ENTAKSISOLUTIONS

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

Manuale Utente

UM ePRI en 20250519 User manual

Entaksi Solutions SpA

Index

Document information

Project	User Manuals
Type	User Manual
Document ID	UM ePRI en 20250519 User manual
Version	1.4.0
Creation Date	19/05/2025
Last Revision	01/12/2025
Author	Anna Mazzotta
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
01/12/2025	Paola Caioli	DelM	*Digital signed*

Revisions

Date	Version	Name	Mansion	Action	Distribution
19/05/2025	0.0.1	Anna Mazzotta	ICT Team	Draft creation.	Internal
30/06/2025	1.0.0	Anna Mazzotta	ICT Team	Released.	Public
01/07/2025	1.1.0	Anna Mazzotta	ICT Team	Forced protocol registrations and Email attachment inclusion settings has bee added.	Public
16/07/2025	1.2.0	Anna Mazzotta	ICT Team	Folder management in register of documents and related metadata.	Public

Date	Version	Name	Mansion	Action	Distribution
29/09/2025	1.3.0	Anna Mazzotta	ICT Team	Uniqueness checks have been introduced for the DMD code, the classification scheme node code, and the email address of the subjects.	Public
01/12/2025	1.4.0	Anna Mazzotta	ICT Team	Smart Folder	Public

1. Introduction

This user manual describes the **ePRI** service which is provided by Entaksi Solutions SpA, hereinafter referred to as "Entaksi".

The ePRI service allows the assignment of registration numbers to inbound, outbound, and internal documents, enabling generation, management, and preservation of the daily registration logs, which is dematerialized and digitally signed.

eCON Digital Preservation Service is the system on which ePRI 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 ePRI. For a detailed description of all the features of the qualified services offered by Entaksi, you can consult the page within the corporate website at the following link: https://www.entaksi.eu/en/services-documentation/.

This manual describes:

- The functionalities provided by the service.
- The methods of access to the service and its use.
- The procedures in place to ensure information security.

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.

ePRI 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 the top.

1.1. ePRI service features

ePRI is the Entaksi service that enables registration management by integrating it with the preservation system and generating

a daily submission information package that contain the register of documents.
ePRI is the service that allows the registration of analog documents and the creation of their corresponding digital copies, which are then sent to the preservation system along with the daily registration logs in which the documents have been recorded.

The solution proposed by Entaksi integrates the technical specifications required by regulations with archival needs, ensuring the ability to enter, to register, to preserve, and to retrieve specific documents at any time, it interfaces with the document management system, the preservation system, and the modules for managing certified emails (PEC) and standard emails.

The service includes:

- assignment of registration numbers to inbound, outbound, and internal documents;
- document classification and assignment to the relevant Document Management Division (DMD);
- integrated management of Certified Email (PEC) with electronic registration of inbound and outbound email;
- generation, management, and preservation of the daily registration logs, digitally signed;
- user profiling with the ability to segment and restrict functionalities based on a user type;
- integration with the document management system and related document classification;
- document search functionality by registration number and associated metadata;
- activity log management for tracking performed actions.

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.

Regarding the document access component, the service is integrated by a customized management software **eDOC** based on Alfresco Community Edition.

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

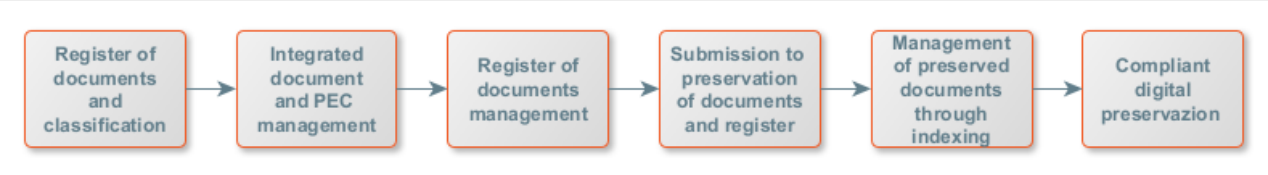

Figure 1. Servizio ePRI.

