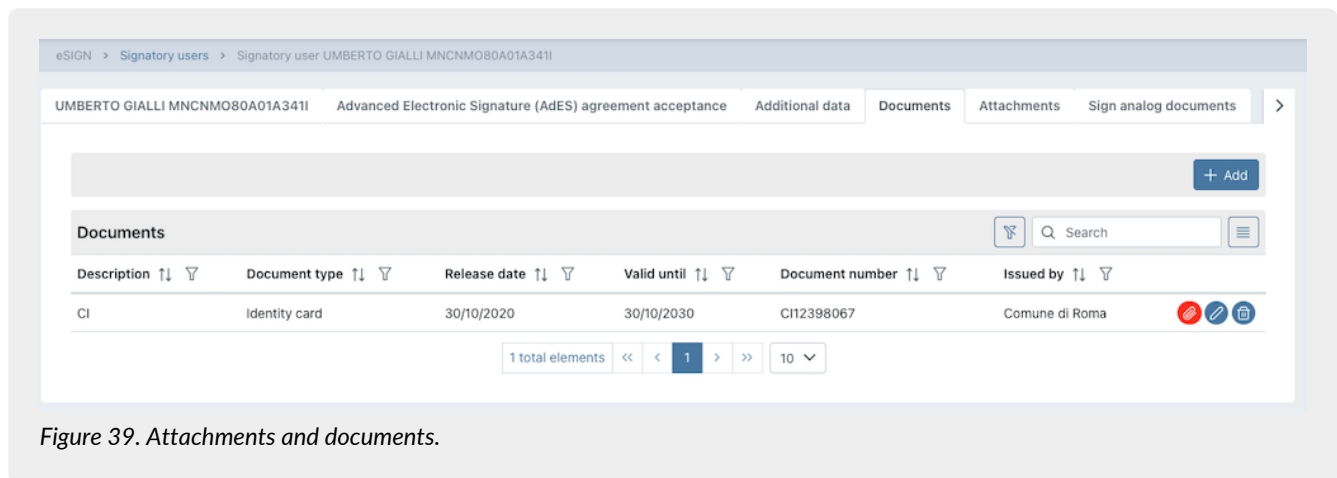







Figure 39. Attachments and documents.

By clicking on the **"Add"** button, it is possible to enter the data of the identity document, specifying the type, number, issue date and validity date. Furthermore, by clicking on the **"Select identity document scan"** button, it is possible to attach a document scan.

From the identity documents list it is possible:

- to order the columns and filter the elements as described in the [Console tables](#) chapter;
- to view document status. If a document is uploaded there is  icon, otherwise there is  icon on the row;
- to modify the document by clicking  on the row;
- to delete the document by clicking  on the row.
- by clicking on the icon , the upload form will open, where, in addition to modifying the previously entered data, user can:
 - to upload a document, if it was not previously uploaded, by clicking the button at the bottom left **"Select Identity Document Scan"**;
 - download the previously uploaded document by clicking the button at the bottom left with the file name;
 - to modify the previously uploaded document by clicking the icon and proceed with another upload or save without attaching any documents.

In the **"Attachments"** section, it is possible to attach different documents from the previous ones.

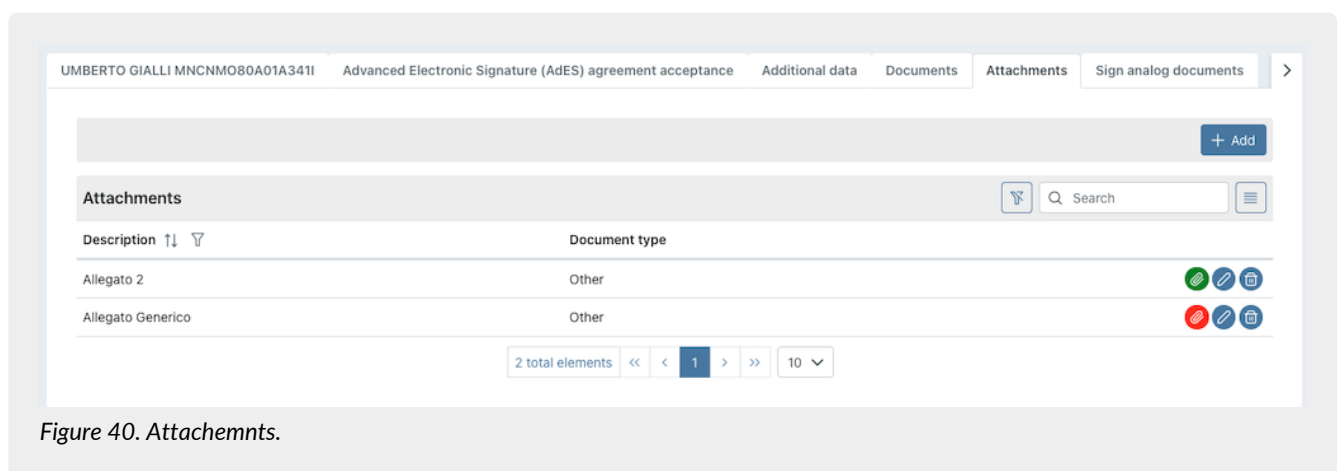






Figure 40. Attachemnts.

By clicking on the **"Add"** button, it is possible to enter a new attachment entering its description and by clicking on the **"Select"** button, it is possible to attach the document scan.

From the list of the attachments it is possible:

- to order the columns and filter the elements as described in the [Console tables](#) chapter;
- to view document status. If a document is uploaded there is  icon, otherwise there is  icon on the row;
- to modify the document by clicking  on the row;
- to delete the document by clicking  on the row.

6.3.5. Signing of analog documents and remote certificates

In case you also use the "eCON LUL", "eLUL", "eNSP", "eAMB" o "ePLUS" services, in the "Sign analog documents" section it is possible to enable an user to sign analog documents simply ticking the relevant item.

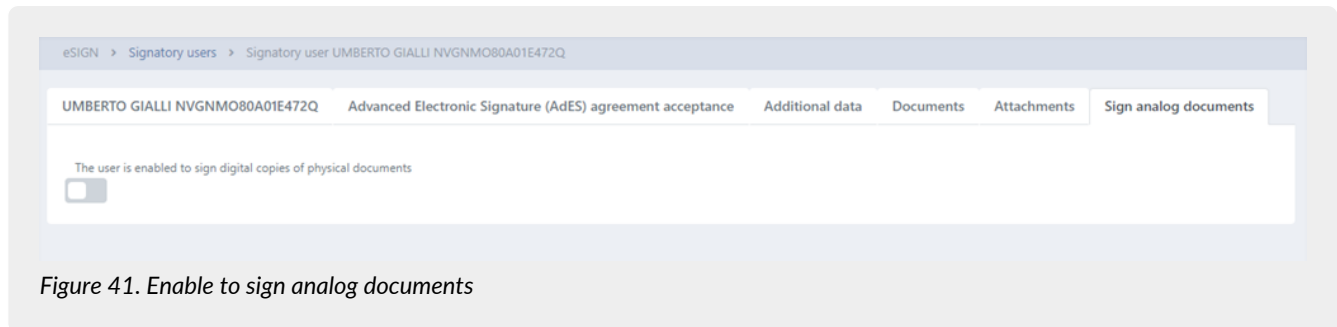


Figure 41. Enable to sign analog documents

The user with this ability can digitally sign analog documents through the eSIGN Desktop application. It will be possible to return to the page of the list of signatory users through the navigation path placed in the top left by clicking on the "Signatory Users" item. In the event that a signatory user is enabled to sign analog documents, the company can request remote certificates from Entaksi in his name.

Once the remote certificates are enabled, the analog documents will be signed automatically: it will no longer be necessary to have a signature device and install eSIGN Desktop. When uploaded the analog documents will be automatically signed (without any notification emails) and then paid into storage. The "Remote Certificates" section lists all the certificates registered to signatory user.

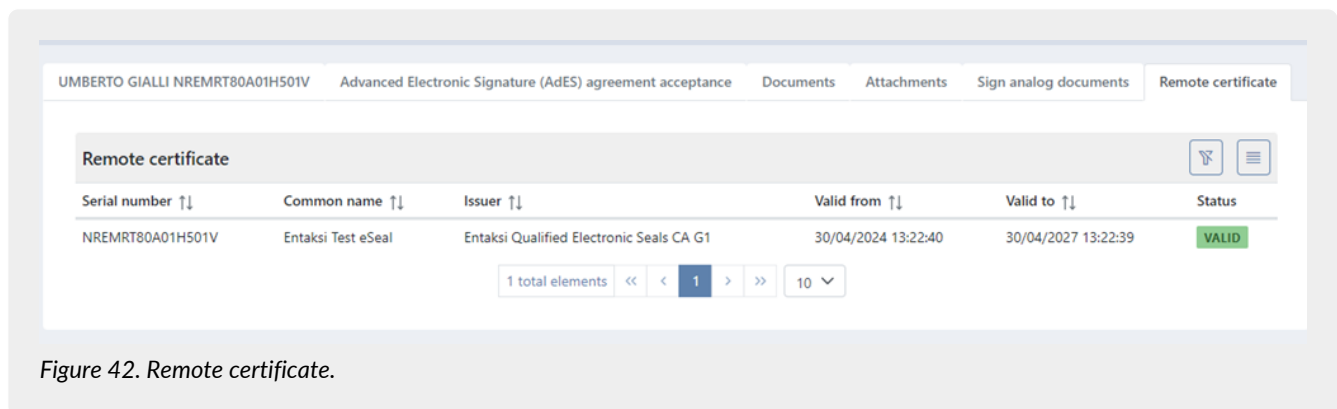


Figure 42. Remote certificate.

The information provided is:

- **Serial number:** certificate serial number;
- **Name:** name given to the certificate;
- **Issuer:** Issuer of the certificate;
- **Start Date:** the start date of the certificate's validity;
- **End Date:** the end date of the certificate's validity;
- **Status:** the status of the certificate.

6.3.6. Management of outdated signatory user


In eSIGN service, it is possible to make an user outdated, but it isn't possible to delete him. In order to make an user no longer usable, you have to enter a deactivation date in the "Configurations" section in the user personal data page.

In case the user is a signer in uncompleted processes, he can't be outdated. In order to make the user obsolete, you have to

exclude him from the process or to delete the process itself.

When the user is outdated, you can not:

- send AdES agreement acceptance, insert additional data and attachments and documents: the three sections are no longer visible;
- insert the user in a signatory group. In case the outdated user is present in a previously added group, it is not necessary to modify the group: no signing requests are sent to the outdated user;
- insert the user in a new signing process;
- insert a notify to the user in a new signing process.

Outdated users can be easily identifiable thanks to the "Yes" value within the list of signatory users in the "Outdated" column and the deactivation icon , shown at the top of the user personal data page.

If you want to re-enable the signatory user at a later time, cancel the deactivation date and save.

6.3.7. Integration of personal data by file

If you want to enter personal data in bulk or to make massive changes to already registered signatory users (such as inserting or change a value of an additional data), "Import CSV file" function is particularly useful.

To import a file in CSV format, click on the "Import .csv file of personal data" button in the "Signatory users" page and upload it from the file upload form.



The screenshot shows a web form with a title bar that says "Select a CSV file containing signatories' data". Below the title bar is a large white area. In the top left of this area is a blue button with an upward arrow icon and the text "Select file". In the bottom right corner of the white area are two blue buttons: one with a checkmark icon and the text "Save", and another with an 'X' icon and the text "Close".

Figure 43. File upload form.

By clicking on "Select file", you can select the CSV file to upload. By clicking on "Close", the upload is canceled; while clicking on "Save" the upload is confirmed.

If the tax code in the csv file is already present in the database, the import procedure **overwrites** the data previously recorded. If the tax code in the csv file is not present in the database, the import procedure **inserts** the data.

The upload result is displayed in the central part of the form. In the form are displayed the total number of lines processed, the total number of master data that have been updated or inserted and the number of rows that have problems that have produced neither insertions nor updates.

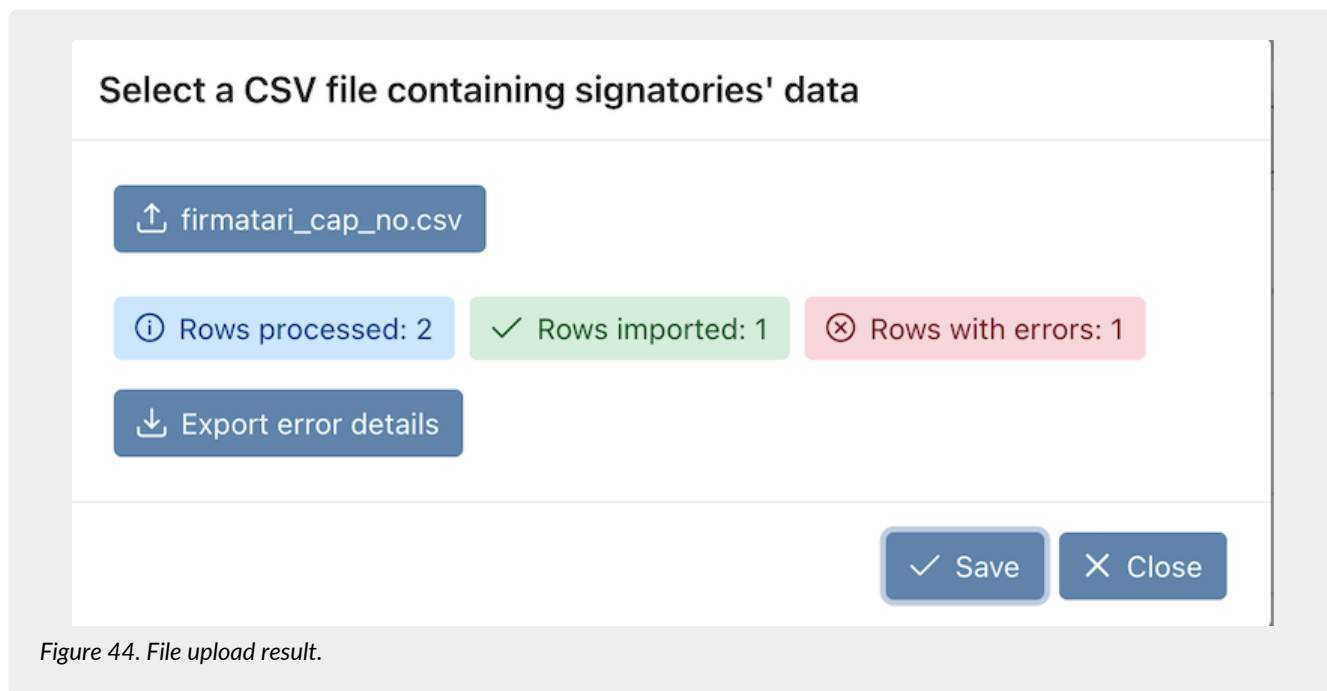


Figure 44. File upload result.

By clicking on **"Export error details"**, a file is downloaded. In this file you can find all anomalies and the reason of the rejection. By clicking on the **"Close"** button you return to the section of signatory users. All changes or entries of the personal data are visible.

Below are the rules for the correct construction of the CSV file.

The CSV file must have:

- the master data or additional data fields name as column headers;
- the values to be entered or modified in the registry as rows ;
- as separator the semicolon character (;);
- as string delimiter the double quote character (").

In order to make a correct file, in the table below you can find the names of the heading columns, the relative descriptions and if it is mandatory.

Field Name	Description	Mandatory
email	email of the signatory user.	YES
phone	Phone number of the signatory user.	NO
first_name	Name of the signatory user.	YES
last_name	Surname of the signatory user.	YES
tax_code	Tax code of the signatory user.	YES
birth_date	Birth date of the signatory user.	NO
address	Address of the signatory user.	NO
postal_code	Residence postal code of the signatory user.	NO
city	Residence city of the signatory user.	NO

Field Name	Description	Mandatory
province	Residence province of the signatory user.	NO
country	Residence country of the signatory user.	NO
birth_city	Birth city of the signatory user.	NO
birth_province	Birth province of the signatory user.	NO
birth_country	Birth country of the signatory user.	NO
obsolete_from	Date from which the user is considered obsolete. If the user is active, this field will be empty	NO
not_have_digital_signature	It can have the values <i>true</i> or <i>false</i> and determines "The signatory user is not enabled to use the digital signature" option in the "Configurations" section of the signatory's registry.	NO
identity_document_acquired_outside	It can have the values <i>true</i> or <i>false</i> and sets the "The identity document has been acquired externally" option in the "Configurations" section of the signatory's registry.	NO
exportable	It can have the values <i>true</i> or <i>false</i> and sets the "User is exportable" option in the "Configurations" section of the signatory's registry.	NO
identity_document_type	Identity document type. The possible values are: Carta d'identità (Identity card); Passaporto (Passport); Patente di guida (Driver's license); Patente nautica (Boat license); Libretto di pensione (Pension certificate); Porto d'armi (Firearms license); Altro (Other).	NO
identity_document_number	Identity document number.	NO. It becomes mandatory if a value has been entered in the field <code>identity_document_type</code>
identity_document_released_from	Identity document issuing body.	NO. It becomes mandatory if a value has been entered in the field <code>identity_document_type</code>
identity_document_release_date	Identity document issuing date.	NO. It becomes mandatory if a value has been entered in the field <code>identity_document_type</code>

Field Name	Description	Mandatory
identity_document_validity_end_date	Identity document validity end date.	NO. It becomes mandatory if a value has been entered in the field identity_document_type

In order to insert or modify additional data, you have to append a column to the previously listed columns for each additional data you want to manage.

The name of the field has to correspond to the code of the "Key" field in the additional data (see [Additional data](#)) and its valorisation is **not** mandatory. In case of valorisation, however, the import procedure performs a consistency check between the entered value and the type and rules defined in the additional data (see [Additional data](#)). In case of inconsistencies, the import will be stopped.

Entering the additional data by .csv file is closely related to the configuration of the role and the enabling of visibility as explained in [Access management](#) paragraph.

In fact, you can import files containing additional data for which you are enabled. **Exclusively** a user without any restrictions can insert new additional data by simply appending new columns.

For example, if you want to add the additional data *CentroCosto* and *Level* to the master data, you have to append two new columns named "CentroCosto" and "Level" to the previously listed columns and to valorise them.



The additional data column name should **not** contain special characters and spaces.

If you simply want to massively modify previously saved data, just download the CSV by clicking "**Export .csv file of personal data**" as described in the [Signatory users](#) paragraph and manually modify values.

Furthermore, it is also possible to "combine" the modification of the personal data with the insertion of new ones.

In this case, you have to download the CSV file, to make changes in the existing rows and add new rows. The added rows are the new signatory users inserted.

6.4. Signatory groups

In the **Signatory groups** section, signatory groups are listed.

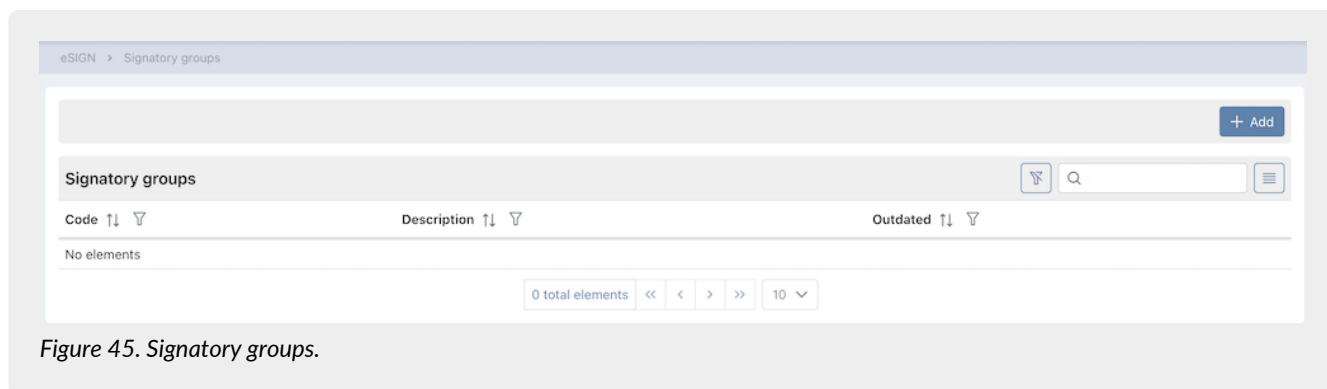


Figure 45. Signatory groups.

Below there is a brief description of the items and filters on the list.

- **Code:** it is the group code assigned during insertion.
- **Description:** it is the description of the group assigned during insertion.
- **Outdated:** it indicates whether the group is obsolete ("Yes" value) or is still active (value "No").

From this section you can:

- order the columns and filter the elements as described in the [Console tables](#) chapter;
- modify the group by clicking on the row;
- add a new group by clicking on "**Add**" button and entering the mandatory data.

6.4.1. Entering signatory groups

In the **Signatory groups** section, a list displays a previously signatory user groups added and there are identified by a code and a description.

In eSIGN service, it is also possible to make a group outdated (no longer usable) entering a deactivation date (see [\[Management of outdated signatory groups\]](#)).

Although both fields are free text, in order to facilitate the use of the system and the possible searches, it is suggested to enter values that are clear and easy to find.

Figure 46. Signatory group detail.

By clicking on "Save" a new group is created with the entered data and an additional section the "Signatory users of the group" will appear, in which are displayed all active signatory users belonging to the group (with the obsolete column filter selected) and where user can include or exclude signatory users from the group.


Figure 47. Signatory users of the group.

The following is a brief description of the fields in the grid:


- **Name:** name of the signatory user registered in the registry.
- **Surname:** surname of the signatory user registered in the registry.
- **Date of birth:** date of birth of the signatory user registered in the registry.
- **Telephone:** telephone of the signatory user registered in the registry.

- **Email:** email of the signatory user registered in the registry.
- **Tax code:** tax code of the signatory user registered in the registry.
- **Obsolete:** indicates whether the signatory user has been made obsolete ("Yes" value) or if it is still active (default value "No").