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

Back to the 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 “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" and 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 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**.

ePRI 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 ePRI 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 on the and on the Entaksi Website: https://www.entaksi.eu/en/entaksi-solution-spa-english/.

The roles are represented in the following diagram.

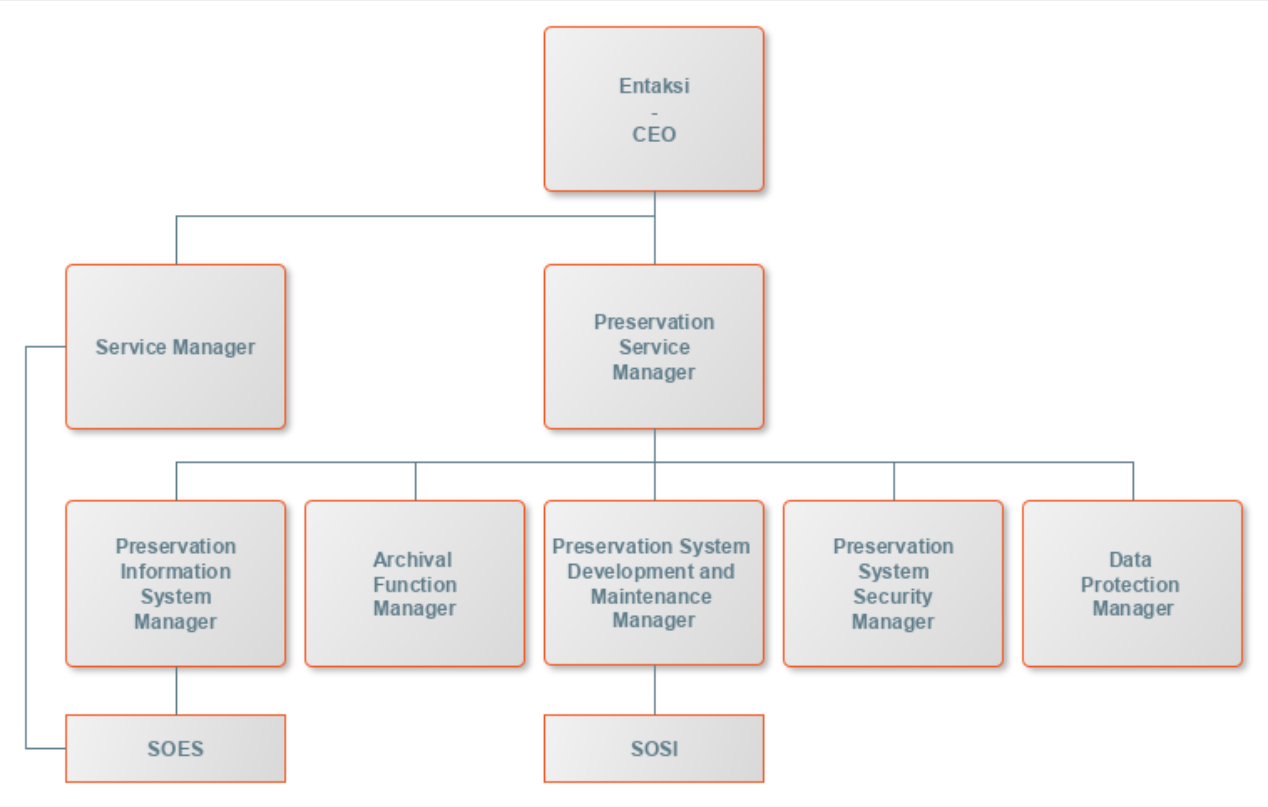

Figure 2. Roles and responsibilities.

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 the 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 ePRI 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 the 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 ePRI 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 the top.

2.3. ePRI Manager tasks

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

Table 1. Tasks.