From this section user can:

- sort columns and filter items in the table as described in the chapter [Console tables](#) ;
- add one or more signatory users to the group by clicking the "Add" button located at the top right;
- remove one or more signatory users from the group;
- access the details of the signatory user's profile directly by clicking on the icon in line  to any changes.

Remove one or more users from the group

Signatory users in the group can be removed individually by clicking the icon  in the row, or by selecting one or more users and clicking on the "Remove selected" button located at the top left.

Specifically, with the following buttons:

- **Select visible:** to select only the signatory users on the current page.
- **Deselect visible:** to deselect only the previously selected signatory users on the current page.
- **Clear all:** to deselect all previously selected signatory users, regardless of the page.
- **Remove selected:** to remove the selected signatory users from the group.

Add one or more signatory users to the group

To add new signatory user to the group, click on the "Add" button at the top right: a list of all available active (non-obsolete) signatory users who are not yet part of the group will be displayed.

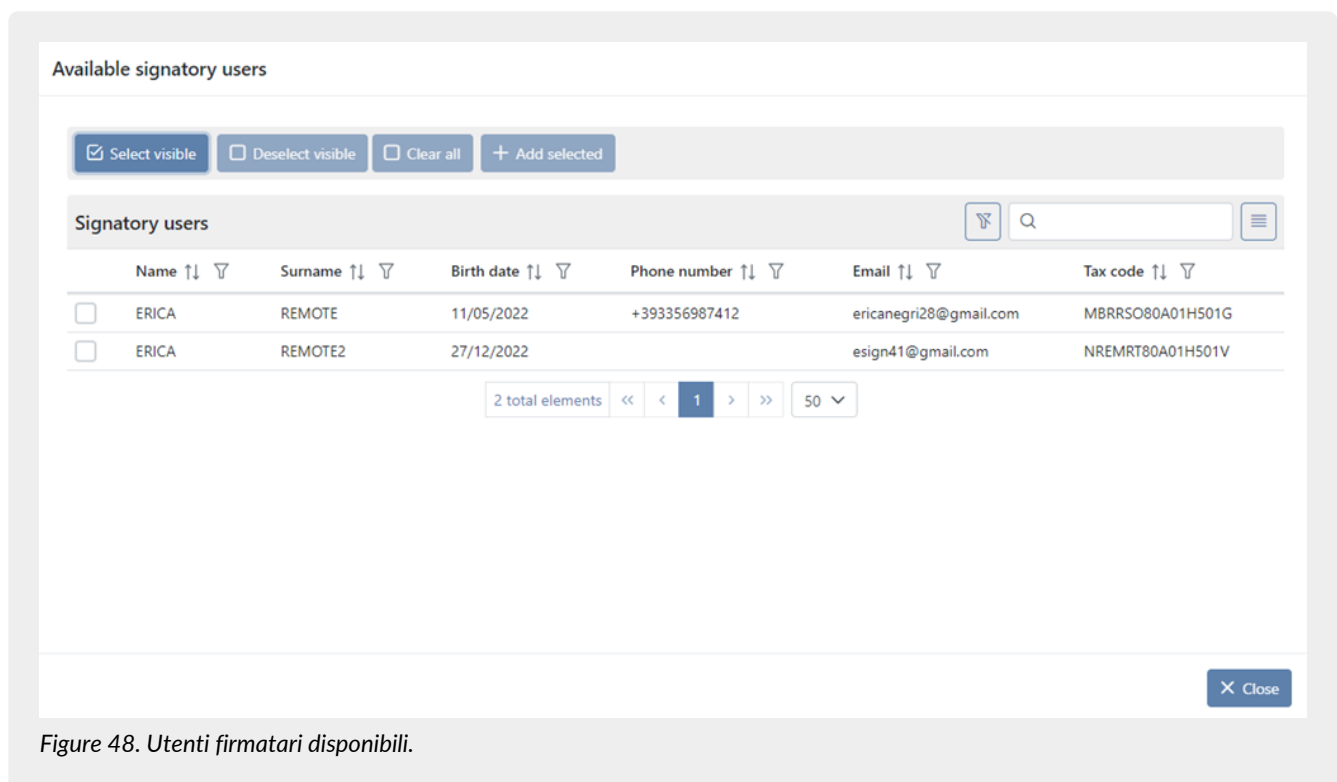


Figure 48. Utenti firmatari disponibili.

To add new signatory users, select the desired ones from the list and then click the "Add Selected" button.

Selection can be made individually or in a mass manner by clicking the "Select Visible" button: **only** the signatory users on the current page will be selected.

With the "Deselect Visible" button, the signatory users on the current page will be deselected, while the "Clear All" button will deselect all signatory regardless of the displayed page.


Clicking the "Close" button at the bottom right will close the list of available signatory users.

6.4.2. Management of outdated signatory groups

In eSIGN it is possible to make a signatory group outdated (no longer usable), inserting a deactivation date in the "Configurations" section on the group detail page.

In case there are unfinished processes (in "waiting for signature" status or new ones) within a group as signer, it can't be outdated.

From the deactivation date, it is not possible to change the signatory users within the group (the section is no longer visible). The group is not visible within the signatory groups in new processes, too.

Outdated groups can be easily identifiable thanks to the "Yes" value within the list of signatory groups in the "Outdated" column and the deactivation icon , shown at the top of the group registry.

If you want to re-enable the signatory group later, just delete the deactivation date and save.

6.5. Signing process

The **Signing process** page contains a list of all processes created by eSIGN.

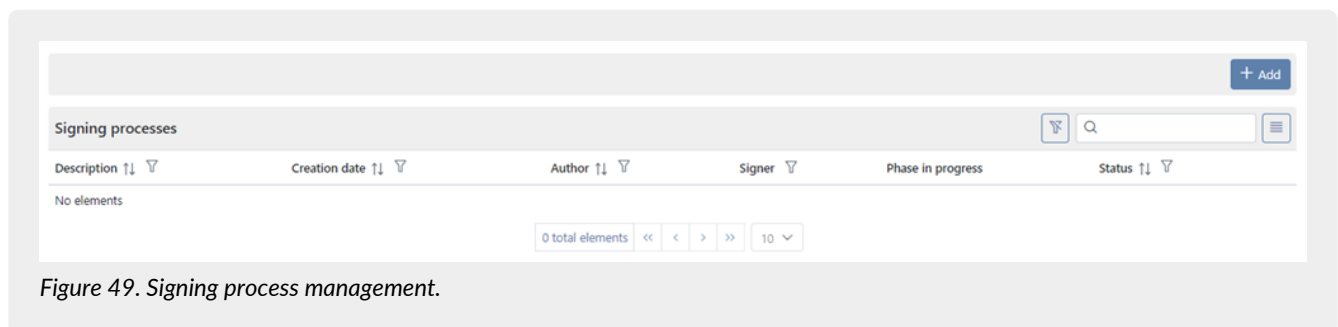


Figure 49. Signing process management.

Below there is a brief description of the items and filters on the list.

- **Description:** it is the description of the signing process that is entered during its creation.
- **Creation date:** it is the date the signature process is created.
- **Author:** it is the name of the person who creates the signing process.
- **Signer:** it shows the names of the signatory (users or groups) of the documents in the signing process.
- **Status:** it indicates the progress of the signing process.

From this section it is possible:

- to sort the columns and to filter the elements in the table as described in [Console tables](#);
- to enter the detail page by clicking on the single row. In case the process is in "New" status, you can modify the previously loaded data. For all the others status types, you can't edit the data that is read-only as descriptive information about the process;
- to insert new signing processes by clicking on "Add";
- to delete a process by clicking on [040 eSIGN Elimina.png] icon. You can delete only new processes or processes in "waiting" status without signed documents.

The table below shows the statuses available during the signature workflow:

Value	Description
CREATED	The process is created but not started. In this state it is still possible to make any changes to the process or to delete it.
CONFIRMED	The process is confirmed and the system starts the signing workflow: the system sends signing request emails.
WAITING FOR SIGNATURE	One or more signing requests are delivered, but the signing process is not finished yet.

Value	Description
COMPLETED	The signing process is completed: all signatures are placed on the document.
REJECTED	This message indicates that the process is not completed because it has a phase whose signature was rejected by the signing user. However, a rejected process can always be restarted at a later time.

Not all processes may be visible to all users. Their visibility depends on both the role attributed to the user and by the segregation of additional data (see [Access management](#)).

6.5.1. Signing process detail

From the "Signing process" page, by clicking on a process in "Waiting for signature", "Completed" or "Rejected" status, it is possible to enter the **Signing process detail** page.

Processo Demo

Author: Carlo Rossi | Creation date: 22/10/2024 12:34:32 | Start process date: 22/10/2024 12:38:40 | Consumption: 1 Single signature

Workflow status: **COMPLETED**

Document	Signer	Phase	Signature	Signature field	Date of signature	Signature status
DocumentoDemo.pdf	Bianchi Umberto (QDSSDR80A01H501Z)	Fase2	firma2	Field Firma2 at page 1	22/10/2024 12:38:30	CANCELLED
DocumentoDemo.pdf	Rossi Umberto (NGRRCE75E42F032K)	Fase1	firma1	Field Firma1 at page 1	22/10/2024 12:38:30	COMPLETED

2 total elements | << < 1 > >> 10

Figure 50. Signing process detail.

In the top section, main information about the process is shown: the process signature description, the author, the creation and start date of the process, the status, the consumption, and, only in the case of a rejected process, the reject reason.

In the section below, all the documents and the related signatories are listed.


Below is a brief description of the list columns you can sort or filter as described in [Console tables](#) paragraph.


- **Document:** it contains the name of the document to be signed. If the document has several required signatures, it is listed more times. In this case, in the following columns, the single signatory and the related signatures are shown.
- **Signer:** it contains the signatory user name.
- **Phase:** it contains the value inserted in the "Phase description" during the creation of the process.
- **Signature:** it contains the value inserted in the "Signature description" during the creation of the process.
- **Signature field:** it contains name of the signature field entered in the document to be signed.
- **Signature status:** descriptive field with double icon. Starting from the left, the first icon indicates the type of signature required or affixed (you can view the full description through a descriptive tooltip); the second icon indicates the progress of the signature. The states are listed below.

- **Information icons:**

The "forward" icon () appears both in case the process is in "To be processed" and in "Completed" status. By clicking on it: in case of "To be processed" status a new request email is sent to the signatory user; in case of "Completed" status a new notification email with the signed document is sent to the signatory (see paragraph [Company configurations](#)).

The "delete" icon () appears only if the process is in "To be processed" status. By clicking on it, the signature request is cancelled. The signature status changes from "To be processed" into "Canceled" and the process will be complete when the remaining signatures are affixed.

The "information" icon () appears only in completed processes. By clicking on it, a form opens where there are further details about the signature such as: the method of affixing the signature (by app or OTP code), any information concerning the OTP code and its sending (via email or SMS), any information concerning the app and the device used. the hash of the OTP code, the number of the mobile phone, etc.

The "attachments" icon () appears in completed processes and only if signers have attached documents during the signing process ([Signature pages](#)). By clicking on it, a form opens where all the attached documents are listed. You can download the attached document by clicking on the relative icon placed in line.

The table below shows the various statuses that signatures can assume during the signature process workflow.

Value	Description
TO BE PROCESSED	The document is sent to the signer, but the required signature has not been on purpose.
SIGNING	This state can occur in the case of a digital signature. The document is sent to the signatory and the signature is being affixed, but not completed. If during the digital signature, after confirming the OTP, the eSIGN Desktop signature application is disconnected from eSIGN (for example for closure of the program or for removal of the signature device), the affixing procedure signature is started but not finished. In this case you will have to start the application again, to connect it to eSIGN and to perform the signing procedure again.
COMPLETED	The document is correctly signed.
ERROR	This status indicates that the signature has an error.
CANCELLED	This status indicates that the signature requested has been canceled. The process will complete when all remaining signatures are affixed.
REJECTED	This status indicates that the requested signature is rejected by the signing user. The entire process will be in "Rejected" status, but it may be possible to start it later.

The "**Delete process**" appears only for processes in "Waiting for Signature" status. By clicking on it, you can delete the process.

By clicking on the "**Restart process**" button, the rejected process restarts (see [Restarting a rejected signature process](#) for more details).

By clicking on a single row, another detail page is displayed.

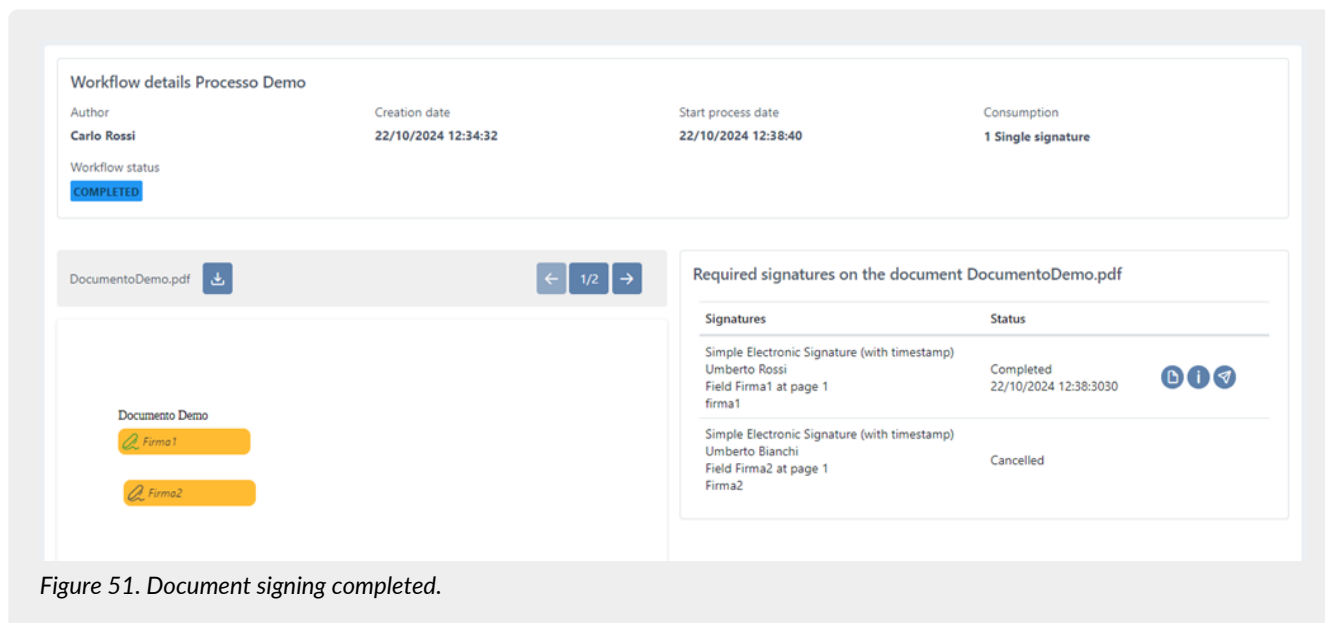


Figure 51. Document signing completed.

At the top of the page, general information about the process is shown.

The part below is divided into two sections that show all information about the document.

Only if all the signature in the document are affixed, in the left section there is the signed document and you can also download it.

In the right section, information about the document signature is shown:

- The **"Signatures"** column shows the data of the signature:
 - the type of signature;
 - the signing user;
 - the name of the signature field;
 - the signature field location page;
 - the description of the signature entered in the "Signature description" field.
- The **"Status"** column shows the data of the signature status:
 - whether the signing is in progress or completed (the process is completed);
 - date and time of signing, in case the process is completed.
- The last column shows the information icons whose functions are equal to those previously described.

It will be possible to return to the previous pages using the breadcrumb. By clicking on the "Signature processes" item, you return to the main page with the list of signature processes; by clicking on the item "Details of the signature process" you return to the detail page of the signing process.

6.5.2. Adding a signature process

By clicking on the **"Add"** button in the **Signature processes** page, you can add a new process. The entry page is divided into two sections:

- in the left section (**"Documents to be signed"**), you can upload all documents to be signed;
- in the right section (**"Signature process definition"**), you can define the signing workflow.

Figure 52. Adding signature process.


In "Documents to be signed" section, you can upload documents by clicking on the upload button : a file upload management form opens.

Figure 53. File upload management form.

If you request it, "**PDF models**" function can be enabled in order to automatically recognize signatories.

This function is optional, so the list at the top of the selection is not visible for companies without configured models: you can upload directly your documents.

If you have configured models, you can upload directly documents without referring to a specific model: just not select anything from the list and continue with the upload. On the other hand, if you want to upload a document referring to a specific model, select the model in the list and upload the related document. If the file is not conform to the selected model, the system displays an error and prevents the upload. Since it is an automatic signature recognition feature, each signatory must be recorded in the registry of signatory users in eSIGN. If a signatory user is not recorded, the file is not loaded and an error icon appears with the related message.

By clicking on **Select file**, an explorer window opens and you can choose files to upload which are visible in the central list. Only PDF format files can be uploaded.



If there are special characters in the file name (for example "ù", "à", etc.), it is recommended to rename the file by removing these characters, otherwise the system automatically removes them when the file is acquired.

By clicking on  the file is removed and it is not uploaded.




The **Load documents** is enabled only if there are files in the list. By clicking on it, the system uploads all files in the list. If there are no errors there is a green check, otherwise there is an error icon (a triangle with an exclamation mark). The files with errors are not loaded into the system.

By clicking on **Close** the form closes.

If you click the close button without having loaded documents, they are not uploaded in the system.






When one or more files are loaded, a list with their names appears.

By selecting a single file from the list, you can view its content in the section below and you can:

- scroll the pages if the file has more than one page;
- delete the file by clicking the button . You can upload another file and continue with the management;
- reduce the file size by clicking the button  to enlarge the management section of the page. By clicking again on the file it returns to its original size.
- rename the file, it is possible by clicking the button , entering the new file name in the proposed form, and clicking the "Save" button located at the bottom right

In the **Signature process definition** section, you have to define the process and its workflow.

In this section you have to enter the following values:

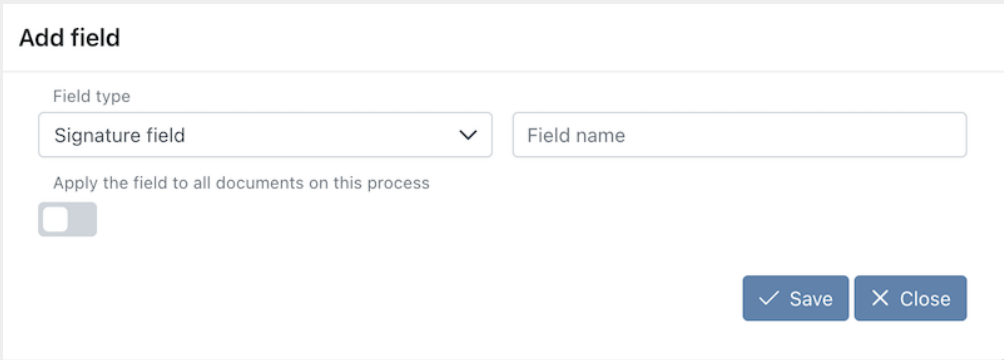
- **Signing process description:** it is a mandatory field. It defines the signing process and it is recognizable from this description. The description is also reported in the signature processes list. For this reason, in order to facilitate future sorts and searches, it is advisable to enter a name that contains the minimum data to be recalled later.
- **Signature template:** it isn't a mandatory field. In case templates have been previously inserted (see paragraph [Adding signature process template](#)) and you want to define the process starting from one of these, click on the list. In this list there are all the templates previously inserted, and you can search them by description.
If templates contain additional data, you can view **exclusively** the templates containing the additional data for which you are enabled (see [Access management](#)).
By selecting the template, all the fields of the signature phases and the documents defined in it are automatically loaded. In this way, the process is already created and you just have to insert the signatories. If you want, you can modify it.
In case there is an empty .pdf file in the template, before starting the process it is necessary to upload a .pdf document to replace the empty one, by clicking the  icon.
It is not permitted to start a process with an empty or non-replaced .pdf file.
In the case of .odt or docx extension files, since the editable and the signature fields were previously defined within the file itself, they **cannot be** modified, deleted, moved and it is not possible to insert new fields.
However, in the case of .pdf files, the editable and signature fields **can be** modified, deleted and moved and, if necessary, it is possible to insert new fields simply by clicking on the file itself. However fields can **only** be moved on the same page: moving between pages is not allowed. To move a field from one page to another, you need to: delete the field, move to the desired page (with the arrows located at the top right next to the document), click on the page and create the new field.
- **Fill out the form:** is the button for filling out the form containing the parameters to be populated and is located at the top right next to the label "Signature process definition": it is visible only when creating a signing process from a template containing parameter-type markers (see [Markers](#) and [Process template](#)).
Clicking this button will open a form containing all the parameter-type markers defined in the template, where they can be populated. By clicking the "Save" button, the entered data will be saved, and the document will be customized; however, by clicking the "Close" button, the entered values will not be saved.
If mandatory parameters are defined in the template, the button displayed will be : it will not be possible to start the process without having previously populated the mandatory parameters.
If no mandatory parameters were defined during the template creation, the displayed button will be  and the process can be started even without populating the parameters.
If parameters have been populated and the changes have been saved, the displayed button will be .
- **Document type:** It is the type of document, selected from a list of predefined ones, through which the minimum and standard metadata is automatically set for the correct SIP automatic compilation by ePLUS service.
- **Classification:** it is the classification scheme. This section is present only if an active classification scheme data has been defined in the company and if the author of the process is authorized to select the classification. (see [Classification scheme](#)). By clicking on  the button, you can select the classification of the documents to be signed. The standard metadata for the classification scheme are automatically set to submit the SIP and to preserve documents in eDOC.
- **Signature fields.**
- **Editable fields.**
- **Signing phases.**

Signature fields and Editable fields

By **Signature Fields** we mean those fields used for electronic signature. They are mandatory fields.

By **Editable fields** we mean the fields that will enter by the signatory user when he signs the document. They are not mandatory fields.

To insert both the signature fields and the editable fields on the document, it is necessary to click on it in the position where you want to insert the relative field. The system proposes a form in which you have to define the field.



Add field

Field type
Signature field ▼

Field name

Apply the field to all documents on this process
☐

✓ Save ✕ Close

Figure 54. Entering document fields.

As a first step you have to choose the type of field you want to insert. The insertion options are displayed. By default the system proposes the "Signature field" as field type.

It is possible to configure the height and width of editable fields or additional data in both signature templates than in manual processes.

Unless otherwise specified, the standard field measures 20 px in height and 100 px in width, while the minimum values and maximum attributable values, always expressed in pixels, are the following:

- Height: minimum 20, maximum 250;
- Width: minimum 200, maximum 600

If a text field is assigned a height greater than 20 px, during the signature process, the field will automatically be defined as a text area. This means that any text formatting entered by the signatory user, such as a new line, will be reflected in the signed document.

If not inserted mandatory options are highlighted in red in saving phase.

The table below shows the options for each field type.

Field type	Description	Options
Signature field	Signature field.	Field name: name of the signature field you are entering.


Field type	Description	Options
Text field	Text type field. The imputable characters will be free, respecting, however, the length maximum and/or minimum if entered.	<p>Field name: name of the field you are entering;</p> <p>Description: description of the field you are entering. It appears in the form in the signing phase;</p> <p>Mandatory: if checked, the field is mandatory in the signing phase;</p> <p>Field min length: it is the minimum length of the field;</p> <p>Field max length: it is the maximum length of the field;</p> <p>Validation pattern: it is the validation criterion that you want to adopt to verify the correctness of the entered text by the signer. Since validation patterns have a complicated and non-standard construct, please search online the correct string according to your needs and check it on the site regex101.com.</p>
Numeric field	When signing, signatory can only enter a numerical value with or without the decimal digits.	<p>Field name: name of the field you are entering;</p> <p>Description: description of the field you are entering. It appears in the form in the signing phase;</p> <p>Mandatory: if checked, the field is mandatory in the signing phase;</p> <p>Digits: they are the decimal digits of the numeric field.</p>
Date field	Date type field.	<p>Field name: name of the field you are entering;</p> <p>Description: description of the field you are entering. It appears in the form in the signing phase;</p> <p>Mandatory: if checked, the field is mandatory in the signing phase.</p>
Date-time field	Date-time type field.	<p>Field name: name of the field you are entering;</p> <p>Description: description of the field you are entering. It appears in the form in the signing phase;</p> <p>Mandatory: if checked, the field is mandatory in the signing phase.</p>

Field type	Description	Options
Values list field	It is a list type field. The values in the list are configurable in the options.	Field name: name of the field you are entering; Description: description of the field you are entering. It appears in the form in the signing phase; Mandatory: if checked, the field is mandatory in the signing phase; Values list: it is the list of values that can be chosen during the signing phase. List values must be entered with the following construct: Value1#Value2#Value3#.
Yes/NO field	Tick type field that can be selected or not during the signature phase. It can assume the values "YES", "NO" or empty (if it is not mandatory).	Field name: name of the field you are entering; Description: description of the field you are entering. It appears in the form in the signing phase; Mandatory: if checked, the field is mandatory in the signing phase.

By clicking on **Close**, the form closes without saving the field.

By clicking on **Save**, the form closes saving the fields and they appear on the document and in "Signature fields" or "Editable fields" sections. On the document, the fields appear in the same position where they were inserted. They have different colors (yellow for the signature field and blue for any other type), and the description. Hovering over each field with the mouse, the type of the editable field is displayed.

To return the signature field or the editable field on all uploaded documents just tick the **Apply the field to all documents on this process** item.

To delete an editable field, click on  and it is removed from both the document and the list.

To modify an editable field, click on it on the document or on  in the list.

In this section, you can also set a font and a font size to the editable field: when printing or previewing the signed document, the enhancement of this field saved during the signature phase will be displayed with the font and size selected during the creation of the process.

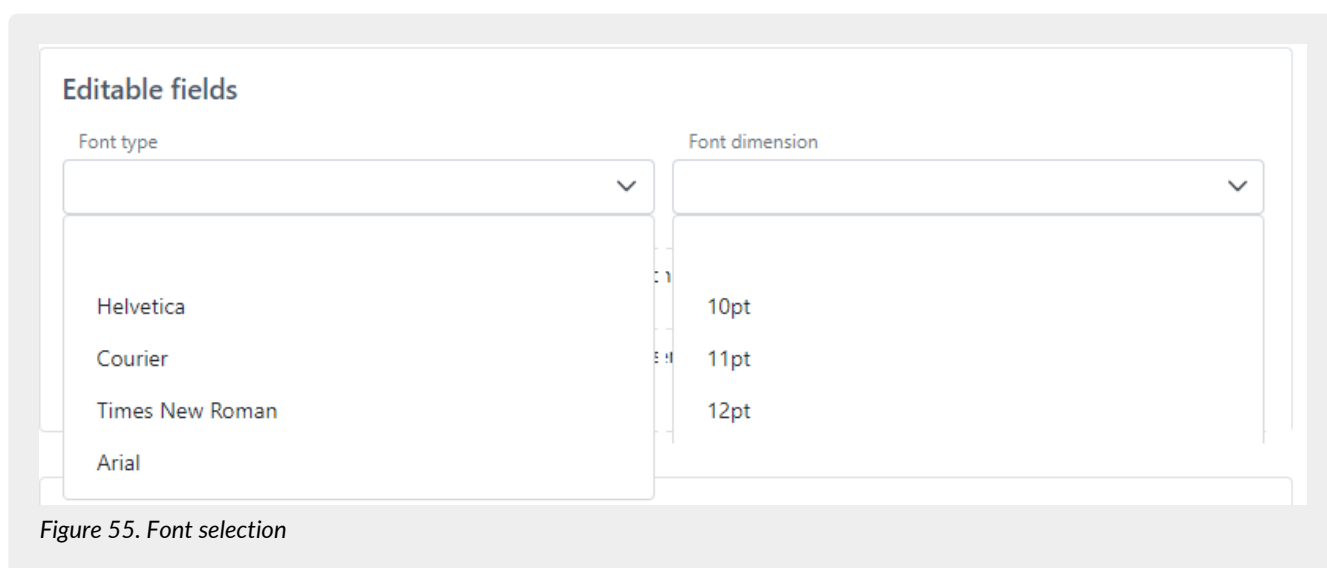


Figure 55. Font selection


Fonts available are *Helvetica*, *Times-Roman*, *Arial* and *Courier* and the font sizes available are 10, 11 e 12.

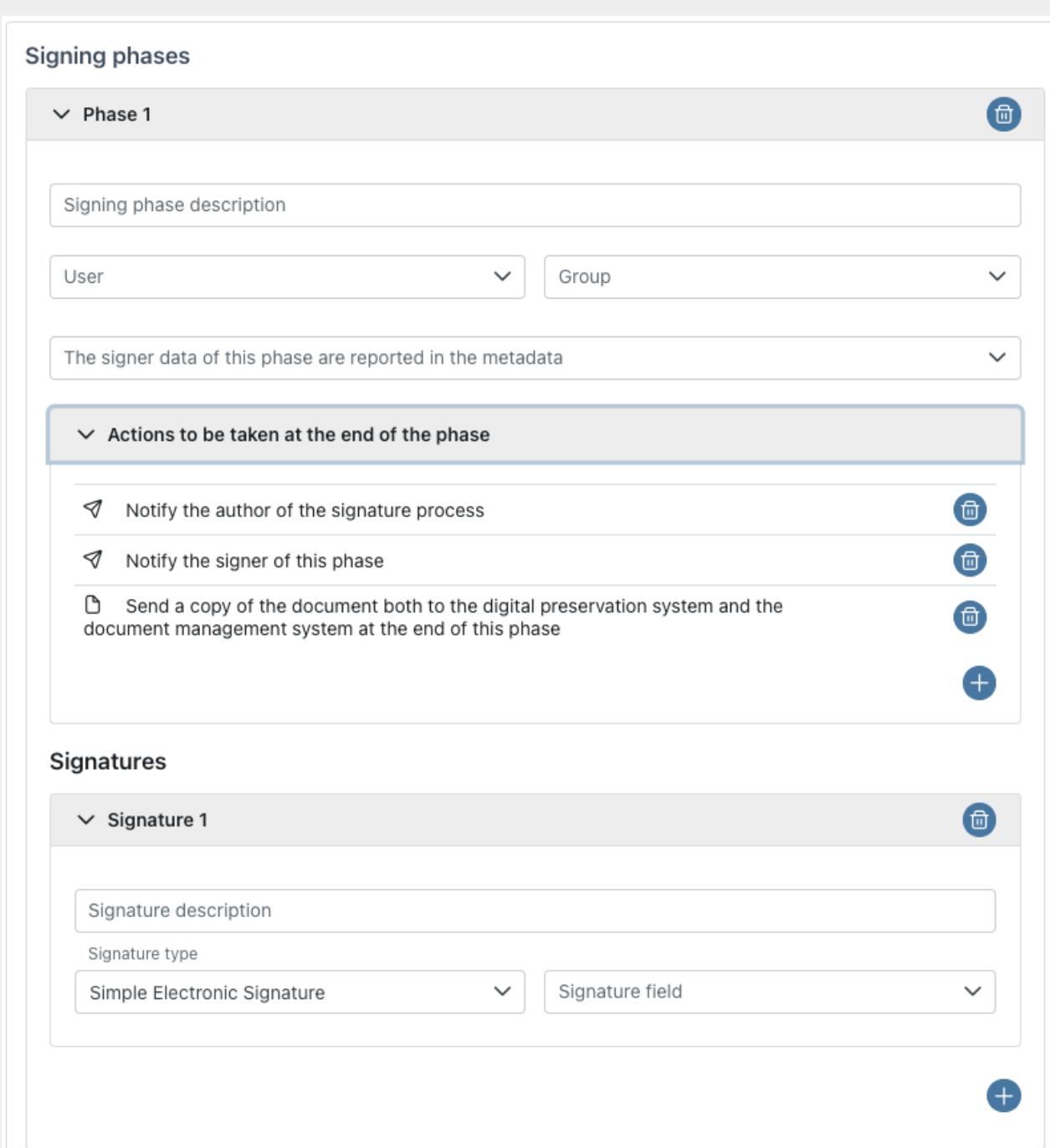
If no font or font size is specified, editable fields will be automatically displayed with default values, which are *Helvetica* for the

font and 10 for the font size.


Signature fields are not editable.

Signing phases

By clicking on the blue icon  at the bottom right of the signature phases section, a signature workflow step is added.



Signing phases







▼ Phase 1 


Signing phase description

User ▼ Group ▼


The signer data of this phase are reported in the metadata ▼

▼ Actions to be taken at the end of the phase

-  Notify the author of the signature process 
-  Notify the signer of this phase 
-  Send a copy of the document both to the digital preservation system and the document management system at the end of this phase 



Signatures

▼ Signature 1 

Signature description

Signature type

Simple Electronic Signature ▼ Signature field ▼





Figure 56. Signing phases.

To cancel the entire signature phase (including all the sections present in it), click on  next to the relevant phase.

To insert a further signature phase, click on the blue icon at the bottom right with the symbol  placed inside the phase section.

The added signing stage consists of various sections, a section relating to general information, a section relating to the editable fields (present only if they are previously entered), a section relating to the signature and its definition and, finally, a section relating to the notifications and the document sending to the ePLUS service.

Below a list of fields in the section relating to the general information.


- **Signing phase description.** It is the description to recognize the phase within the whole process.
- **User.** In this field, you have to specify the signatory user. The user can be chosen by the list: only previously entered users are selectable. If the list is too long, you can search for him through the field at the top of the list. To cancel any selection, select the first empty field in the list.
- **Group.** In this field, you have to specify the signing user group. In this case the signature phase that you are creating affects multiple users. The group can be chosen from the list: only groups that have been previously recorded as non outdated in the database can be selected.
If the list is too long, you can search it through the field at the top of the list. To cancel any selection, select the first empty field in the list. To cancel a previously made selection and reset the group choice to "empty," select the first field in the list (empty field).
If the group contains signatory users marked as outdated, the process cannot be started. It is necessary to access the group's record and remove these users (see [Signatory groups](#)).
- **"The signer data of this phase are reported in the metadata".** If you choose an option among those proposed (sender, recipient, intermediary) the data of signatory is set in the appropriate metadata when the signed document is sent to ePLUS service. If nothing is specified, the data of the signatory metadata set by default is the recipient one.




The signatory user **cannot** reject processes that involve a group as a signatory at any stage during the signing phase.

If editable fields are inserted, you can decide which of them should be filled in phase just selecting them in **"Fields list"** section. To select/deselect a single editable field, just click on the relative item. To select/deselect several fields at the same time, just press the Ctrl key and click the items at the same time. In case the list is particularly long, it will be possible to filter.

In the section "Action to be taken at the end of the phase," it is possible to view/edit the notifications and actions previously inserted "Company master data" from the "Configuration" menu (see [Company master data](#)).

If, for the given phase, the default notifications from the configuration do not meet the requirements, the notification can be deleted by clicking the appropriate button  on the right side of the respective row.

To add an additional action to be performed at the end of the phase (whether it's a notification or sending to the ePLUS service), simply click the blue button at the bottom right  and the relevant entry form will open. From there, select the desired action from the list and click the **"Save"** button.

Among the available options, there is also the option **"Send a copy of the documents completed in this phase to another user"**. By selecting this option, it will be possible to send a notification to a third-parties user, different from the signatory user, which can be selected from the appropriate list in the previous form.



Notifications in intermediate phases will be sent **exclusively** to the author of the signing process. Notifications to the signatory user or a third-parties user will be sent **only** when the document is fully signed.

In the case of actions related to the ePLUS service (only for preservation system, only for document management system or both), the option will automatically be available **only** in the final signing phase. In fact, if there are two or more phases, this option will be visible and active automatically only in the final phase introduced: if the user returns to the previously added phases, will find that the option is absent. However, if there is a need to send the document to the ePLUS service at the completion of any intermediate phase (or even all of them) user modify the relevant phase and add the desired action as previously described.

It is important to note that, while three types of notifications (one for the signature requester, one for the signatory user and one for the third-parties user) can be present only one type of notification to the ePLUS service.



Below a list of fields relating the signature section.

- **Signature description.** it is the signature description.
- **Signature type.** You can choose between three different signature options: **simple electronic signature**, **advanced electronic signature** and **qualified (or digital) electronic signature**.
When starting the process, the service carries out consistency checks of the information contained in the signatory registry with the selected signature type.
In particular:
 - to affix a simple signature, the details of the signing user can only be completed with minimal data: name, surname, email address and tax code;


- to affix a digital signature, the signatory user's details must be name, surname, email address, tax code and phone number. The signatory must have a signature device, such as a reader and a smart card, and install the **eSIGN Desktop** application (see [eSIGN Desktop](#));
- to affix an advanced signature, the signatory user's details must be completely filled out: all the fields present in the general, birth and residence data section must be filled in.


There must be the acceptance of the FEA information acquired either on paper or from a dedicated and completed process.

Furthermore, identity documents must be saved in the registry. In the event that the company is in possession of these documents, but they have not previously been saved in the registry, it is necessary to tick the item "The identity document was acquired externally" in the general section of the registry (see [Enter signatory users](#)).

- **Signature field.** You have to specify the signature field. To cancel only the created signature, click on  next to the signature. To insert a further signature within the same phase, click the blue icon in bottom right with symbol .

In "Action to be taken at the end of the phase" section, it is possible view or modify the previous notifications and actions defined in the "Configuration company" from the "Configurations" menu (see paragraph [Company configurations](#)).

If the default configuration doesn't correspond to your needs, you can delete it by clicking the designated button  on the right of the respective row.

To add an action to be performed at the end of the phase (whether it's a notification or sending to the ePLUS service) simply click the blue button at the bottom right  and the corresponding input form will open. Simply select the desired action from the list and click on "Save".

Among the selection options, there is also the option "Notify as user of this phase (not the signer)". By choosing this option, at the end of the phase a notification is sent to the selected user different than the signatory.



Notifications during the intermediate phases will be sent exclusively to the author of the signing process. Notifications to the signatory or a third-parties user will be sent only when the document has been fully signed.

In the case of the actions referring to sending copy of the documents to ePLUS service, the option is present **exclusively** on the last signature phase. If there are more than a phase, this item is visible **only** in the last phase. If you need to send the document to ePLUS service upon completion, you have to introduce it in the intermediate phases.

It should be emphasized that, we can insert three types of notification (one for the signature requester, one for the signer and the last one for another user) at the same time, but we can enter only one type of sending documents to ePLUS service.

The **Delete Process** button allows you to delete the entire process. The **Start Process** button allows you to start the signature process as described in paragraph [Signing process workflow](#).

It should be emphasized that **it is not possible to start a process with documents without signature fields**. Every document of a process (whether manual or from templates), must contain at least one signature field associated with a phase.

It is possible to return to the list of signing processes page by following the navigation path at the top left and clicking on the "Signing Processes" option.

6.5.3. Restarting a rejected signature process

Restarting a process consists of **creating a new process identical to the one rejected, both in the phases and in the signatories, and connected to it**.

Workflow details

ProcessoRifiutato

Signing process description

ProcessoRifiutato

Consumption

2 Single signatures

Workflow status

REJECTED

Reject reason

Dati inseriti errati

Restart process

Signature information

Q

Search

Document	Signer	Signature type	Signature field	Signature status	Signature description	Phase description
DocumentoDemo.pdf	ROSSI UMBERTO (SQDXAA80A01E472A)	Simple Electronic Signature (with timestamp)	Field FirmaDipendente at page 1	REJECTED	firma dipendente	Dipendente
DocumentoDemo.pdf	GIALLI UMBERTO (MBRGLL66A01E472R)	Simple Electronic Signature (with timestamp)	Field FirmaDatore at page 1	COMPLETED	firma datore	Datore

2 total elements

<<

<

1

>

>>

10

Figure 57. Restarting a rejected signature process.

To restart a rejected process it is necessary to go into its detail and to click on the **"Restart process"** button.

You will be asked whether to reuse the data already entered during the signing phase in the rejected process or not. In the event that during the signing of the original rejected process, it was requested the insertion of attachments or personal, additional or editable data and these data have been valorised, by confirming this "reuse", during signature the signing user must not have to enter this data again, because they are already valued. However, he may make any changes if necessary.

A process can be restarted **only** once.

The new process, which we call "son", and the original process, which we call "father", they are connected to each other.

By going into detail about a rejected and restarted process, by clicking on the **"Go to the restarted process"** button, the detail page of the "child" process is opened in order to monitor its status.

Similarly, going into detail about any process, if this turns out to be a restarted process from a rejected one, by clicking on the **"Go to the origin process"** button the detail page of the "parent" process is opened.

6.6. Process template

In the **"Process template"** section you can view, insert, edit and outdate (see [Management of outdated templates](#)) any signature process templates. They can be used to standardize and automate processes ([Adding a signature process](#)).


In the event that the templates contain additional data, you can view **exclusively** the templates containing the additional data for which you are enabled (see [Access management](#)).

eSIGN > Process template		
+ Add		
Process template		
Code	Description	Outdated
No elements		
0 total elements << >> 10		



Figure 58. Process template

Below there is a brief description of the items and filters on the list.

- **Code:** it is the template code entered during insertion.
- **Description:** it is the template description entered during insertion.
- **Outdated:** it indicates whether the template is obsolete ("Yes" value) or is still active(value "No").
- **AdES agreement:** AdES agreement: it indicates whether a template has been marked as a template for AdES agreement or

not it can only have the values "Yes" and "_No". The column is not directly visible in the list: it must be included by the user by clicking the function button .

From this section you can:

- order the columns and filter the elements as described in the [Console tables](#) chapter;
- modify the template by clicking on the row;
- add a new template by clicking on "Add" button;
- duplicate the template by clicking on  icon. A new form opens where you have to insert the code and the description of the duplicated template. By clicking on "Save" a new template is created with the code and description inserted in the form and documents and phases of the original template.
- delete the template by clicking on . You can delete a template only if it isn't used in a new process.

6.6.1. Adding signature process template

By clicking on "Add" in the "Template process" page, you can insert a new template.

In the event that the template contains additional data, you can upload **exclusively** the templates containing the additional data for which you are enabled (see [Access management](#)).

In case you are enabled for the complete management of the additional data, you can upload also templates with additional data not previously entered in the system. In this case the service creates new additional data and you can see it in the "Configurations" section (see [Additional data](#)).

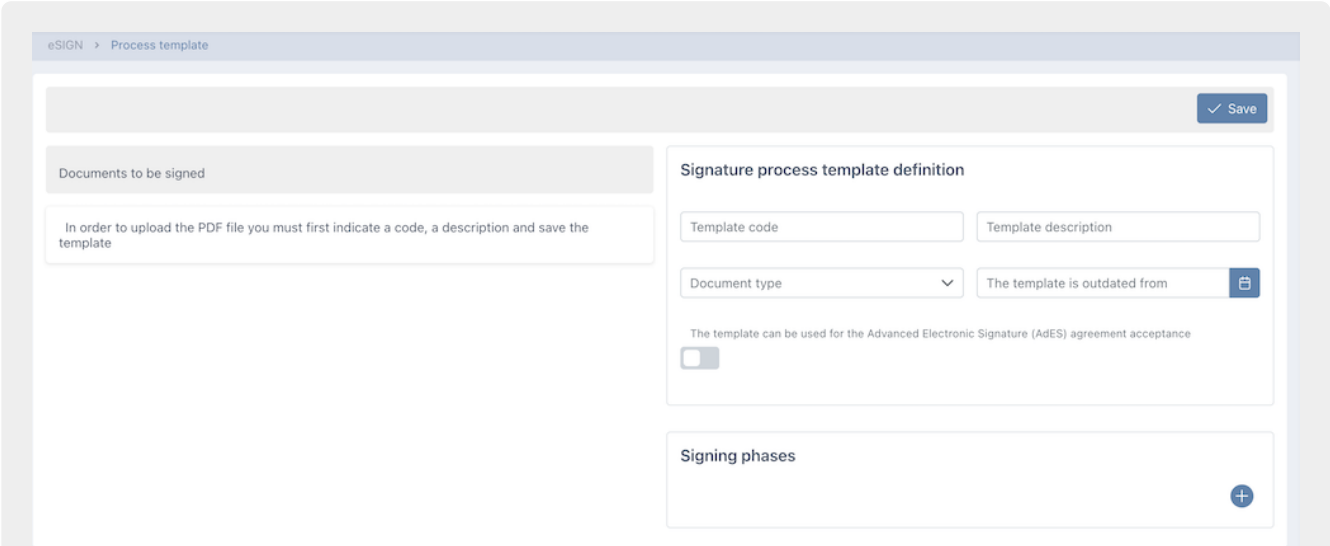









Figure 59. Adding signature process template.