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

Service Manager	Customer	ePRI Manager
Management and periodic update of system software and database		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 the top.

3. Registration procedure

The registration to the Entaksi Console platform, which allows users to enter and manage their credentials for accessing all services provided by Entaksi, is a unified system compliant with the OAuth2 standard, ensuring high levels of access protection and data security.

Access to service functionalities is subject to the completion of the contract.

The services available through this interface may be combined or used individually and are described on the company website at the following https://www.entaksi.eu/en/services-documentation/.

To access the functionalities of the ePRI service, users must log in to the Entaksi authentication system at https://entaksi.eu/console enter username (email) and password, and click the “**Login**” button.

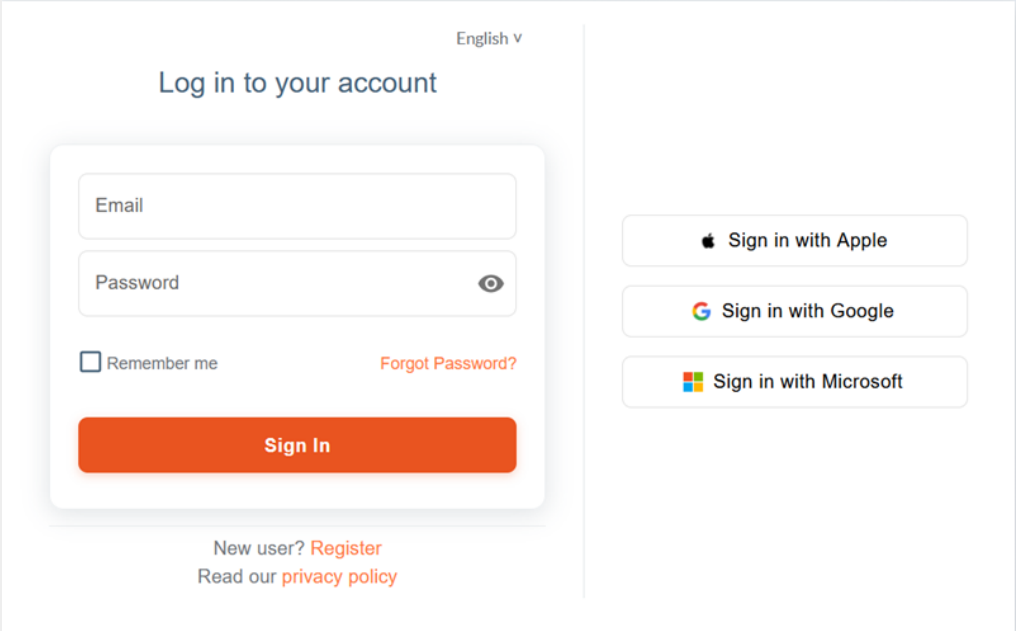

Figure 3. Authentication system.

In the event that the user has not previously registered and therefore has not confirmed their access credentials, they must click on the "**Register**" link located next to the question “**New User?**” at the bottom of the page.

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.