In the right section, **Signature process template definition**, you must enter the following data.

- **Template code.** It is the code that you want to attribute to the template. In order to facilitate your searches, it is suggested to enter a "speaking" code.
- **Template description.** It is the code that you want to attribute to the template.
- **Document Type.** It is the document type to set standard metadata to compile SIP by ePLUS service.
- **AdES agreement:** by ticking this item you specify that the template is usable for AdES agreement. For this type of template, you can specify whether the signatory user added or updated through the acceptance can be 'marked' as exportable by simply checking the "the signatory user as exportable" option.
- **Entering of a new signatory:** this item is visible **exclusively** if the loaded template (.ODT or .DOCX) contains the markers to enter the personal data, i.e. U_CFI, U_COG, U_NOM, U_EMA (see [Markers](#)). By enabling this check, a new signatory user (different from the signer of the process) will be added with the values entered for the requested data during the signing process. By checking the "the signatory user as exportable" option, the added signatory user will be "marked" as exportable.
- **Mandatory documents:** this item can be selected **only** if the FEA information or the entering of a new signatory have been previously selected.
Checking this item, during the signing phase of the processes started by this template the documents are mandatory.

The documents entered during signature **are automatically saved** in the created registry: either that of the signatory user (in case of AdES acceptance) or that of a new user;

- **The template is outdated from:** It is the deactivation. Starting from this date the template is outdated, no longer usable (see [Management of outdated templates](#)).
- **Classification:** it is the classification scheme. This section is present only if an active classification scheme data has been defined in the company and if the author of the process is authorized to select the classification. (see [Classification scheme](#)). By clicking on the  button, you can select the classification of the documents. The standard metadata for the classification scheme are automatically set to ensure the correct creation of the Submission Information Package, its automatic submission to ePLUS, and the proper publication in the eDOC document management service.
- **Template parameters:** in this section, once the template is uploaded, the parameter-type fields (not related to signing and not editable, as outlined below) defined through the marker construct will automatically appear (see [Markers](#)).
By default, the parameters will be loaded as text fields, with the name `nomeparametro` defined by the marker being non-editable and with the description "Parametro" + "nomeparametro" (editale).
Clicking the button  it is possible to modify the properties of these fields as defined by the marker:
 1. the field type can be selected from the available options in the list (text, number, list, date, date and time, YES/NO);
 2. the description automatically proposed by the service;
 3. the dedicated properties for each selected field type are as follows: Minimum length, maximum length, and validation pattern (not mandatory) for a text field; number of decimals (not mandatory) for a numeric field; list of items (mandatory) for list-type fields;
 4. the mandatory or not mandatory nature of the parameter's value during the process creation phase.
The user can populate the parameters defined in the template during the creation of the signing process. (see [Signing process](#))
- **Signature fields.** After loading the template, in this section all signature fields are listed. They must be inserted in the template file as described in the [Markers](#) paragraph.
- **Editable fields.** After loading the template, in this section all editable fields are listed. They must be inserted in the template file as described in the [Markers](#) paragraph. By clicking on the editable field or on  icon, you can enter the editable field properties. It is important to make sure that you have defined all properties, because you can't modify them during the process definition.
As in signing processes, the height and width of editable fields can be configured for any type of field.
If not specified, the standard field size is 20 px in height and 100 px in width.
If a text-type field is assigned a height greater than 20 px, during the signing phase, the field will automatically be defined as a text area. This means that any text formatting entered by the signatory user, such as a new line, it will be reported on the signed document. For editable fields derived from additional data of the list type, the concept of "inheritance" of saved values in the registry is present. When creating a template, the additional list-type data present on the document is populated with the current data in the registry. If the values in the registry are subsequently updated (by adding or removing elements), these changes are not automatically reflected in the already loaded templates. However, if the field **"Inherit possible values from the company's additional data"** is enabled in the edit screen of the list-type additional data, the values selectable by the signatory user for the list-type field during the signing process will be those modified and present in the registry of the additional data.
You can also set a font and font size to the editable field: during printing or preview of the signed document, the enhancement of the editable field saved during the signature phase will be displayed with the font and font size selected when creating the template.
The available font are *Helvetica*, *Times New Roman*, *Arial* and *Courier* and the available font size are 10, 11 and 12.
If no font or font size is specified, editable fields will be automatically displayed with the default value: *Helvetica* for the font and 10 for the font size.
- **Signing phases:** the method for entering the signature phase is similar to that described in paragraph [Adding a signature process](#). By clicking the button  in the bottom right, a signature step will be added to the template being created. User be able to enter the identifying details of the signature step, select any editable fields, add the various signatures along with their details, and confirm or modify the configured actions.
For signature processes involving recurring signers (users or groups), setting up these signers in the template will automatically include them during the process creation, significantly reducing user effort. However, it will always be possible to modify the predefined signers in the template during the process creation stage.
Clicking the icon  in the bottom right will add a new signature, if needed.
Clicking the icon  next to the signature will delete the associated signature along with all the entered information.
Clicking the icon  next to the signature step, on the other hand, will delete the entire step, including any previously

added signatures.

In the left section, **Documents to be signed**, you can upload a template document. You can load documents only if you have previously saved the template, at least the code and its description.


The document upload process is the same to the one described in the paragraph [Adding a signature process](#).

Documents that you can upload as templates could be:


- in .ODT or .DOCX format;
- in .pdf format;
- in empty .pdf format: the pdf document will be associated when defining the signature process.

A template can contain one or more documents of the three types listed above.

By clicking the **Save** the template is saved.

In order to download a template document, you have to enter in the template detail page, to select the document in the list on the left and to click on .

The document is downloaded and you can use it to create a new template.

In case, instead, the user have the need to change the template's file name previously saved, it is enough to use the function of editing the template, select the desired document and click on the button : a mask will be displayed where the user will be able to enter the new name, then click the "Save" button located at the bottom right to confirm the change.

After saving the template, it can be associated with a signature process such as described in [Adding a signature process](#). The template will turn out to be modifiable or removable **only** if it is linked to a signing process that has been started or completed. In case the process associated to the template is in new status, the template cannot be modified or deleted.

6.6.2. Entering a template in .odt or .docx format

In order to correctly define a template, the uploaded documents in .ODT or .DOCX format must have the following characteristics:

- to contain markers to automatically load the signature fields, the editable fields and any additional fields;
- the used font must be one of those indicated in the list below.

Fonts that can be used to create a template
Andale Mono
Arial
Arial Black
Carlito
Comic Sans MS
Courier New
DejaVu Math TeX Gyre
DejaVu Sans
DejaVu Sans Mono
DejaVu Sans,DejaVu Sans Condensed
DejaVu Sans,DejaVu Sans Light
DejaVu Serif

Fonts that can be used to create a template
DejaVu Serif,DejaVu Serif Condensed
Georgia
Impact
Lato
Liberation Mono
Liberation Sans
Liberation Sans Narrow
Liberation Serif
Open Sans
Open Sans Condensed
Open Sans,Open Sans Condensed Light
Open Sans,Open Sans Extrabold
Open Sans,Open Sans Light
Open Sans,Open Sans Semibold
OpenSymbol
Times New Roman
Trebuchet MS
Verdana
Webdings

If you need to use a font other than those listed above, it is possible to request the addition opening a support ticket by sending an email to helpdesk@entaksi.eu.



Also, in case your template is for an AdES agreement, you can insert specific text-type field markers on it. When it is signed, the signer will enter in the signatory users list. In fact, in order to sign the document, the signatory has to insert his personal data.


If, however, you are uploading a template for entering a new registry, exactly as for the AdES agreement, it is possible to insert specific ext-type field markers to insert or modify a signatory user different from the signatory of the process.

To define markers, please refer to the [Markers](#) paragraph.

When the document is loaded, the markers are displayed with their values in the right section.

The three types of markers are easily distinguishable by the icons on the left side of the field:

-  : it is a "personal data" type marker. This type of markers enters or updates a signatory user's personal data (see [Markers](#));
-  : it is an "additional data" type marker. This type of markers enters or updates an additional data (see [Markers](#));

-  : it is an "editable field" type marker. This type of markers fills a value into the document during signature by the signing user (see [Markers](#)).

When entering a template, this third marker type requires a manual valorisation of the mandatory or additional fields: it is therefore necessary to enter in edit mode and save the changes.

In order to complete the template registration with editable fields, it is necessary to edit each of them to enter the mandatory fields and any additional fields (not mandatory).

If this type of marker is not correctly filled, it has the  icon on its left side, otherwise it has the  icon.

Below is the list of mandatory or additional fields divided by editable field type.

Text field	
Valuable field	Mandatory
Description	SI
Field min lenght	NO
Field max lenght	NO
Validation pattern	NO
Numeric field	
Valuable field	Mandatory
Description	YES
Digits	NO
Date field	
Valuable field	Mandatory
Description	YES
Date-time field	
Valuable field	Mandatory
Description	YES
Values list field	
Valuable field	Mandatory
Description	YES
Values list	YES

Yes/No field	
Valuable field	Mandatory
Description	YES

In case of AdES agreement acceptance template, it is not necessary to edit markers: specifications are automatically recognized by the system.


It could happen that for some markers it is not possible to assign a value. For example, all markers that refer to a signer are valued only when the signer is entered in the signing process. In this case these markers are valued with "???" in the template.

When the template is associated with a signing process and a signatory user, or a signatory groups is assigned to it, the fields related to the signatory user will be automatically populated.

6.6.3. Entering a template in .pdf format

The management of a document in .pdf format within a template, whether empty or not, is same as that described in the [Adding a signature process](#) paragraph.


To insert an empty .pdf document, click on , enter its name and its number of pages.

Empty .pdf files will be recognizable in the list by the icon .

The empty .pdf file is to be considered as a neutral identifier of a .pdf document to be signed: it will then be punctually defined later when creating the signature process (see [Adding a signature process](#)).

By inserting these files, therefore, it is possible to maximum generalize the template. In this way, by not specifying any document, the template can be used to create processes with different characteristics.


The uploading process of the .pdf document is similar to the .odt and .docx files one.

By clicking on the upload button  a management opens to upload one or more files (see [Adding a signature process](#)). The uploaded .pdf files, unlike the empty ones, cannot be replaced during the creation of the process: they will characterize its structure.

After uploading the .pdf file, both valued and empty, any signature and editable fields can be inserted simply clicking on the document and choosing the type of field.

To optimize their positioning, simply select them and move them with the mouse drag and drop function.

To change the properties of editable fields, just click on the field itself on the pdf or on the icon .

To delete a previously inserted editable or signature field, simply click on the icon .

In the case of an empty .pdf file, the positioning of any editable or signature fields is very important.

In fact, when creating a process, the service will allow you to associate a blank .pdf file with a valued .pdf file that has the same or greater number of pages to the number of the last page containing editable or signature fields (see paragraph [Adding a signature process](#))


For example, in case the blank .pdf document was created of seven pages, but the last page that has signature fields is the fourth, during the creation of a process this empty .pdf can be replaced with a .pdf document of at least four pages.

6.6.4. Management of outdated templates

In order to outdate a template (no longer usable), you have to modify it entering the deactivation date.

If there are new processes defined by that template, you can't enter the deactivation date.

From the deactivation date, the template will no longer be available in the list of templates to define a new signature process.

Outdated templates can be easily identifiable thanks to the "Yes" value within the list of templates in the "Outdated" column and the deactivation icon  shown in the detail page.

If you want to re-enable the template, just enter the edit mode and cancel the deactivation date and save.

6.7. Signing process workflow

This paragraph describes the signature process workflow of eSIGN service: from its start to its end.

The signature process ends when the signatures of all phases in all documents are affixed.

In the event that the signing phase is associated with a group of signatories, the document is started for each user in the group (identifying it with a unique code).

After starting a signature process, if the relative notification action is defined in the phase, the system automatically send start confirmation email to the author of the process.

This email contains the name of documents to be signed and the signatory's name.

Each signatory receives a signature request email at the address recorded.

In order to sign documents, the signatory must access the eSIGN portal. By clicking on the **"Sign Documents"** button in the body of the email, a new page with a short introduction to eSIGN service is opened. By clicking on **Start signing process**, the eSIGN portal opens.

In this page signatory can view all information about the document and compile it if required.

Once the document has been viewed and completed in its entirety (where required), it is possible to sign it both via Entaksi app and via a verification code (OTP). In this second case, the code is sent via SMS or via email to the signatory.

By entering this code, the signature process is finished and the document is correctly signed and available for download.

When the signing process is finished, in case of notification to the signatory or to the signature requester are requested, a conclusion email is sent with the signed document as attachment.

In the event that the sending of notification to a third user is also requested, he receives the same email.

In the "Signature Processes" section, the status of the above workflow can be monitored at any time.

In particular, it is possible to view the details of the signatures and the progress of affixing for each document (see paragraph [Signing process detail](#)).

When the process is completed, the signed documents are automatically sent on ePLUS service according to the rules defined in the signature process.

The documents are submitted according the configuration (only documentary, only preservation or both) and they contain the minimal metadata to be validated.

The SIP are automatically confirmed (and therefore closed) only if expressly specified in the company configuration (see paragraph [Company configurations](#)).

For more information, please read the [ePLUS service user manual](#) and the [eCON service user manual](#)

6.8. Signature pages

Through the signature pages, it is possible to affix electronic signature to documents.

The signatory can access to the signature page via the link sent by email from the system.

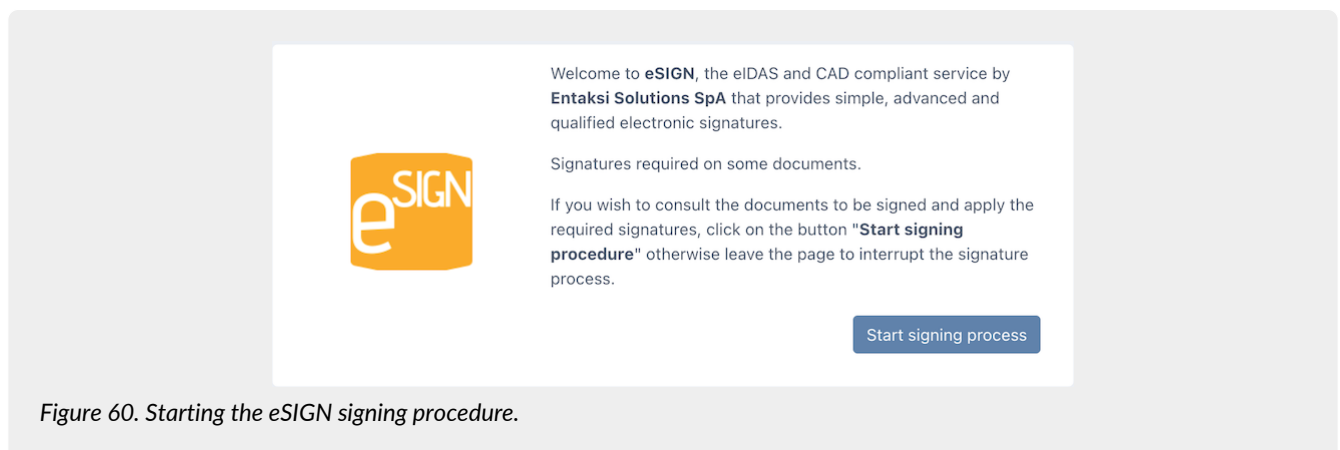



Figure 60. Starting the eSIGN signing procedure.

By clicking on **Start signing process**, a new eSIGN page opens where the signatory can sign documents.

The page is divided into two sections. In the left section the signer can view or download the documents to be signed. In the right section information relating to signatures is displayed.

In the case of digital signature is required, there is an additional section on the right of the page where the status of the signature smart card reader is shown.

The list of involved documents is shown in the top left-hand list. By clicking on  you can download the document to be signed. When viewing the document, any required editable fields is displayed: those required at the current phase and those required in other phases of the process (before or after).

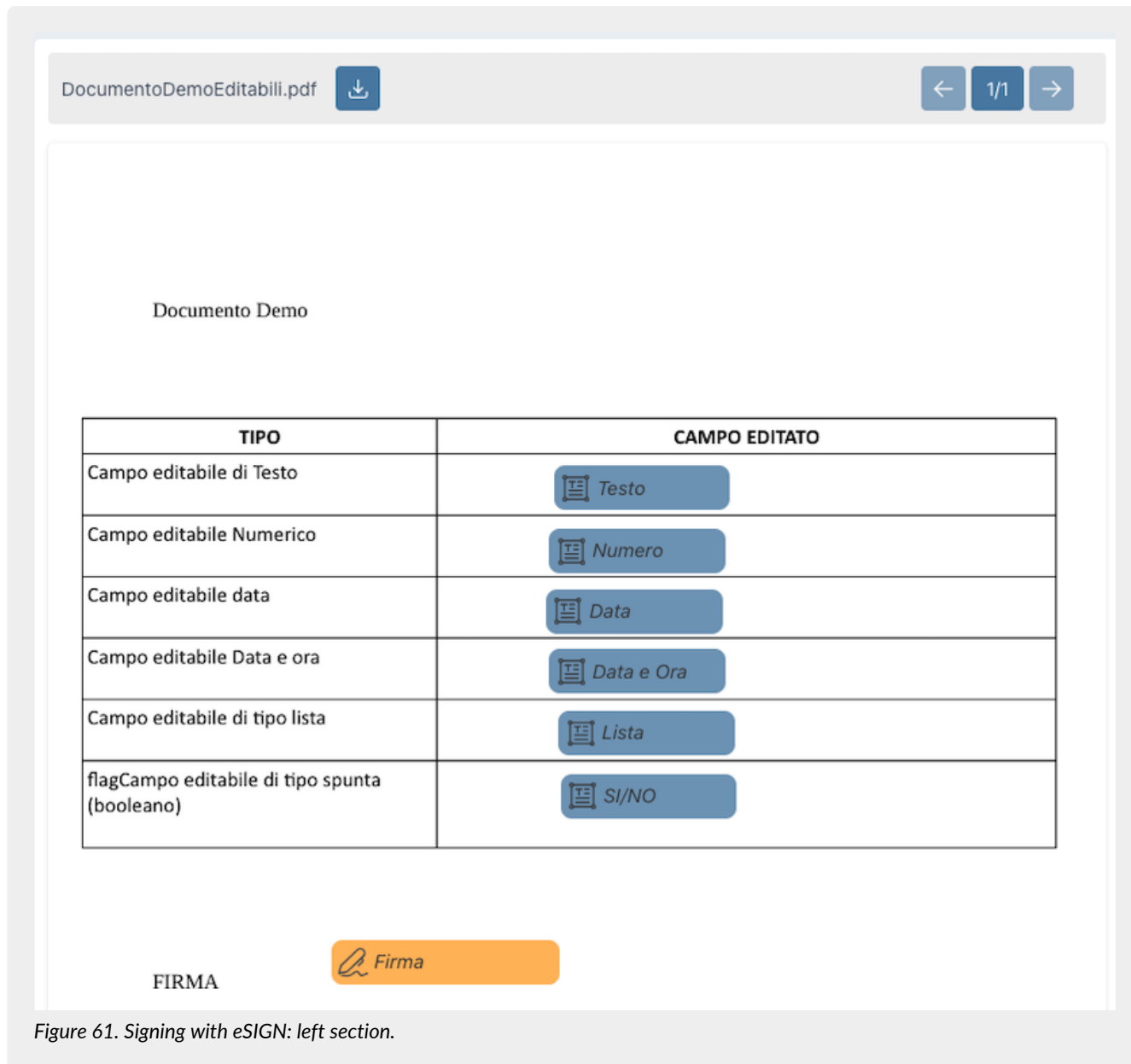


Figure 61. Signing with eSIGN: left section.

To display information regarding these fields such as the name, the signatory who filled them or who will value and any values entered, you have to hover over them with the mouse. A tooltip with this information is shown.

The editable fields to be inserted in the current signature phase, are those whose signatory is the same of the phase.

For quicker viewing, any dark blue editable fields is required in the current phase and those with a gray color are required in different phases. In the absence of entered values, the internal icon next to the description is black, otherwise it is green.

Similarly, the signature fields displayed in the document are also both those requested in the current phase than those requested in other phases (before or after).

Just like the editable fields, just hover over them to view information about the type of the requested signature, the name of the signatory, the reason for the signature and the date and time they were affixed (in the case of signatures from previous phases).

The signature fields of the current phase are those whose signatory is the same of the phase.

For a quicker view, the signature fields shown in dark yellow are the signatures required in the phase, while those in a lighter yellow refer to signatures requested in other phases. The internal icon is green if the signature is just affixed, otherwise it is black.

The right section is instead divided into several subsections.

The screenshot displays the right-hand side of the eSIGN interface, which is organized into several distinct sections:



- Top Section:** A white box containing the text "Dear **Umberto Gialli**," followed by "signatures are required on this document."
- Information Section:** A white box with instructions: "Before completing the signing operation it is necessary to indicate some information." and "Fill out the form by clicking on the button near the document name." It also states: "Attach an identity document by clicking on the  button below."
- Action Buttons:** Two white buttons with blue borders. The first is labeled "Add files to attach to the signed document" and features a blue paperclip icon. The second is labeled "Reject all signatures" and features a blue circle with a diagonal line through it.
- Document to be signed:** A white box with the title "Document to be signed". Inside, it shows a document icon and the filename "INS_Anag_datiaggLista.pdf" next to a blue warning triangle icon. Below this, it specifies the signature type: "Simple Electronic Signature (with timestamp) on field **Firma1** at page **1**" and the reason: "Signature reason: Firma 1". A blue paperclip icon is positioned to the left of the signature details.

Figure 62. Signing with eSIGN: right section.

By clicking on  icon will open a form for viewing the attached files during the entire signing process and for the possible insertion of new attachments in the current phase.

Add files to attach to the signed document

Signature process attachments		
Description ↑↓ ▾	Attachment type ↑↓ ▾	Signer ↑↓ ▾
Carta Identità Prima Fase	Identity card	Gialli Umberto
Documento Generico Prima Fase	Other	Gialli Umberto

Signature request attachments		
Description ↑↓ ▾	Attachment type ↑↓ ▾	
Documento Generico seconda fase	Other	

+ Add X Close

Figure 63. Attachment list.

In the **"Attachements of signing process"** section any attachments previously added by other signatory user during the signing process phase are displayed.

In the **"Attachments of signing request"** section, attachments added during the current phase of signing request will be displayed.

Clicking the **"Add"** button will display an additional form where you can select the type of file to be attached and the mandatory data to be inserted.




If the selected type is "Other", simply enter a description, select the file to attach and, click the "Save" button.

If the document type is different from "Other", you need to input, in addition to the scanned document, the description, the number, the institution that has released the document and the start and end validity dates.


The inserted documents are displayed in the list "Attachments of signing request".



If there are special characters in the file name (for example "ù", "à", etc.), it is recommended to rename the file by removing these characters, otherwise the system automatically removes them when the file is acquired.

The file uploaded in this way are displayed in the "Attachment of signing request" list where, in line, for each attachment, you can both modify the description (by clicking on ) proceed to its deletion (by clicking on ) or download it locally (by clicking on )

By clicking on **"Close"**, you can return on the signing page.


In the event that attachments have been added, either in the current phase or in previous one, the button icon will appear in green ()

Information about the presence of attachments is also provided by the descriptive tooltip that appears when hovering over the icon.

If the attachments are mandatory in order to complete the signature, the saved attachments **will be automatically inserted** into the user's registry that the process will insert into the Console, or the signatory users (in case of AdES agreement acceptance) or a user different from the signatory.

The document will be visible in the "Identity Documents" section of the signatory user profile.

In the second section, it is possible to reject the sign request.

By clicking on  a new form opens to enter the reason of the rejection. By clicking on the "Save" button and confirming the action, the signing phase is rejected and the rejecting reason is saved.

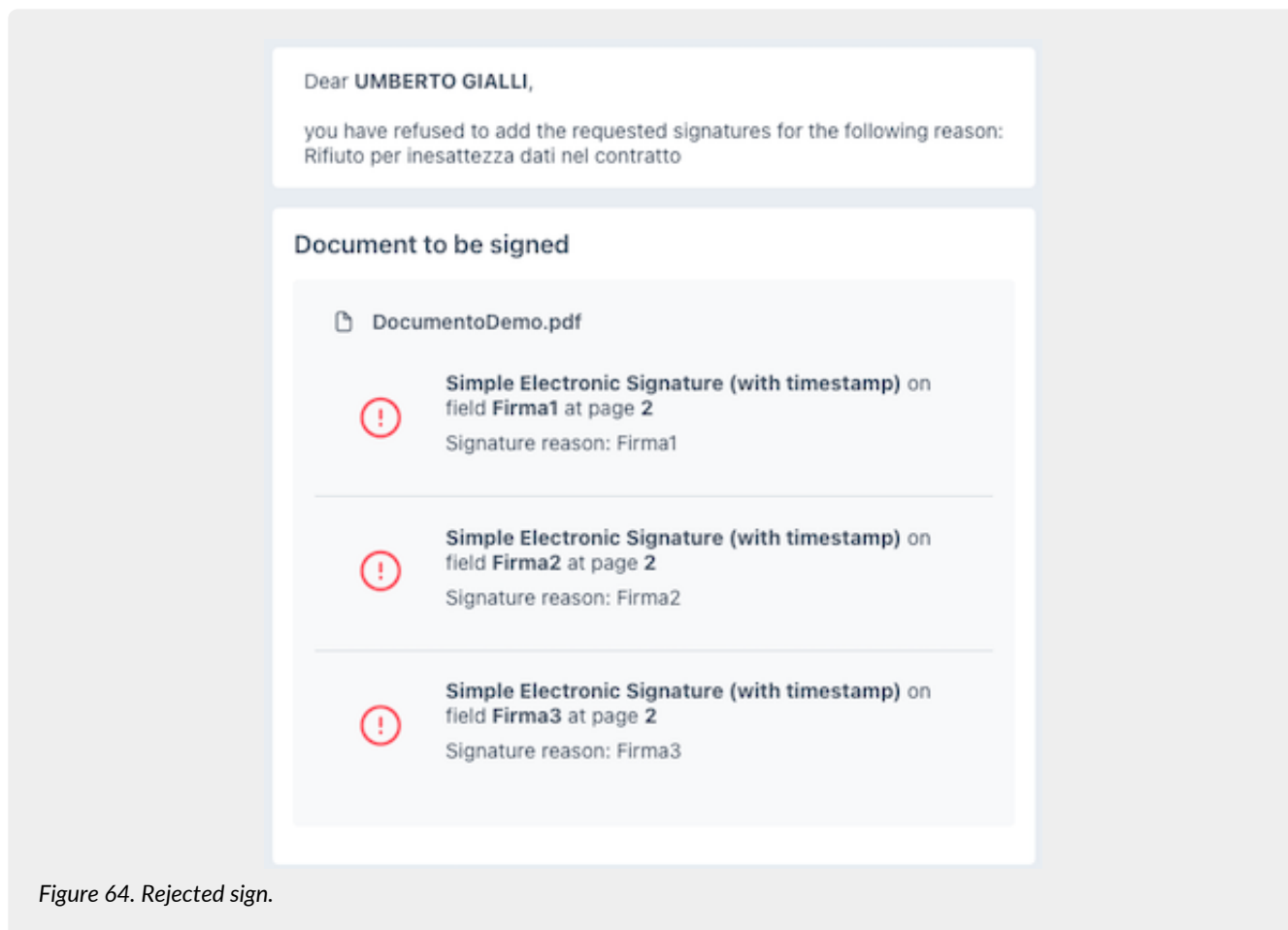




Figure 64. Rejected sign.


All the requested signatures are rejected and they are listed with the  icon. The rejection reason is shown at the top of the page.

Rejecting the signature, the entire process will be in "Rejected" status in Console. However, it will be possible to start it again later (see [Restarting a rejected signature process](#)).

The third section contains the list of documents to be signed with the main descriptions of the electronic signatures required (if one or more). If additional fields have been defined during the signature process setup, a button will appear,  which the signatory user must click to enter the values for the additional fields that were set during the process definition.

Clicking this button will open a new form where the data can be entered according to the rules established during the signature process setup (field order; maximum and minimum values; decimal places, etc.).




If none of the requested data is mandatory, it is still necessary to save in order to confirm the "non-entry of data" to complete the signature process.

The  icon next to the document indicates the correct completion and saving of the fields.

If you wish to modify the previously entered values, click again  and make the desired changes.

The field description corresponds to the one entered in the "Description" field during the definition of the editable field (see chapter [Adding a signature process](#)).

Fill out the form DocumentoDemo.pdf

Text Field	Numeric Field
Data Field 	Date-Time Filed 
Values List Field 	<input type="checkbox"/> Yes <input type="checkbox"/> NO Filed



 

Figure 65. Entering additional data values.

To check type fields (Yes/No), leave the field empty if you do not want to indicate any value. If you want to indicate a positive value ("Yes"), click on the field until the image of a tick appears. If you want to indicate a negative value ("No"), click on the field until the image of an "X" appears. If the editable field is mandatory, you can't leave the field empty.

By clicking on the **"Close"** button, the form closes without saving any data.

By clicking on the **"Save"** button, the form closes and data are saved.

If there are additional data requested, it is not possible to sign until all data has been correctly entered and confirmed. The signatory has to enter in the additional data form and saving even if there aren't values to enter.

The saved additional data are shown in the document on the left by hovering over it.

In case a digital signature has been requested and the eSIGN Desktop application is not connected correctly, an additional section appears. The section provides the instructions to connect correctly the application.

Connect your Smart Card using eSIGN Desktop. You can download and install eSIGN Desktop from [here](#)



Figure 66. eSIGN Desktop is not connected correctly.

In order to sign the document, signatory must have a special reader and a card for signature, and **eSIGN Desktop** has to be installed and correctly connected (see chapter [eSIGN Desktop](#)).

In the event that the digital signature application is not correctly connected to eSIGN service, the icon is red and it is not possible to require the OTP code and to affix the signature.

Only when the eSIGN Desktop application is correctly connected to the eSIGN service, a green icon is displayed indicating the correct connection and the section for affixing the signature is shown.

In case the signatory has not downloaded and installed the Entaksi app to sign documents, it is possible to do it directly in this section.

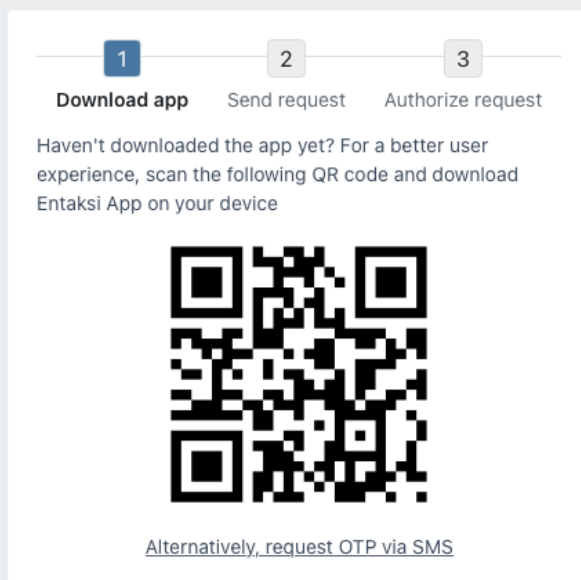


Figure 67. QR Code for Entaksi app download.

To download the app, scan the QR code with your device, through the link you can download and install the app as described in the chapter [Entaksi app](#).

In case the signatory user has already installed the Entaksi app to sign documents, in this section he can decide how to sign: either through the app or through the OTP code.

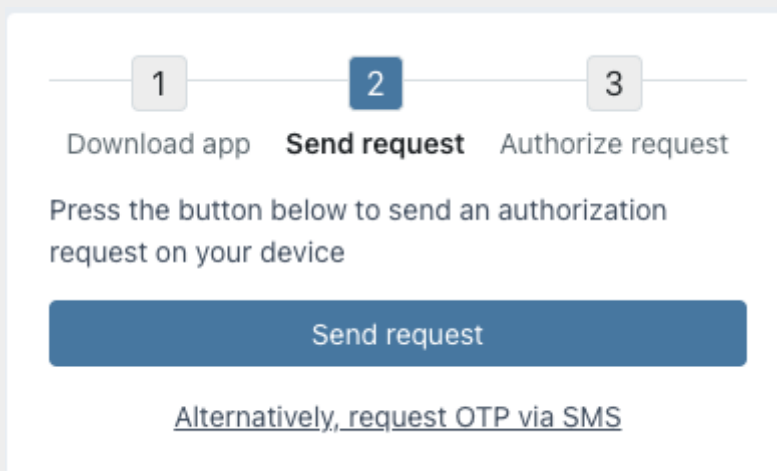


Figure 68. To sign documents.

By clicking on the **"Send request"** button, a signature request is sent to the app and the signatory can authorize the signatures as described in [App access and signing documents](#).

It is possible to sign the documents using the OTP code, by clicking on the link below **"Sign with OTP verification code"**. An One-Time Password (OTP) is sent to the signatory in two ways: via SMS or via email.

The OTP code is sent to the email of the document signer, only if the all the requested signature in the phase are in "simple" type. Otherwise, or with signatures in the phase other than the simple typology, the OTP code will be sent via SMS to the signing user's phone.

With these methods of sending the OTP code, the identity of the signatory is automatically confirmed: this allows you to sign digital documents quickly, legally and securely.

By entering the OTP code and clicking on the **"Confirm verification code"** button, the document will sign.

When all documents are signed, a time-stamped qualified electronic seal is inserted.

6.9. Markers

To customize the templates, it is possible to create a text document in .docx format or .odt. Customization takes place through markers. They are variables (of Freemarker tags) whose display the data saved in the service.

Markers are divided into two parts, **Elements** and **Attributes**.

The elements constitute the category of the variable, the attribute, on the other hand, the true value of the variable.

For example, for the tag `${t.reseller.description}`, the element is "t.reseller" which contains, among its attributes, "description" which is the real value of the marker (for example the dealer description).

The markers that you can use to create a template document are shown in the table below.

Value	Item	Description	Attributes
Date	<code>t.date</code>	It is the process date.	
Company	<code>t.company</code>	It contains information about the company.	descr vatId taxCode
Reseller	<code>t.reseller</code>	It contains information about the reseller.	descr vatId
Process	<code>t.wf</code>	It contains information about the Process.	descr
n-th phase:	<code>t.wf.step[n]</code>	To indicate the n-th phase of the process. For example if you want to report phase 1, you have to insert the <code>t.wf.step[1]</code> element, for the phase 2 the <code>t.wf.step[2]</code> element, etc.	descr
Signatory user of the n-th phase	<code>t.wf.step[n].user</code>	To display information about the signatory user entered in the n-th phase. For example if you want to display the signatory user of phase 1, you have to insert the <code>t.wf.step[1].user</code> element, for the phase 2 the <code>t.wf.step[2].user</code> element, etc.	firstName lastName email phone birthDate birthCity birthProvince birthCountry address postalCode city province country taxCode

Value	Item	Description	Attributes
Additional data signatory user of the n-th phase	<code>t.wf.step[n].user.extra</code>	<p>To display the information about the signatory's additional within the n-th phase.</p> <p>For example, if you want to display the additional data of the signatory of phase 1, you have to enter the <code>t.wf.step[1].user.extra</code> element, for the signatory of step 2, you have to enter the <code>t.wf.step[2].user.extra</code> element, etc.</p>	<p>Value of the "key" field inserted in the "Additional data" master data of the signatory user.</p> <p>It is necessary to distinguish the case in which the code of an additional data starts with an alphabetic character from where it starts with a numeric character.</p> <p>In the case of an alphabetic character, for example a type code "additionaldata", the attribute must have the name <code>additionaldata:t.wf.step[n].user.extra.additionaldata</code></p> <p>In the case of a numeric character, for example, a type code "1DATAGG", the attribute must have the name <code>["1DATAGG"]</code>: <code>t.wf.step[n].user.extra["1DATAGG"]</code></p> <p>Therefore the attributes are as many as the additional data inserted in the "Additional data" of the user.</p>
m-th signature of the n-th phase	<code>t.wf.step[n].sign[m]</code>	<p>To indicate the information relating to the m-th signature within the n-th phase.</p> <p>For example:</p> <p>if you want to display the signature 1 of phase 1, you have to insert the <code>t.wf.step[1].sign[1]</code> element;</p> <p>if you want to display the signature 2 of phase 1, you have to insert the <code>t.wf.step[1].sign[2]</code> element;</p> <p>if you want to display the signature 1 of phase 2 you have to insert the <code>t.wf.step[2].sign[1]</code> element, etc.</p>	descr type field

Value	Item	Description	Attributes
m-th identity document of the n-th phase user	<code>t.wf.step[n].user.attach[m]</code>	To indicate the information relating to the m-th identity document within the n-th phase. For example: if you want to display the document 1 of phase 1, you have to insert the <code>t.wf.step[1].attach[1]</code> element; if you want to display the document 2 of phase 1, you have to insert the <code>t.wf.step[1].attach[2]</code> element; if you want to display the document 1 of phase 2, you have to insert the <code>t.wf.step[2].attach[1]</code> element, ecc.	descr type docNumber docReleasedFrom docReleaseDate docValidityEndDate filename

Below there is a table showing the complete markers (elements and attributes) usable to create a customized template document.

Value	Marker	Description
Date	<code>\${t.date}</code>	It is the date of the process.
Company description	<code>\${t.company.descr}</code>	It is the company description.
Company VAT number	<code>\${t.company.vatId}</code>	It is the company VAT number.
Company tax code	<code>\${t.company.taxCode}</code>	It is the company tax code.
Reseller description	<code>\${t.reseller.descr}</code>	It is the reseller description.
Reseller VAT number	<code>\${t.reseller.vatId}</code>	It is the reseller VAT number.
Process description	<code>\${t.wf.descr}</code>	It is the signing process description.
n-th phase description	<code>\${t.wf.step[n].descr}</code>	It is the Riporta la descrizione della fase n-esima.
n-th phase signatory's name	<code>\${t.wf.step[n].user.firstName}</code>	It is the name of the signatory user entered in the n-th phase.
n-th phase signatory's surname	<code>\${t.wf.step[n].user.lastName}</code>	It is the surname of the signatory user entered in the n-th phase.
n-th phase signatory's email	<code>\${t.wf.step[n].user.email}</code>	It is the email of the signatory user entered in the n-th phase.

Value	Marker	Description
n-th phase signatory's phone number	<code>\${t.wf.step[n].user.phone}</code>	It is the phone number of the signatory user entered in the n-th phase.
n-th phase signatory's birth date	<code>\${t.wf.step[n].user.birthDate}</code>	It is the birth date of the signatory user entered in the n-th phase.
n-th phase signatory's birth city	<code>\${t.wf.step[n].user.birthCity}</code>	It is the birth city of the signatory user entered in the n-th phase.
n-th phase signatory's birth province	<code>\${t.wf.step[n].user.birthProvince}</code>	It is the birth province of the signatory user entered in the n-th phase.
n-th phase signatory's birth state	<code>\${t.wf.step[n].user.birthCountry}</code>	It is the birth state of the signatory user entered in the n-th phase.
n-th phase signatory's residence address	<code>\${t.wf.step[n].user.address}</code>	It is the residence address of the signatory user entered in the n-th phase.
n-th phase signatory's residence ZIP code	<code>\${t.wf.step[n].user.postalCode}</code>	It is the residence ZIP code of the signatory user entered in the n-th phase.
n-th phase signatory's residence city	<code>\${t.wf.step[n].user.city}</code>	It is the residence city of the signatory user entered in the n-th phase.
n-th phase signatory's residence province	<code>\${t.wf.step[n].user.province}</code>	It is the residence province of the signatory user entered in the n-th phase.
n-th phase signatory's residence state	<code>\${t.wf.step[n].user.country}</code>	It is the residence state of the signatory user entered in the n-th phase.
n-th phase signatory's Tax Code	<code>\${t.wf.step[n].user.taxCode}</code>	It is the Tax Code of the signatory user entered in the n-th phase.
Description of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].descr}</code>	It is the description of the m-th identity document of the signatory user inserted in the n-th phase.
Type of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].type}</code>	It is the type of the m-th identity document of the signatory user inserted in the n-th phase.
Number of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].docNumber}</code>	It is the number of the m-th identity document of the signatory user inserted in the n-th phase.
Body issuing the m-th document of the user identity of the n-th phase	<code>\${t.wf.step[n].user.attach[m].docReleasedFrom}</code>	It is the body issuing the m-th identity document of the signatory user inserted in the n-th phase.
Release date of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].docReleaseDate}</code>	It is the release date of the m-th identity document of the signatory user inserted in the n-th phase.

Value	Marker	Description
Expire date of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].docValidityEndDate}</code>	It is the expire date of the m-th identity document of the signatory user inserted in the n-th phase.
Scan file name of the m-th identity document of the n-th phase signatory	<code>\${t.wf.step[n].user.attach[m].filename}</code>	It is the scan file name of the m-th identity document of the signatory user inserted in the n-th phase.
n-th phase signatory's additional data. They are the "Additional Data" entered in the signatory's personal data. The values are dynamic and correspond to the value entered in it. Suppose that we have the additional data key "additionaldata" for the signatory of the n-th phase.	<code>\${t.wf.step[n].user.extra.additionaldata}</code>	It is the value entered in the signatory's "Additional data" personal data corresponding to the "additionaldata" key field.
m-th signature description of the n-th phase	<code>\${t.wf.step[n].sign[m].descr}</code>	It is the description of the m-th signature within the n-th phase.
m-th signature type of the n-th phase	<code>\${t.wf.step[n].sign[m].type}</code>	It is the type of the m-th signature within the n-th phase.
m-th signature field of the n-th phase	<code>\${t.wf.step[n].sign[m].field}</code>	It is the field of the m-th signature within the n-th phase.

If the "null" field error occurs while uploading the file, you have to correct the marker by inserting ! " " or an if formula. The example below shows the marker Company tax code, in which they are inserted both types of control:

Value	Marker	Marker in case of "null" field
Company tax code	<code>\${t.company.taxCode}</code>	<code>[#if t.company.taxCode?has_content] \${t.company.taxCode} [/#if]</code>
Company tax code	<code>\${t.company.taxCode}</code>	<code>\${t.company.taxCode!""}</code>

To dynamically introduce the **signature fields** on the template, the following construct must be adopted:

```
####SignatureFieldName####
```

To dynamically introduce the **additional data** on the template, the following construct must be adopted:

```
####AdditionalData#type#obb####
```

In the table below, the definitions of the construct, its descriptions and values are shown.

Definition	Description	Value
AdditionalData	Name of the field (equivalent to filling in the "Name" field as described in the paragraph Adding a signature process).	Free imputation.
type	Type of the field	TEX: if it is a text field. NUM: if it is a numeric field. DAT: if it is a date field. DTI: if it is a date and time field. LST: if it is a list field. FLG: if it is a boolean (Yes/NO) field.
obb	It indicates if the field is mandatory (equivalent selecting the "Mandatory" field as described in the paragraph Adding a signature process)	S: to indicate a mandatory field. N: to indicate a non-mandatory field.