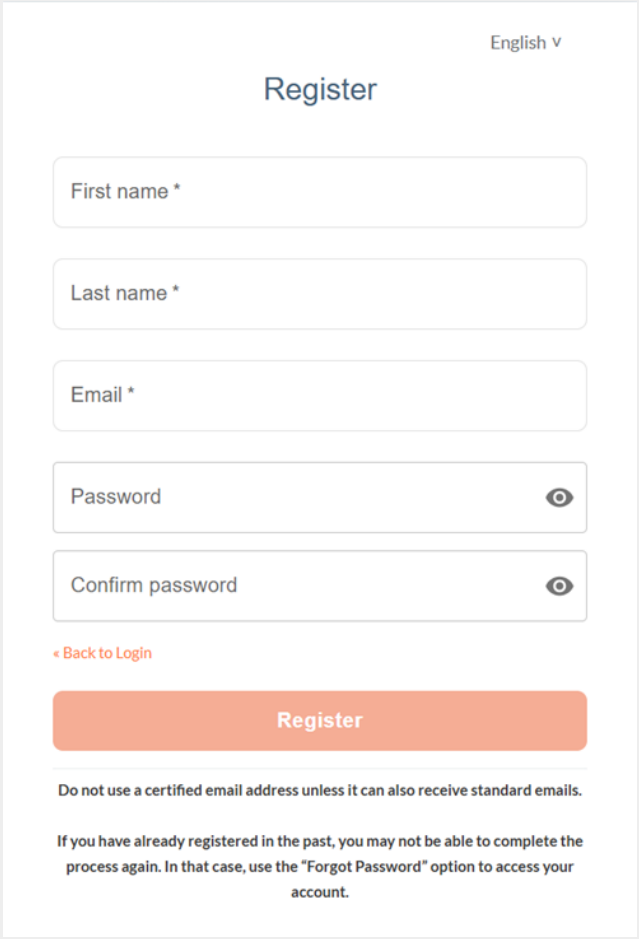

Figure 4. Input of data.

The password must contain a minimum of 12 characters, including at least one uppercase letter, one lowercase letter, and one number. The password will be valid for 90 days, after which the system will automatically prompt the user to update it. For the update, the last five previously used passwords cannot be reused.

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, the "Register" button will be enabled.

The "Register" button will remain disabled in the following cases:

- The password entered in the "**Password**" field and the one entered in the "**Confirm Password**" field do not match. In this case, click the button to display the entered value and make any necessary corrections;
- The email address is already registered in the system. In this case, user must follow the password recovery procedure to obtain updated credentials (see Resend registration link and password recovery).

By clicking the "*Register*" button, 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**.

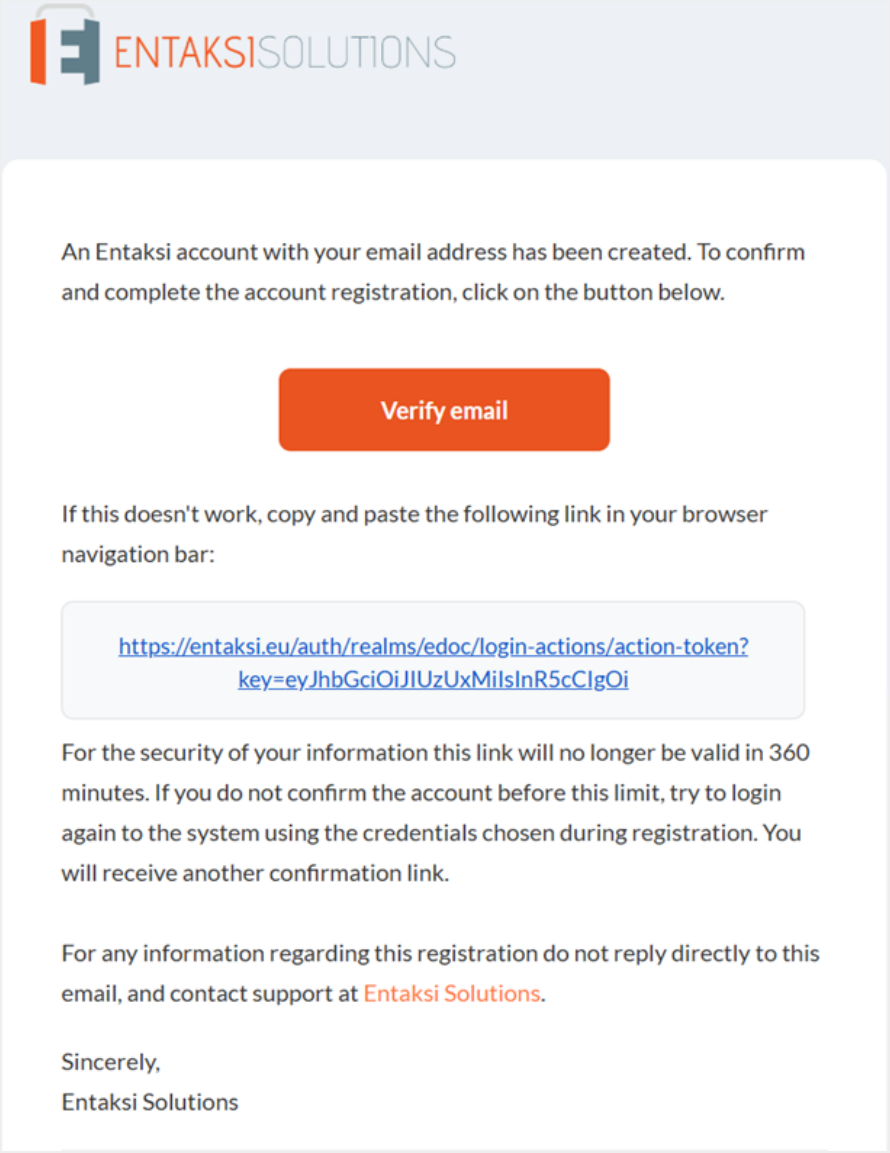

Figure 5. Email confirmation.

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?**". A new page will be displayed to continue with the password recovery process.

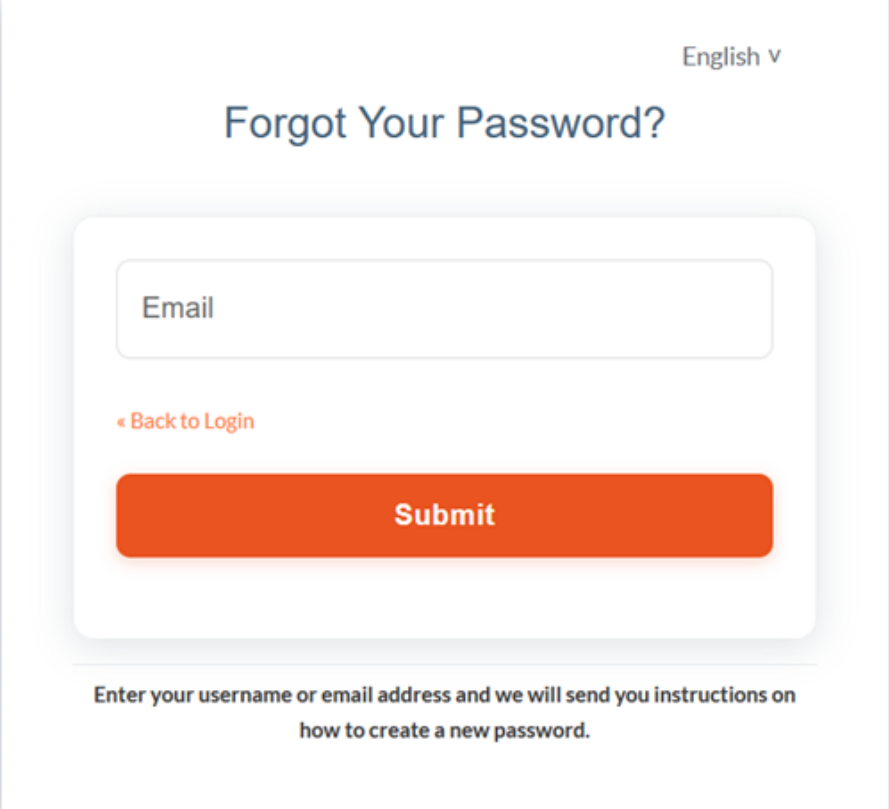

Figure 6. Password recovery procedure.

By entering the username or the registration email and clicking the "**Submit**" button, the system will send a message to the registered email address containing the instructions and a link to start the password recovery procedure.