If you want to create markers to automatically update the signatory user's master data (in case of AdES agreement template), you have to respect the following construct:

```
####U_XXX####
```

The table below shows the values that "U_XXX" can have with the relative field description:

Value	Description
U_NOM	Signer's name.
U_COG	Signer's surname.
U_CFI	Signer's Tax Code.
U_TEL	Signer's phone number.
U_EMA	Signer's email.
U_DNA	Signer's birth date.
U_CNA	Signer's birth city.
U_PRN	Signer's birth district.
U_PAN	Signer's birth country.
U_IND	Signer's residential address.
U_CRE	Signer's residential city.
U_CAP	Signer's residential postcode.
U_PRR	Signer's residential district.
U_PAR	Signer's residential country.

Value	Description
U_DAT	<p>Signer's additional data. In this case it is possible to indicate the following construct:</p> <pre>####U_DAT_additionaldata####</pre> <p>where additionaldata is the additional data key which is inserted.</p>

To dynamically introduce parameters into the template, the following construct must be used:

```
${t.params.nomeparametro}
```

where **nomeparametro** represents the code of the parameter to be inserted.

The font marker color must be identical to that of the sheet to avoid misalignments between the marker and its content.

Below there is an example of an .ODT template with some markers whose data is just inserted and markers of additional type text fields.

```
The undersigned company    ${t.company.descr}
VAT number                 ${t.company.vatId}

requires employees listed below to sign this document:

employee:                  ${t.work.step[1].user.firstName} ${t.work.step[1].user.lastName}
Tax Code:                  ${t.work.step[1].user.taxCode}
Test description:         ####TestDesc1#TEX#S####
Passed test:               ####OK1#FLG#S####

Signature
####Signature1####

employee:                  ${t.work.step[2].user.firstName} ${t.work.step[2].user.lastName}
Tax Code:                  ${t.work.step[2].user.taxCode}
Test description:         ####TestDesc2#TEX#S####
Passed test:               ####OK2#FLG#S####

Signature
####Signature2####
```

Below is an example of an .ODT template for AdES agreement with markers to automatically create signatory personal data:

```
The undersigned company    ${t.company.descr}
VAT number                 ${t.company.vatId}

requires the data below to accept AdES:

employee:                  ####U_NOM####   ####U_COG####
Tax Code:                  ####U_CFI####
Qualification:             ####U_DAT_QUAL####

Signature
####Signature####
```

6.9.1. Inserting markers on a document

Custom templates are text documents in .docx or .odt format.

The methodology for inserting markers is different: it depends on the writing editor you are using.

Inserting markers with "Libre Office" to create .odt files and with Word to create .docx files is described below

6.9.2. Inserting markers with "Libre Office"

Figure 69. Inserting markers with "Libre Office" menu.

Open the menu **Inserisci** → **Comando di Campo** → **Altri Campi** and click on "Altri Campi". You can also press the Ctrl+F2 function key.

A form opens where you can enter markers.

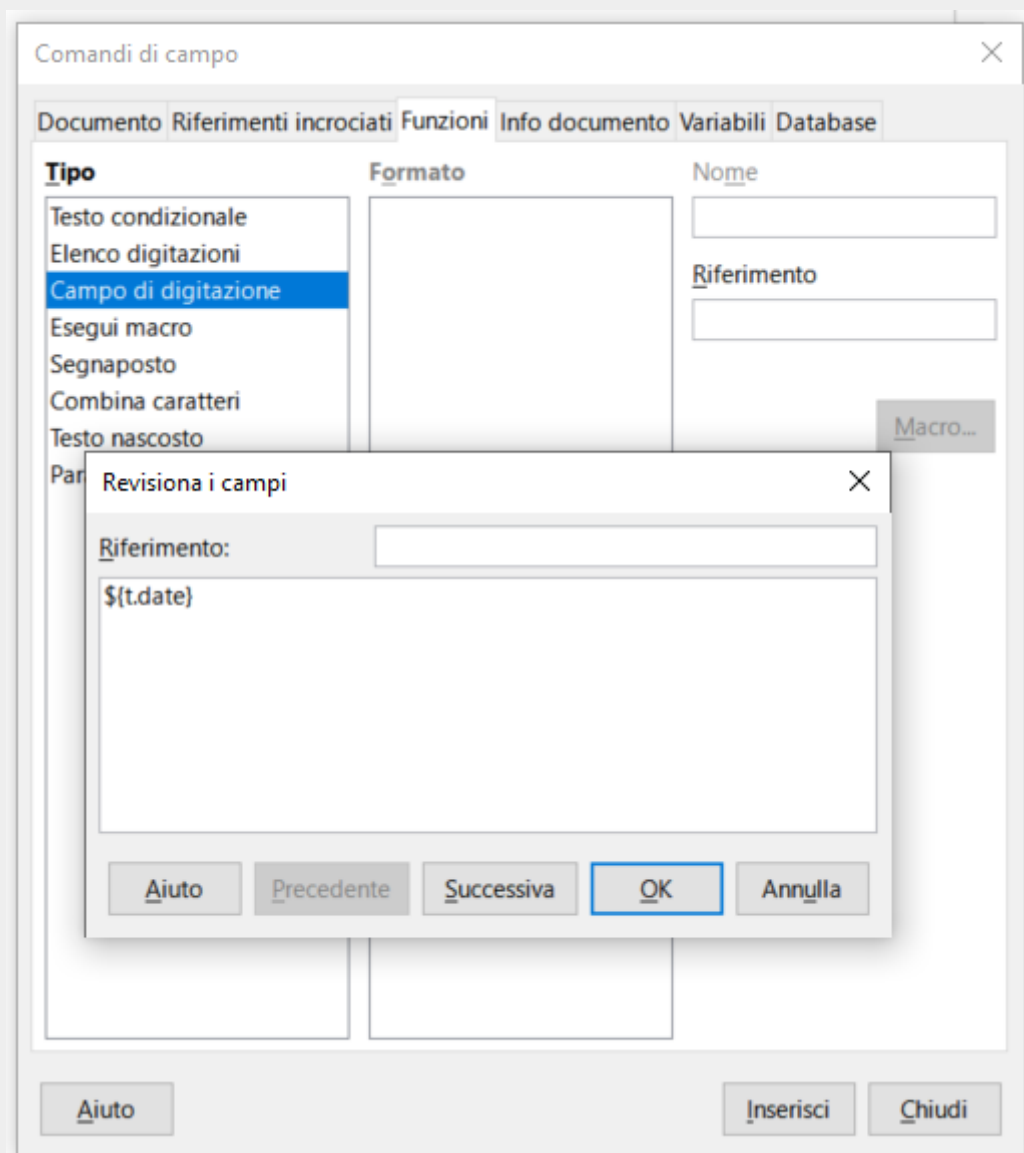


Figure 70. Entering LibreOffice markers.

From this window in the "Functions" section select "Type-in field" as type e click on "Insert".

A form opens where you can enter the name of the marker.

By clicking on "OK" the marker is inserted on the document.

To insert other markers you can:

- do the previously described process again;
- copy and past the marker. In this case, you must pay attention the gray outline is copied too. To change the value you can:

- double-click on the marker. You can change value in the form;
- change the name directly inside the gray field.

6.9.3. Inserting markers with "Word"

Figure 71. Inserting markers with "Word" menu

Open the menu **Inserisci** **Parti Rapide** **Campo** and click on "Campo". You can also press the Ctrl+F2 function key.

A form opens where you can enter markers.

Figure 72. Entering Word markers.

In the "Choose a Field" section, select the "MergeField" item as the Field Name category.

In the "Field Properties" section, in the "Field Name" box, enter the name of the marker and leave all the options unchanged. It is especially important to leave the "Keep the formatting during updates".

By clicking on "OK" the marker is inserted on the document.

To insert other markers you can:

- do the previously described process again;
- copy and past the marker. In this case to change the marker is necessary right-click the field and select Edit Field.

[Back to top.](#)

7. Entaksi Token

There are different types of kits available on the market for applying digital signatures to documents, the most common are smart card readers and token.

To use them, it is necessary to download drivers for hardware recognition and specific software used for applying digital signature.

The smart card reader is a device that must be connected to the PC via USB in which must be inserted a chip card, in "credit card" format, which contains the data of owner and of service provider, as well as the signature certificate.

Tokens (compatible with Windows, Linux and MAC) are USB "pens", similar to common data storage devices, which contains a chip like to the smart card where data of the owner, the service provider and signature certificate are saved. Unlike smart card, these devices do not require a reader as they directly connect to the PC via a USB port.

The signature token chosen by Entaksi Solutions SpA is the model "**SafeNet eToken 5110 CC**", a USB-A device containing the IDPrime 940 chip from Thales Group (formerly Gemalto).

This model has been selected by Entaksi Solutions SpA for use as Qualified Signature/Seal Creation Device that it meets the eIDAS requirements for this purpose.

The model is shown at the [compiled list of devices](#) with the name "Carte IAS Classic en version 4.4.2 avec serveur MOC 1.1 sur plateforme Multiapp v4.0.1" among the certified devices of France, the manufacture's member state.

Regarding the difference between the chip name included in the token (IDPrime 940) and the one listed in the list (Carte IAS Classic en version 4.4.2), the following manufacture's declaration on the change of nomenclature applied in 2018:

<https://m1.entaksi.net/public/tsp/software/IDPrimeProductnames.pdf>

The device certification was obtained from the Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).

The available certification reports are [Certification Report](#) and [Security Target](#)

With these characteristics the device hosts the certificate and the relative private key for the application of qualified signatures with legal validity throughout the European Union.

Through the Entaksi token it is possible to digitally sign documents both through Acrobat (see paragraph [Sign local documents through Acrobat](#)) and through the Entaksi signature application eSIGN Desktop (see paragraph [Signing documents with eSIGN Desktop](#)).

7.1. Management

The Entaksi token must be input into a USB-A port of a Windows, macOS, or Linux computer.

For proper use of the signature device, it is necessary to download and to install the drivers and management software, which depend on the adopted operating system, available at the following links:

- [SafeNet Authentication Client Tools for Linux 10.8 R1](#)
- [SafeNet Authentication Client Tools for Windows 10.8 R8](#)
- [SafeNet Authentication Client Tools for macOS 10.8 R2](#)

The token has four roles, each corresponding to four passwords (or PIN):

- **Role#1 "Token password"**: It is used to perform operations such as writing and deleting keys. It is exclusively used when writing operations need to be performed, for example, during certification renewal.
- **Role#2 "Administrator password"**: It is used to reset the value of the "Token password" and to initialize the device. The device comes with factory default value, that is, a string of 48 zeros. With this password you can reset the value of the "Token password", in case it is forgotten.
- **Role#3 "Digital Signature PIN"**: It is used to authorize electronic signature operations using keys for signature only in the Common Criteria protected zone. It corresponds to the PIN for daily use of the electronic signature and must be inserted whenever you want to affix an electronic signature.
- **Role#4 "Digital Signature PUK"**: It is used to restore the value of "Digital Signature PIN" for device initialization, in case it is forgotten.



ATTENTION: The Digital Signature PIN is invalidated after 3 incorrect insertion attempts and must then be restored using the "Digital Signature PUK".



IMPORTANT: The Digital Signature PUK is invalidated after 3 incorrect insertion attempts and it is **not recoverable** either with the intervention of Entaksi or the device manufacturer. **Invalidating the Digital Signature PUK the token becomes unusable and must be replaced with a new one.**



It is recommended to avoid performing operations to modify these passwords if not setting up an orderly environment, making sure you have the time to record or securely memorize the values you want to set.

7.1.1. Driver and management software installation

For the correct use of the token you need to download and install the drivers and the management software.

The drivers and the software depend on the operating system of your computer, and they are indicated in the previous paragraph [Management](#).

Once you have been downloaded the software and the drivers, you can proceed with their installation by extracting the downloaded folder and following the simple installation workflow.

Click to "Next" on the first introductory screen, choose the language and click "Next", accept the contractual terms and click "Next" again.

The default installation path will be displayed, click "Next" to continue, or change the path if necessary and click "Next".

Choose among the three installation options: the suggested one is Typical, but you can choose the desired one. Once the installation option is set, click "Next", and finally, click "Install".

The software and token drivers will be installed in the previously indicated path, and you can now digitally sign documents with the Entaksi token.

Using the Entaksi token, you can digitally sign your local documents with Acrobat (see [Sign local documents through Acrobat](#)) or through the eSIGN Desktop application (see [eSIGN Desktop](#)).

7.2. Sign local documents through Acrobat

Using the Entaksi token, you can digitally sign your documents through Acrobat with just a few simple steps.

After connecting the token to your computer, open the document you want to sign with Acrobat, in the left side menu click on "Visualizza più" ("View more"): an additional menu will appear. By clicking on the "Utilizza certificato" ("Use certificate") option and then on the submenu "Firma digitalmente" ("Digitally sign"), you can start the configuration process for signing.

By clicking and holding down the left mouse button, you can define the area where you want to place the signature: once this operation is completed, you can proceed to the next phase of the signature process.

If multiple certificates are available on your computer, select the option to sign with the certificate issued by Entaksi.

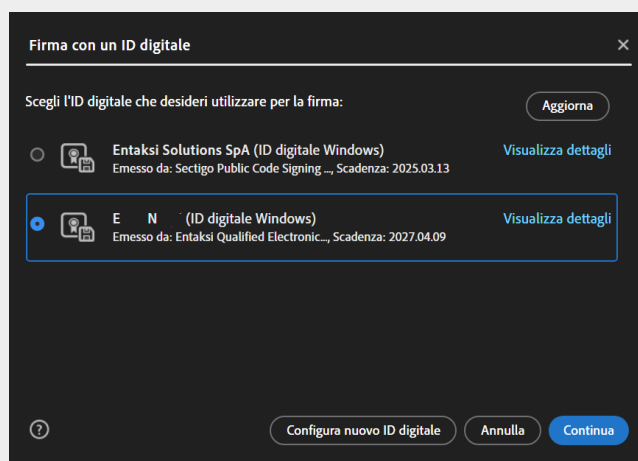


Figure 73. Select certificate.

You will see how the signature appears on document after it's been applied. From this screen, you can modify the appearance to the standard one proposed, view the certificate details and lock the document after signing.

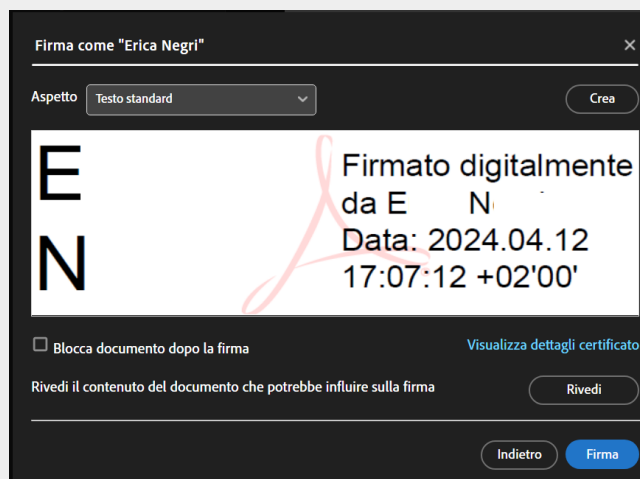


Figure 74. Signature creation.

By clicking the "Crea" ("Create") located at the bottom right, you will be prompted to enter the PIN code received with the token.

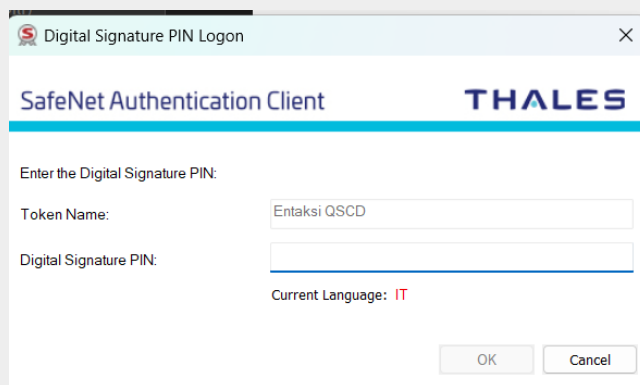


Figure 75. Enter PIN.

By entering the PIN code and clicking the "OK" button at the bottom right, the document will be successfully signed.

8. eSIGN Desktop

In order to affix the qualified electronic signature (or digital signature) on documents in a eSIGN signing process, you must install the Entaksi application "**eSIGN Desktop**" and have the smart card and related device.

The download is available in the "**eSIGN Desktop**" section, where you can download both the application and the drivers to install for the correct smart card operation.

The software is available for Windows, macOS and Linux environments.



Figure 76. Operating systems

Once the operating system has been found, you have to select the relevant item.

On the page below you will find all the instructions necessary to download the application and drivers for the smart card.

In order to download "eSIGN Desktop", click on "**Download eSIGN Desktop**" button. Once the package has been downloaded, it will be possible to install it following the instructions in the [eSIGN Desktop Installation](#) paragraph.

In order to download the smart card drivers, you will first need to locate your smart card type by choosing from the options shown (ATHENA card, card Oberthur / IDEMIA, card STMicro).

Once the type of card has been identified, you can click on the link of the driver and download it.


To install the downloaded driver, you have to unzip the folder and to click on the "Setup file". It will be possible to continue with the installation following the wizard instructions.

8.1. eSIGN Desktop Installation

Once the "eSIGN Desktop" software has been downloaded, it will be possible to proceed with its installation by clicking on the executable file you just downloaded.

A wizard will be opened. By clicking on the left bottom buttons you can print and download the user licence. With the right bottom buttons it will be possible to refuse the license (in this case the installation wizard will close) or to accept it continuing with the installation.

The program's default destination is displayed, and you can modify it.

Once the installation is finished, the management icon  will display, and by clicking it, the program will start automatically.

When the application is launched, two main menus, "File" and "Help" will be displayed in the top right corner, whose main features are outlined in the following sections.

By connecting the signing device, whether it's a token or a smart card, it will be possible to digitally sign documents saved locally or those started through the eSIGN service (see [Signing documents with eSIGN Desktop](#)) Simply by connecting to the service itself (see [Connecting eSIGN Desktop to the eSIGN service](#)).

8.2. File Menu

In the top left corner, there is the 'File' menu, which contains the following options.

Clicking "Quit" (the last option) will close the application.

8.2.1. Verify

In this section you can check the correctness of the signatures affixed to a file.

The libraries used by the application to perform the check are the same as those used by the DSS and, consequently, the results will be in accordance with those reported on the page of verification signatures [verify signature](#) of the European Commission.

By clicking on the "Select file" button in the top left corner you can choose the file that you want to check.

Once the file is uploaded, the system will start the scanning procedure.

As a first step, the Trusted Lists (TLS) will be updated if they have not been updated for more than 24 hours and will be saved in the ".entaksi/cache/tls" folder in the home directory of your device.

Then the DSS validation procedure will start, which uses a cache for the Certificate Revocation List (CRL) that is saved in the ".entaksi/cache/crl" folder in the home of your device. Once the verification process is complete, the results will be reported in the four sections described below.

Simple Report

This section, divided into three additional subsections, displays the validation policy and general information about the document. In the central part, along with the main information about the signature (such as signature format, date, and time), the compliance status of the verified signature is also shown.

For this check, you can download a document in either .pdf or .xml format by clicking the respective buttons located at the bottom right, which contain the same information presented in the section.

Detailed Report

This section lists all the steps taken to verify the signature.

For each check performed, the outcome is reported, and for each step of the check, any relevant icons indicating a successful, warning, or failed check are displayed.

For this type of report as well, you can download a document in .pdf or .xml format by simply clicking the respective buttons located at the bottom right.

Diagnostic Data

This section reports the diagnostic results, which are available exclusively in .xml format.

To download the document, click the corresponding button located at the bottom right.

ETSI Validation Report

This section reports the result of the ETSI validation, which is available exclusively in .xml format.

To download the document, click the corresponding button located at the bottom right.

8.2.2. Connect to the Registration Authority

Clicking on this option will open a connection form for the Registration Authority.

By clicking "**Connect**" a page will open from which you can, by entering your credentials, access the Registration Authority.

8.2.3. Settings

Clicking this option will open a new form where you can enter settings for a customized use of the application.

The form is divided into the following sections.

General

This section displays the last update of the Trusted Lists (TLS).

By clicking the "**Start TLS Update**" button, you will manually force an update of the Trusted Lists in the ".entaksi/cache/tls" folder in your device's home directory (instead of automatically as indicated in [Verify](#)).

Clicking the "**Clear CRL Cache**" button will delete all items in the Certificate Revocation List (CRL) in the ".entaksi/cache/crl" folder in your device's home directory.

Custom Stamp

In this section, it is possible to customize the signature that will be applied to a .pdf file using the visible local signing method.

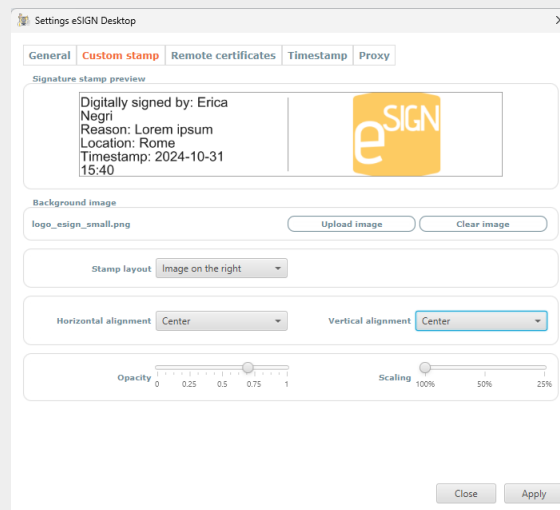


Figure 77. Custom Stamp.

At the top, a preview of the stamp, that is the signature, is available, which will be applied to the document using the visible local signing method: any changes made to the stamp are displayed in this section.