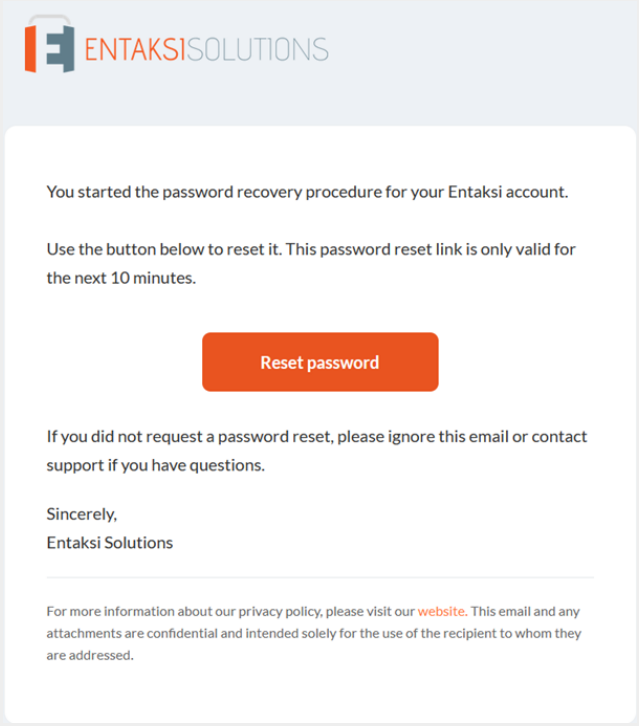

Figure 7. Password recovery email.

By clicking the "**Reset password**" button, an additional page will open where user can enter and confirm the new password.
By clicking the "Submit" button, the change will become effective.
The password must contain at least 12 characters, including at least one uppercase letter, one lowercase letter, and one number, and the last five previously used passwords cannot be reused.

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 TSL protocols.

Back to top.

3.4. User settings management

From the ePRI 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. ePRI Console

The ePRI is available on **Entaksi Console**,the web application that allows Entaksi Customers **to upload documents, register of documents and to manage electronic registration, to preserve the daily registration logs, to search them in the preservation system, and and to download Dissemination Information Packages (DIP), which contains legally-compliant documents to show in case of inspections and controls.**
The service provides access to the document management system, allowing users to search, view, and download documents.

Through the Console you can access the ePRI 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.

This segregation must be requested when the service is activated.

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. The Entaksi Console header

The Entaksi Console header features a grey band with information on the right regarding the company and the currently logged-in user.
The displayed company is the active company currently being used.

If the user is authorized for multiple companies, clicking the  button will display a list of available companies for the user. By selecting the desired company, the user can seamlessly switch the workspace area without having to leave the platform.
Next to the company name, the logged-in user is displayed: at the top, the first and last name entered during registration are shown, while at the bottom, the email associated with the user account is displayed.
By clicking on the user profile, a dropdown menu allows the user to view their account settings by selecting the "**User Settings**" option, additionally, the user can change the Console language (available in both Italian and English) by clicking on the "**Language**" option and selecting the desired language.

4.2. Footer Console

The footer, like the header, is common to all pages of the Console.
On the right, the main contacts for Entaksi are displayed, namely the email for general inquiries info@entaksi.eu and the support email helpdesk@entaksi.eu.
Clicking on the Entaksi icon will open a panel containing, in addition to the contacts, all the company's key information and certifications (see Company certifications).
On the right-hand side, general information about the Console is shown, including the currently published version and the version of the service the user is currently using.

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.

4.4. 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.