By clicking the **Select image** button, you can choose an image that will be applied to the signature. Only if an image has been selected will the following options be enabled:

- **Stamp layout.** With this option, you can choose the position of the image relative to the descriptive information of the stamp by selecting one of the three options available in the list:
 - Text overlay: the text overlaps the image, which will appear in the background;
 - Image on the right: the image is placed to the left of the text, with a vertical line displayed as a divider between the text and the image;
 - Image on the left: the image is placed to the left of the text, with a vertical line displayed as a divider between the text and the image.
- **Horizontal alignment - Vertical alignment.** The user can decide the horizontal or vertical alignment of the image relative to the previously set layout. The available options are listed as follows: Center, Right, Left for horizontal alignment; Center, Above, Below for vertical alignment

- **Opacity.** Adjust the transparency of the selected image: by moving the gradient slider to the right or left, the image will become more or less opaque.
- **Scaling.** Adjust the size of the selected image: by moving the gradient slider to the left or right, the image will be respectively decreased or increased in size.

By clicking the **"Remove Image"** button, the previously uploaded image will be removed, and the options below will be disabled.

Remote Certificates

By clicking the **"Log In"** button, after logging in with your credentials, a page will open displaying the available remote certificates.

If no remote certificates are available for the user, a message indicating their unavailability will be shown, from which you can access the Entaksi website to request additional certificates.

Timestamp

In this section, you can configure the data for using a timestamp and its authentication.

To enable the use of time stamp, you need to check "Use timestamp service" checkbox located at the top left and define the timestamp provider (Entaksi or another service) by selecting one of the two options available in the list.

If the chosen service is Entaksi, it is necessary to enter the "Username" and "Password" (mandatory fields) and, optionally, fill in the "Policy Oid" field.

If another service is selected, it is necessary to fill in the "Service URL" field (mandatory) and, optionally, the "Policy Oid", "Username", and "Password" fields (for third-parties services, credentials are not mandatory).

Proxy

In this section, you can enable the connection to a proxy server and its authentication by simply checking the relevant options and entering the required data.

In the bottom right, by clicking the **"Apply"** button, all changes made will be saved, clicking the **"Close"** button the changes made will not be saved.

8.3. Help menu

In the top left corner, next to the File menu, there is the **"Help"** menu, which contains the following options.


User Manual

Clicking this option will open a page from which you can download the User Manual for the eSIGN service, which includes a chapter dedicated to the proper use of the eSIGN Desktop application.

About

Clicking this option will open a panel that provides general information about the eSIGN Desktop application and Entaksi's contact details for any needs.

8.4. Launch eSIGN Desktop

In order to apply a digital signature to any type of document, it is necessary to connect your signing device to the computer and launch eSIGN Desktop by clicking the icon  on your computer after installing the software (see the [eSIGN Desktop Installation](#)).

If the signed device is connected and recognized correctly, the screen of connected device will be displayed.



Figure 78. Connected device.


If the device has not been previously connected, the application will notify its absence. Without closing the application, you can connect the device to your computer, and it will be automatically detected, displaying the connection screen.

The connection screen displays the following information:

- the first name, last name, and tax code of the user holding the certificate;
- the Certification Authority that issued the certificate;
- the certificate's start validity date;
- the certificate's end validity date.

To the left of the information about the certificate holder user there are images indicating both the type of certificate (signature, seal, or authentication) and the issuing Certification Authority (Entaksi or third-parties).

Image	Description
	The certificate on the device is a "signature" type, and the issuing Certification Authority is Entaksi Solutions SpA - Irish Branch.
	The certificate on the device is "signature" type, and the issuing Certification Authority is a third-parties CA.
	The certificate on the device is "seal" type, and the issuing Certification Authority is Entaksi Solutions SpA - Irish Branch.
	The certificate on the device is "seal" type, and the issuing Certification Authority is a third-party CA.
	The certificate on the device is "authentication" type for websites, and the issuing Certification Authority is Entaksi Solutions SpA - Irish Branch.
	The certificate on the device is "authentication" type for websites, and the issuing Certification Authority is a third-parties CA.

Image	Description
	The certificate on the device is an unknown type, meaning it is not recognized as any of the three types listed above.

8.5. Connecting eSIGN Desktop to the eSIGN service

In order to apply the digital signature to documents initiated through the eSIGN service (not locally saved documents), it is necessary to connect eSIGN Desktop to the eSIGN service by clicking the "**Connect to eSIGN**" button: a request will be initiated, and the "**Connection in progress**" screen will appear.

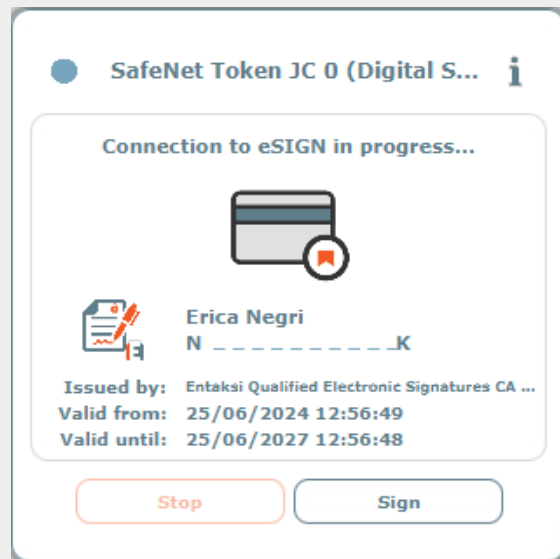


Figure 79. Connection in progress.

Clicking the **"Stop"** button will interrupt the attempt to connect to the eSIGN service.

To proceed with the connection request, you must accept the terms and conditions of use. By checking the acceptance box and clicking the **"OK"** button, the connection request will continue, clicking the **"Cancel"** button will interrupt the process. Once the terms of use are accepted, you will need to enter the device PIN, and by clicking **"Apply"**, the connection request is started. Clicking **"Cancel"** will interrupt the process.

When the application is successfully connected to the eSIGN service, the "**Connection successful**" screen will appear

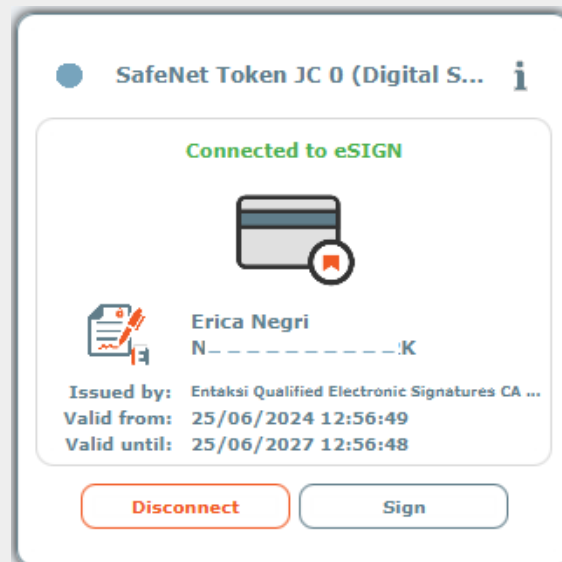



Figure 80. Connection successful.

8.6. Signing documents with eSIGN Desktop

8.6.1. Documents present in eSIGN service signature processes

When the application is connected it is possible to digitally sign the documents inserted within a signature process. In fact, by accessing the signature pages, the section dedicated to the connection with eSIGN Desktop will be active and it will be possible to affix the signature by confirming the OTP code as indicated in the paragraph [Signature pages](#)

By clicking on the  icon, the list of documents signed by the smart card during the connection will be displayed. This list will appear on the right of the connection screen session with eSIGN.

The details shown are:

- **smart card**: it shows the generic information of the smart card connected to the system.
- **data (date)**: it shows the date and time of the signature.
- **tipo firma (signature type)**: it shows the signature type of the document.
- **motivo firma (Reason for signature)**: it shows information relating to the reason for which the signature was requested.
- **documento (document)**: it shows the name of the signed document

All columns can be sorted: by clicking on the column header it will be possible to sort data in ascending or descending order.

By clicking on  it will be possible view the signed document.

8.6.2. Local documents

It is possible to sign with any signature device adopted with eSIGN Desktop, even local documents, that is saved on your computer, by signing like:

- **PAdES (PDF Advanced Electronic Signature)**: the signature can be **exclusively** affixed to documents in .pdf format, allowing the document to retain its name, format, and extension even after the electronic signature is applied.

The validity of the PAdES signature will be immediately readable with the most common PDF readers available for free on the market.

When the signed PAdES file is opened through the reader, a horizontal bar containing the specifications of the signatures applied to the document will appear, and their details will be visible by clicking on the "Signature Panel" option.

- **CAAdES (Cryptographic Message Syntax Advanced Electronic Signature)**: the signature can be affixed to any type of document, in any format.

In the case of a digital signature in CAAdES mode, the original document and the signed document are enclosed in an envelope, which is a new file with the extension .p7m.

Therefore, all digitally signed files in this mode have a secondary .p7m extension. For this reason, electronically signed files

in CAdES format can only be read and recognized with specific software.

- **XAdES** (XML Advanced Electronic Signatures): the signature can be affixed to .xml files. Since there is no enveloping phase, it is possible to access the data contained within the file even after the signature is applied.

For each of the signature types mentioned above, it is also possible to select a signature profile.

The available signature profiles are:

- **BASELINE-B**: basic electronic signature.
- **BASELINE-T**: joins *BASELINE-B*, for which a Trust Service Provider has generated a reliable token (time-mark or time-stamp token) to verify that the signature indeed existed at a specific date and time.
- **BASELINE-LT**: joins *BASELINE-T* signatures with a long-term validation attribute containing certificate values and certificate revocation status values used to validate the signature.
- **BASELINE-LTA**: joins *BASELINE-LT* signatures with one or more long-term validation attributes to prevent the signature from being compromised due to weakening algorithms during extended preservation periods.

After starting the eSIGN Desktop application, on the screen indicating the correct connection of the signing device, whether it is a token or a smart card, click the **"Sign"** button located at the bottom right: a dialog mask for signing local documents will appear.

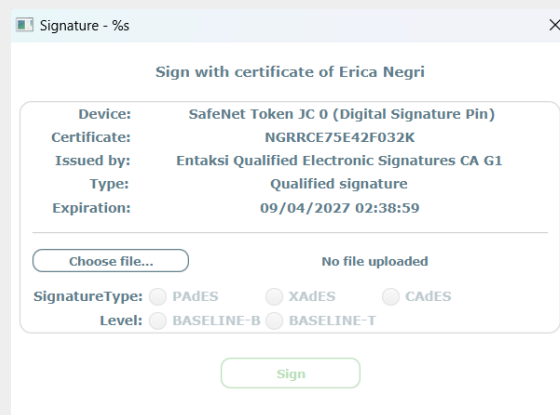


Figure 81. Sign documents locally.

The dialog mask is divided into two sections: the upper part displays all the information related to the signing device and the certificate used; the lower part shows the settings for the correct application of signatures.

By clicking the **"Select file..."** button, a search dialog mask will appear from which it is possible to select the file on which you want to apply the digital signature.

The types of signatures that can be applied will be enabled according to the extension of the selected file: for example, if a .pdf file is selected, the PAdES and CAdES signatures will be enabled; if an .xml file is selected, the XAdES and CAdES options will be enabled.

Once you have selected the type of signature you wish to apply, choose the signature profile: by default, the *BASELINE-B* profile is selected. If you have not enabled the "Timestamp" section of the "Settings" menu (see [Settings](#)), only the *BASELINE-B* profile will be enabled.

You can also add additional information that will be shown on the signature of the document: **"Reason for signature"** which can be enhanced even on multiple lines with a maximum length of 300 characters, and **"Location"** with a maximum length of 200 characters.

These two information are optional: they will be displayed on the signature only if provided.

Visible signature

This type of signature is available **exclusively** for PAdES signatures, i.e., for .pdf documents, by checking the **"Visible Signature"** option.

Clicking the **"Sign"** button will open a new form where you can view the document to be signed.

By clicking on the document at the exact point where you wish to place the signature, a yellow field will be created to help visualize where the signature will be applied.

Click **"Apply"** to confirm the placement and proceed with the signing.

You will be prompted to enter the device PIN, and then a form will open for saving the signed file: by default, it will open in the same folder as the previously selected file to be signed.

Click **"Save"** to save the signed file to your computer.

No-visible signature

This type of signature is automatically applied for *CAdES* and *XAdES*, while for *PAdES*, simply do not select the 'Visible Signature' option.

In this case, the document will be properly signed, but the position of the signature cannot be chosen by the signatory user. Once the desired signature type is selected, click the **"Sign"** button at the bottom.

You will be prompted to enter the device PIN, and then a form will open for saving the signed file: by default, it will open in the same folder as the previously selected file to be signed.

Click **"Save"** to save the signed file to your computer.


9. Entaksi app

As described in the [Signing process workflow](#) paragraph, in order to sign documents in a eSIGN signing processes, you can either request an OTP verification code or use the Entaksi app.

The purpose of this chapter is to walk you through the app installation process and how to use it.

9.1. Installing Entaksi app

To install the Entaksi app scan the QR Code that appears on the signature request page.

The QR Code links directly to the store to proceed with the download and then the installation. Alternatively enter the store and search for "Entaksi Solutions SpA" e cliccare sull'app con icona .

After downloading, entering the app two illustrative slides are displayed, click on **"Next"** and **"Login"** respectively. The app login page has the same functions as that of the Console described in [Entaksi Console registration procedure](#).

Enter email and password and click **"Login"**.

The service simultaneously sends a verification code via SMS to the telephone number indicated in the registry of signatories of eSIGN.

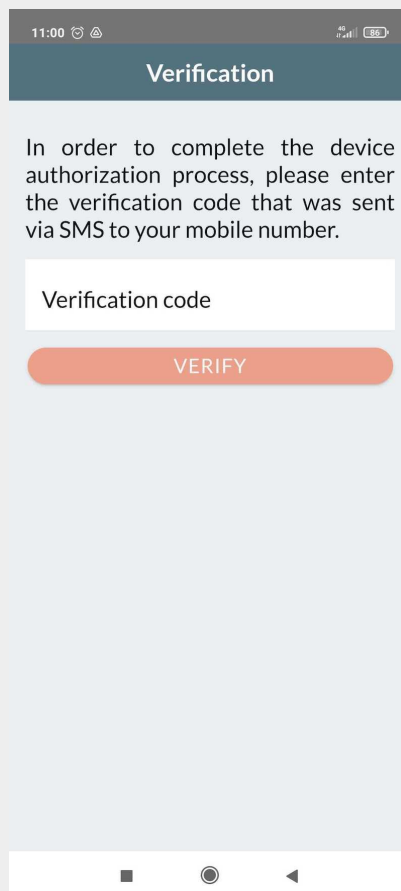


Figure 82. Verification code.

Enter the code and click on "**Verify**".

In order to complete the configuration, it is necessary to enter a personal six-digit code which allows to authorize both future accesses to the app and signatures.

If the device is equipped with biometric recognition, it is possible to use it instead of the Entaksi code.

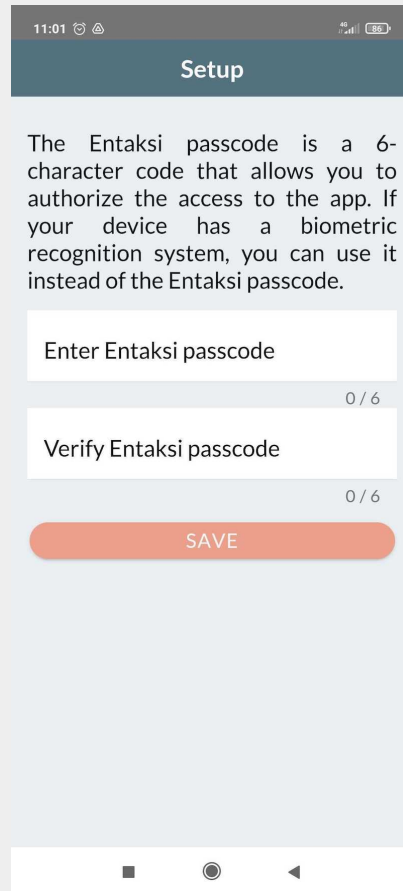
The screenshot shows a mobile app setup screen titled "Setup". It contains a text block explaining the Entaksi passcode: "The Entaksi passcode is a 6-character code that allows you to authorize the access to the app. If your device has a biometric recognition system, you can use it instead of the Entaksi passcode." Below this are two input fields: "Enter Entaksi passcode" and "Verify Entaksi passcode", both with a "0 / 6" character count. A red "SAVE" button is positioned below the verification field. The screen is framed by a light gray border, and the bottom of the phone screen shows standard Android navigation icons.

Figure 83. Entaksi code.

By clicking on "**Save**", the Entaksi personal code is recorded and the configuration is completed and the app access form is displayed.

If the user verification has failed, a screen will be displayed indicating the status of the verification.




Figure 84. User verification in progress.

If you have entered incorrect credentials, for example the email indicated during registration does not coincide with the email entered in the user's personal data, you must re-register from the login page by a logout from the current page.

To do this, click on **"Not you?"** and then **"Confirm"**. The first page will be opened again from where, clicking on the **"Next"** button you can log in again as previously indicated.

9.2. App access and signing documents

To access the signature app, click on the app icon  on the device.

The app access form is displayed.

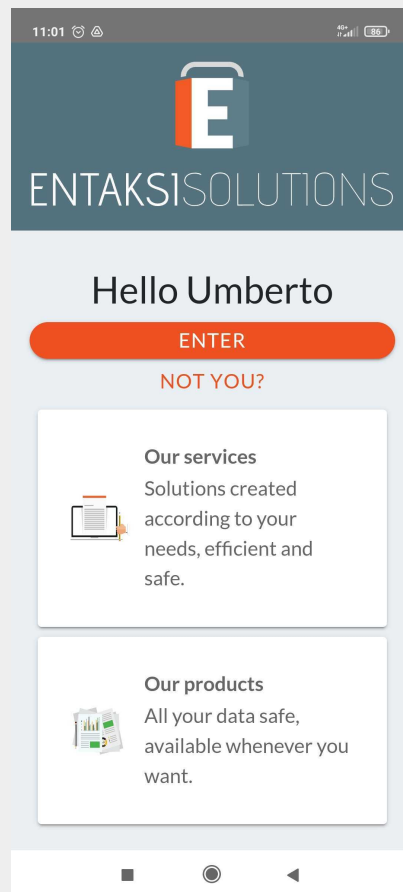


Figure 85. Access the app.

By clicking the central buttons, the Entaksi's site pages relating to the services and products are opened.
By clicking on the "Enter" button, the Entaksi code entered during the configuration phase of the app is requested.
By entering this code and confirming it, the app displays the list of signature requests not yet authorized.
By clicking on the requests, the list of signatures to be authorized in the request is displayed.

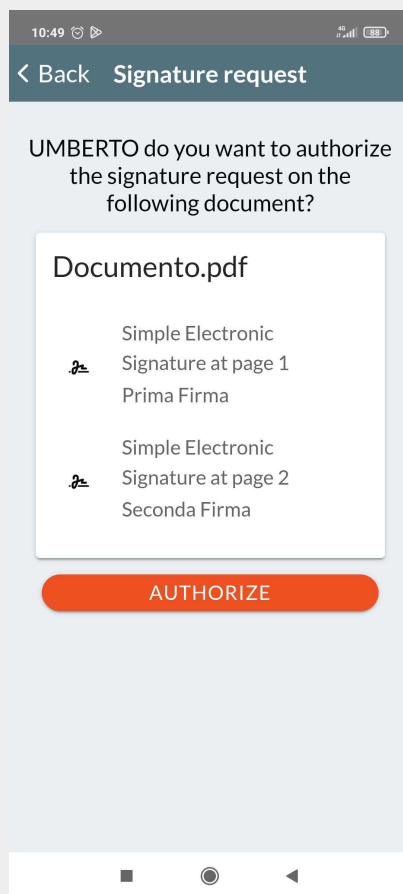


Figure 86. List of signatures to be authorized.

By clicking on the "Authorize" button, the six-digit personal code is requested again. By confirming it, the signatures in the list are all authorized and the document is signed

10. Terminology

The terminology used in the manual is shown below, divided between the glossary of technical terms and acronyms.

10.1. Glossary

Access

It is an operation that allows you to view IT documents.

Reliability

In reference to a document management or preservation system, it expresses the level of trust that the user places in the system itself. In reference to the IT document it expresses the credibility and accuracy of the representation of acts and facts in it contained.

Computerized document aggregation

Set of IT documents or set of IT files grouped by homogeneous characteristics, concerning the nature and form of the documents or the object or the functions of the entity.

Archive

Set of documents produced or acquired by a public or private entity during the carrying out its business.

IT archive

Archive made up of IT documents, organized in IT documentary aggregations.

Homogeneous Organizational Area

In accordance with the provisions of art. 50 paragraph 4 of the Presidential Decree December 28 2000, n. 445, it is a set of functions and offices identified by the institution in order to manage documents in a manner unitary and coordinated. It represents the official channel for submitting applications and initiating proceedings administrative.

Certification of conformity concerning image copies of an analogue document on IT support

Declaration issued by a notary or another public official authorized thereto that is attached or sworn to the IT document.

Authenticity

Characteristic for which an object must be considered as corresponding to what it was in the original moment of its production. Therefore an object is authentic if, in the course of time or space, it has not undergone any unauthorized changes. Authenticity is assessed on the basis of precise evidence.

Certification

Third party attestation relating to compliance with specified product requirements, processes, people and systems.

Classification

Organization of all documents according to a scheme consisting of a set of items articulated in a hierarchical way and which identify the functions, skills, activities and/or materials of the producer in an abstract way.

Cloud of the PA

Virtual environment that allows Public Administrations to provide digital services to citizens and businesses in compliance with minimum safety and reliability requirements.

Codec

Encoding and decoding algorithm that allows to generate binary streams, possibly envelop them in a file or wrapper (encoding), as well as extracting them from it (decoding).

Conservative

Public or private entity that carries out the preservation of IT documents.

Preservation

Set of activities aimed to define and implement overall policies of the preservation system and to govern its management in relation to the organizational model adopted, guaranteeing the characteristics of authenticity, integrity, legibility, availability of documents over time.

File naming conventions

Set of syntactic rules that defines the name of files within a filesystem or package.

Document Management Coordinator

Person responsible for defining uniform classification and archiving criteria as well as internal communication between the AOOs pursuant to the provisions of Article 50, paragraph 4 of Presidential Decree 445/2000 in cases of administrations that have set up more AOOs.

Recipient

Person or system to which the IT document is addressed.

Digest

See Cryptographic Fingerprint.

IT administrative document

Any type of representation, graphic, photographic, electromagnetic or any other especially the content of documents, including internal ones, formed by public administrations, or, in any case, used by the latter for administrative purposes.

Electronic document

Any content stored in electronic form, in particular text or audio, visual or audiovisual registration.

IT document

Electronic document that contains the IT representation of acts, facts or data legally relevant.

IT duplicate

See art. 1, paragraph 1, lett) i quinquies of the CAD: "the IT document obtained through the storage, on the same device or on different devices, of the same sequence of binary values of the original document".

eSeal

See electronic seal.

Exhibition

Operation that allows you to view a stored document.

eSignature

See electronic signature.

Computer document extract

Part of the document taken from the original document.

Abstract for summary of electronic document

Document in which facts, conditions or qualities inferred from IT documents are attested in a synthetic manner

Static data extraction

Extraction of useful information from large amounts of data (e.g. databases, data warehouse etc ...), through automatic or semi-automatic methods.

IT evidence

Finite sequence of bits that can be processed by a computer procedure.

IT file

Structured and uniquely identified IT document aggregation containing deeds, documents or IT data produced and functional to the exercise of an activity or carrying out a specific procedure.

File

Set of logically related information, data or commands, collected under a single name e recorded in the memory of a computer by means of a processing or writing program.

File container

See container format.

File wrapper

See container format.

Manifest file

File that contains metadata referring to a file or a package of files.

Filesystem

A structured file management system through one or more tree hierarchies, which determines the methods of assigning names, storing and organizing within a storage.

Electronic signature

See article 3 of the eIDAS Regulation: "data in electronic form, attached or connected through logical association with other electronic data and used by the signatory to sign "

Advanced electronic signature

See Articles 3 and 26 of the eIDAS Regulation: "An advanced electronic signature satisfies the following requirements: a) it is connected only to the signatory; b) it is suitable for identifying the signatory; c) it is created from data for creating an electronic signature that the signer can use under your own exclusive control with a high level of security; d) it is connected to the signed data in order to allow the identification of any subsequent changes to them data."

Qualified electronic signature

See article 3 of the eIDAS Regulation: "an advanced electronic signature created by a device for the creation of a qualified electronic signature based on a qualified certificate for electronic signatures".

Flow (binary)

Sequence of bits produced in a finite and continuous time interval that has a precise origin but whose moment of interruption may not be predetermined.

Container format

File format designed to allow for inclusion ("enveloping" or wrapping) of one or more IT records subject to different types of encoding in one same file and to which specific metadata can be associated.

Format of the IT document

Type of representation of the sequence of bits that make up the IT document; it is commonly identified by the file extension.

"Deprecated" format

Formerly considered official format whose use is currently not recommended in favor of a latest version.

Additional functions of the IT protocol

In the computer protocol system, they are additional components compared to the minimum ones, that are necessary for the management of document flows, for the preservation of documents as well as for the accessibility of information.

Minimum functions of the computer protocol

Components of the computer protocol system that meet the requirements of operations and minimum information referred to in Article 56 of Presidential Decree 28 December 2000, n. 445.

Cryptographic hash function

Mathematical function that generates a cryptographic fingerprint starting or digest (see) from computer evidence in such a way that it is computationally difficult (in fact impossible) reconstruct the original computer evidence, starting from this, and generate identical footprints a starting from different computer evidence.

Document management

Process aimed at the efficient and systematic control of production, reception, holding, use, selection and storage of documents.

hash

English term used, improperly, as a synonym for the use of "cryptographic fingerprint" or "digest" (see).

Unique identifier

Sequence of numbers or alphanumeric characters associated in a unique and persistent way to an entity within a specific scope of application.

Cryptographic fingerprint

Sequence of bits of predefined length, the result of applying a cryptographic hash function to an IT evidence.

Integrity

Characteristic of an IT document or of a document aggregation through which it appears that they have not undergone any unauthorized alteration in time and space. The characteristic of integrity, together with that of completeness, helps to determine the characteristic of authenticity.

Interoperability

Characteristic of an information system, whose interfaces are public and open and capable to interact in an automatically way with other information systems, for the exchange of information and the provision of services.

Readability

Characteristic of an IT document that guarantees the quality of being able to be decoded and interpreted by a computer application.

Digital preservation manual

IT document that describes the preservation system and illustrates in detail the organization, the persons involved and the roles performed by them, the model of operation, the description of the process, the description of the architectures and of the infrastructure.

Management manual

IT document that describes the management system of IT documents, also for preservation purposes, and provides instructions for the correct functioning of the service for the maintenance of the IT protocol, the management of document flows and archives.

Metadata

Data associated with an IT document, an IT file or a document aggregation in order to identify them describing their context, their content and their structure - so as to allow time management - in compliance with what is defined in the ISO 15489-1: 2016 standard and more specifically by the ISO 23081-1: 2017 standard.

Preservation object

Digital object poured into a preservation system.

Digital object

Digital information object, which can take various forms including those of a IT document, IT file, IT document aggregation or IT archive.

Archival package

Information package generated by the transformation of one or more payment packages consistently with the methods indicated in the digital preservation manual.

Dissemination package

Information packet sent by the storage system to the user in response to his request to access to the preserved objects.

File package

Finite set of multiple files (possibly organized in a subtree structure within a filesystem) which collectively as well as individually constitute a unitary and self-consistent information content.

Submission package

Information packet sent by the producer to the storage system according to the format described in the digital preservation manual.

Information package

Logical container that holds one or more preserved objects with their metadata, or even only the metadata referring to the preserved objects.

Pathname

Ordered concatenation of a file's path and its name.

Path

Information relating to the virtual location of the file within the filesystem which is expressed as an ordered concatenation of the name of the path nodes.

Preserved system security plan

In the context of the general safety plan, it is a document which describes and plans the activities aimed to protect the IT document storage system from possible risks.

Security plan of the IT management system of documents

In the context of the general safety plan, it is a document which describes and plans the activities aimed to protect the IT document management system from possible risks.

Classification plan (Titolaro)

Logical structure that allows you to organize documents and digital objects according to a scheme derived from the functions and activities of the concerned administration .

Preservation plan

Document attached to the management manual and integrated with the classification system. In this document, the criteria for organizing the archive, for periodic selection and for preservation are defined, pursuant to Article 68 of Presidential Decree 28 December 2000, n. 445.

Organization plan of document aggregations

Tool integrated with the classification system starting from the lower hierarchical levels of the latter and aimed at identifying the types of documentary aggregations (types series and types of dossiers) that must be produced and managed in relation to procedures and activities in which the functions performed by the entity are declined.

General safety plan

Document that plans the activities aimed at creating the protection system and all of them the possible actions indicated by risk management within the organization of membership.

Taking charge

Acceptance of a payment package by the storage system as in accordance with the procedures set out in the digital preservation manual and, in the case of assignment of the external service, by the agreements entered into between the owner of the preserved object and the manager of the preservation service.

Process

Set of interrelated or interacting activities that transform input elements into exit elements.

Producer of SIP

Natural person, usually different from the person who formed the document, who produces the submission package and who is responsible for transferring its contents to the system of storage. In public administrations, this figure is identified with the person in charge of document management.

qSeal

Qualified electronic seal, as per art. 35 of the eIDAS Regulation.

qSignature

Qualified electronic signature, as per art. 25 of the eIDAS Regulation.

Submission report

IT document certifying that the system has taken charge of storage of submission packages sent by the producer.

Protocol register

IT register where all the information required by law are stored for all documents received and sent by an entity and for all IT documents of the entity same.

Particular register

IT register identified by a public administration in order to store information relating documents subject to a special registration.

eIDAS regulation

electronic IDentification Authentication and Signature, Regulation (EU) N° 910/2014 of 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 the directive 1999/93 / EC.

Repertoire

Register on which the files are noted with a progressive number according to the chronological order in which they are formed within the subdivisions of the classification plan.

Manager for information systems for preservation

Person who coordinates the information systems within the conservative.

Head of the preservation service

Person who coordinates the preservation process within the conservator, in accordance with the requirements defined by AgID in the "Regulation on the criteria for the provision of IT document retention services"

Preservation Manager

Person who defines and implements the overall policies of the preservation system and governs its management with full responsibility and autonomy, in compliance with the requirements defined by AgID in the "Guidelines on training, management and storage of electronic documents "

Manager of the archival function of preservation

Person who coordinates the preservation process from an archival point of view within of the registrar, in compliance with the requirements defined by AgID in the "Regulation on the criteria for the supply of IT document storage services "

Responsible for document management

Person who is responsible for the management of the document system or for the service or the keeping the IT protocol, the management of document flows and the archives, pursuant to Article 61 of Presidential Decree 28 December 2000, n. 445.

Data protection manager

Person with specialist knowledge of legislation and practices relating to the protection of data, who is able to perform the tasks referred to in Article 39 of Regulation (EU) 2016/679.

Manager of the safety of preservation systems

Person who ensures compliance with the security requirements within the conservator.

Manager of the development and maintenance of the preservation system

Person who ensures the development and maintenance of the system within the conservator.

Time reference

Data set that represents a date and time with reference to Coordinated Universal Time (UTC).

Transfer

Procedure by which one or more IT documents are converted from a file format (envelope, or package of files) to another, leaving the content unchanged as far as possible by the technical characteristics of the format (or formats) of files and of the target files and encodings.

Reject

In accordance with the provisions of the law in force, it is the operation with which the documents that are deemed no longer relevant for juridical-administrative and historical-cultural purposes are definitively eliminated

Series

Grouping of documents with homogeneous characteristics (see also document aggregation Informatics).

Sidecar (file)

See Manifest File.

Electronic seal

Data in electronic format, enclosed or connected by logical association to other data in electronic form, to ensure the origin and integrity of the latter.

Preservation system

Set of rules, procedures and technologies that ensure the preservation of IT documents in implementation of the provisions of art. 44, paragraph 1, of the CAD.

IT document management system

Set of computing resources, equipment, communication networks and procedures information technology used by organizations for document management. As part of the public administration is the system referred to in Article 52 of the Presidential Decree 28 December 2000, n. 445

Timeline

Virtual timeline on which events relating to an information system or to a IT document are arranged. Two very different examples of timeline are a file of system's log, a multimedia stream containing synchronized audio/video essences.

Owner of the object to be preserved

Producer of the objects to be preserved.

Transfer

Transfer of custody of documents from one person or entity to another person or entity.

TUDA

Consolidated Administrative Documentation, Decree of the President of the Republic 28 December 2000, n. 445, and subsequent amendments and additions.

Office

It is referring to a homogeneous organizational area, an office in the same area that uses the services made available by the IT protocol system.

User enabled

Person, entity or system that interacts with the services of an IT management system documents and/or a system for storing electronic documents, in order to use information of interest.

Submission

Transfer of custody, ownership and/or responsibility of the documents. In case of public judicial and administrative authority it is the operation with which the responsible for conservation transfers to the State Archives or to the Central State Archives of the documentation that will be stored there in accordance with current legislation on cultural heritage.

10.2. Acronyms

AgID

Agency for Digital Italy.

AOO

Homogeneous Organizational Area.

CA

Certification Authority.

CAD

Digital Administration Code - Legislative Decree 7 March 2005, n. 82 and later modifications and additions.

eIDAS

Regulation (EU) n. 910/2014 of the European Parliament and of the Council, of 23 July 2014, in electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC.

FEA

Advanced Electronic Signature.

FEQ

Qualified Electronic Signature.

PdA (AiP)

Archival Information Package.

PdD (DiP)

Dissemination Information Package.

PdV (SiP)

Submission Information Package.

UOR

Responsible Organizational Unit

[Back to top.](#)

11. Regulations, reference standards and certifications

In order to guarantee the correct management of eSIGN, Entaksi defines criteria and processes of the Service on the basis of the Italian and European legislation on the matter, and also implements international standards that define the theoretical, operational and functional management of the system. The reference norms and standards for the company are listed below.

11.1. Company certifications

Entaksi, as part of the development and maintenance of its Integrated Management System, has obtained the following certifications:

- **ISO 9001:2015:** Quality management systems - Requirements.
- **ISO/IEC 20000-1:2018:** Information technology - Service management - Part 1: Service management system requirements.
- **ISO/IEC 27001:2013:** Information technology - Security techniques - Information security management systems - Requirements.
- **ISO/IEC 27017:2015:** Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27018:2019:** Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- **ISO/IEC 27035:2016:** Information technology – Security techniques – Information security incident management.
- **ISO/IEC 22301:2019:** Security and resilience – Business continuity management systems – Requirements.
- **UNI ISO 37001:2016:** Anti-bribery management systems - Requirements with guidance for use.
- **eIDAS Regulation for Qualified Trust Service Providers:**
 - **ETSI EN 319 401:** Electronic Signatures and Infrastructures (ESI) - General Policy Requirements for Trust Service Providers.
 - **ETSI EN 319 411-1:** Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements.
 - **ETSI EN 319 411-2:** Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates.
 - **ETSI EN 319 412-1,2,3,5:** Electronic Signatures and Infrastructures (ESI) - Certificate Profiles.
 - **ETSI EN 319 421:** Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
 - **ETSI EN 319 422:** Electronic Signatures and Infrastructures (ESI) - Time-Protocollo di marcatura temporale e profili di token di marcatura temporale.stamping protocol and time-stamp token profiles.
 - **ETSI TS 119 511:** Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

11.2. Regulations

Codice Civile, R. D. 16 marzo 1942 n. 262

Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili, articolo 2215 bis – Documentazione informatica (regarding provisions for commercial enterprises, article on electronic documentation).

Legge 7 agosto 1990, n. 241 e s.m.i.

Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi (new rules on administrative procedures and access rights to administrative documents).

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.

Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (consolidated law on legal and regulatory provisions concerning administrative documentation).

Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.

Codice in materia di protezione dei dati personali (Data Protection Code).

Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.

Codice dei Beni Culturali e del Paesaggio (Code of the Cultural and Landscape Heritage).

Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.

Codice dell'amministrazione digitale (CAD) (Digital Administration Code).

Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013

Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 (Technical rules for the creation, application and verification of advanced, qualified and digital electronic signature).

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013

Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 (Technical rules concerning digital preservation systems).

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio

Regolamento UE del 23 luglio 2014 (eIDAS), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (EU Regulation regarding electronic identification and trust services for electronic transactions in the internal market).

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Linee guida ufficiali sulla creazione, gestione e conservazione dei documenti informatici, pubblicate da AgID in data 11/09/2020 alle quali vengono aggiunte le modifiche con la relativa proroga contenute nella Determinazione 371/2021 del 17/05/2021 (Official guidelines on the creation, management and conservation of electronic documents).

Determinazione AgID 25 giugno 2021 n.455

Concernente l'adozione del "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" (Regulation on the criteria for the provision of IT document preservation services).

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

Regolamento UE del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

Decreto Legislativo 10 agosto 2018, n. 101

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (provisions on General Data Protection Regulation).

Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate

Linee guida ufficiali pubblicate da AgID in data 20/06/2019 (Official guidelines published by AgID on 06/20/2019).

Linee guida per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD

Linee guida ufficiali pubblicate da AgID in data 23/04/2020 (Official guidelines published by AgID on 23/04/2020).

11.3. Standards

ISO 9001:2015

Quality management systems - Requirements.

ISO/IEC 20000-1:2018

Information technology - Service management - Part 1: Service management system requirements.

ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements.

ISO/IEC 27017:2015

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018:2019

Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO/IEC 27035:2016

Information technology — Security techniques — Information security incident management.

ISO/IEC 22301:2019

Security and resilience — Business continuity management systems — Requirements.

UNI ISO 37001:2016

Anti-bribery management systems - Requirements with guidance for use.

EU Regulation no. 910/2014 - eIDAS

EU Regulation 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.

ETSI EN 319 401

Electronic Signatures and Infrastructures (ESI) - General Policy Requirements for Trust Service Providers.

ETSI EN 319 411-1

Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1: General requirements.

ETSI EN 319 411-2

Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates.

ETSI EN 319 412-1,2,3,5

Electronic Signatures and Infrastructures (ESI) - Certificate Profiles.

ETSI EN 319 421

Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-stamps.

ETSI EN 319 422

Electronic Signatures and Infrastructures (ESI) - Time-Protocollo di marcatura temporale e profili di token di marcatura temporale.stamping protocol and time-stamp token profiles.

ETSI TS 119 511

Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

[Back to top.](#)

12. Periodic check of system accessibility

The procedure is performed by the Preservation Service Manager, who personally or through a delegate ascertains the accessibility of the Service by the Customer and its effective usability, also with regard to performances.

[Back to top.](#)

13. Localization of stored data

The data entered and managed during the Service operation are archived in dedicated storage servers located in the IT network of Entaksi Solutions SpA.

The physical servers provided by the datacenter supplier are subject to a rental agreement that includes hardware maintenance and software configuration availability only, so that, after installation, the supplier no longer has access to the system .

The Storage Service is provided by a Private Cloud, consisting of machines that operate in a highly reliable configuration, located, pursuant to law 244/2007, within the borders of the European Union.

For the provision of the service aligned with the terms defined by the requirements from "Agenzia per l'Italia Digitale" for the supply of conservation services to the Public Administration, an instance of the service is based on machines operating in a highly reliable configuration positioned within the borders of the Italian Republic.

[Back to top.](#)

14. Backup copies management policy

The backup security copies managed by the system are created for the sole purpose of ensuring the operational continuity of the service.

The service is hosted on a server cluster which guarantees the redundancy of the information managed, to provide the best accessibility.

In compliance with the internal information security management procedures, a specific process for the generation of the backup copies is however envisaged.

These copies are used by the Service Manager in case of particularly serious events, which make the currently used work environments unavailable.

[Back to top.](#)

15. Maintenance of the application software

Entaksi ICT Department takes care to keep updated the version of the Software used for the Service's provision.

For this purpose, all the software created for the delivery of the application functionalities and the processes connected to them is archived within a certified software management system compliant with the ISO 9001:2015 standard, therefore able to maintain the versioning of the developed source code.

[Back to top.](#)

16. Malfunctions management

Despite the use of the most advanced standards for system development and test, Entaksi recognizes the possibility that a malfunction, an error or a need to adapt to regulatory changes may occur. To remedy these cases, Entaksi has arranged a corrective and evolutionary maintenance service, which keeps the Service regularly updated and usable.

[Back to top.](#)

16.1. Service reports

The Customer can report any problems encountered by sending an email to helpdesk@entaksi.eu.

Entaksi Solutions provides the customer with software environment, called Redmine, accessible via Internet and dedicated to the management and tracking of service reports (incidents, errors, change requestes, etc).

Through this ticket platform the Customer can insert any request related to technical or economic problems encountered in the use of the eCON service, and stay informed on their management and evolution.

Entaksi can also communicate through the site, through the page status.entaksi.eu, any malfunctions detected on the system.

[Back to top.](#)

16.2. Claims

Claim is defined as a special type of report, relating to the failure to comply with the SLAs (Service Level Agreement) established in the service contract.

The customer can redact a claim and follow its evolution through the ticketing management environment described in the previous paragraph.

[Back to top.](#)

16.3. Emergency changes

In the case of accidents that cause sudden blocking malfunctions or significant deviations from the established SLAs, Entaksi reserves the possibility of making a change to the Service, called "Emergency Change", the application of which may involve the temporary suspension of the Service. The modalities of its implementation will be communicated to the Customer via email.

[Back to top.](#)

17. Data protection management

Concerning access to data by Entaksi personnel, please refer to the data protection management procedures included into the official Entaksi's documentation.

Besides, regarding access to data by the Customer's personnel, and in particular by personnel who will have access to the web interface for searching, viewing and exhibiting documents, reference will be made to Customer data protection internal procedures.

As part of the processing of personal data related to the performance of the activities provided for in this Manual, Entaksi acts as a Processor, by virtue of by specific legal delegation conferred by the Customer.

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

The complete set of provisions relating to the processing of personal data is reported in [the Entaksi website](#).

[Back to top.](#)

17.1. Data Breach

According to the General Data Protection Regulation (EU) 2016/679 (GDPR), articles 33-34, "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent".

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay".

Therefore, as soon as Entaksi becomes aware of a data breach of the personal data processed, as data Processor, it will notify the violation both to the Customer than to the supervisory authority, without undue delay, **within 72 hours** from the time it became known.

The obligation does not exist in the event that it is possible to demonstrate that the violation is unlikely to represent a risk to the rights and freedoms of individuals such as: loss of control of personal data or limitation of their rights, discrimination, theft or usurpation of identity, financial losses, unauthorized deciphering of pseudonymisation, prejudice to reputation, loss of confidentiality of personal data protected by professional secrecy, or any significant economic or social damage to the data owner.

After 72 hours from the violation the notification must be accompanied by the reasons for the delay, and must be given in any case the maximum willingness to collaborate with the competent authorities.

[Back to top.](#)

18. Service Level Agreement

The service-levels or SLA (Service Level Agreement) are settled on the service agreement.

[Back to top.](#)

19. Service reporting

Once a year Entaksi sends to the Customer a specific report on the service's SLA, obtained from the processing of specific data from the internal tracking system, which summarize the following indicators:

- service availability time (% on the total solar time of theoretical availability);
- number of critical incidents managed;
- number of Non-Compliance (NC) detected;
- number of customer claims received.

The customer is also asked, annually, to communicate his level of satisfaction in the use of the service by filling a survey, which contains some questions on some critical aspects of the service, and the possibility of sending personal considerations to Entaksi.

[Back to top.](#)