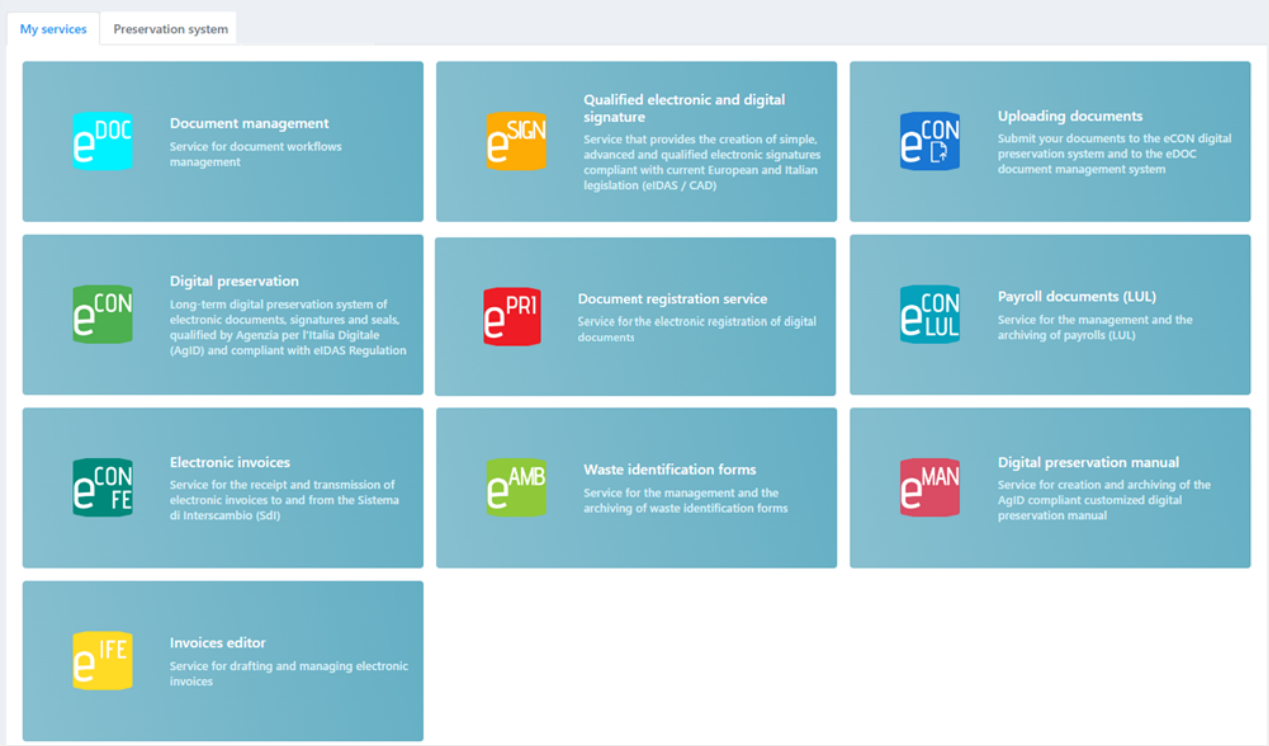

Figure 8. My services

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.

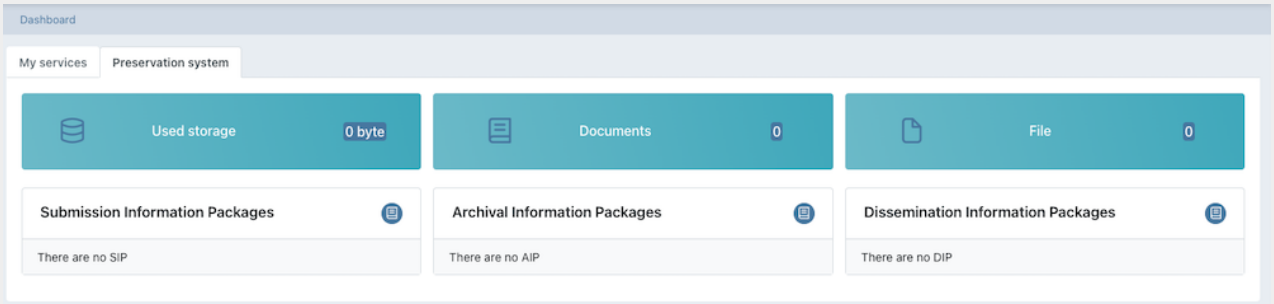

Figure 9. Preservation system.

By clicking on the button the ePRI 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.

4.5. 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**.

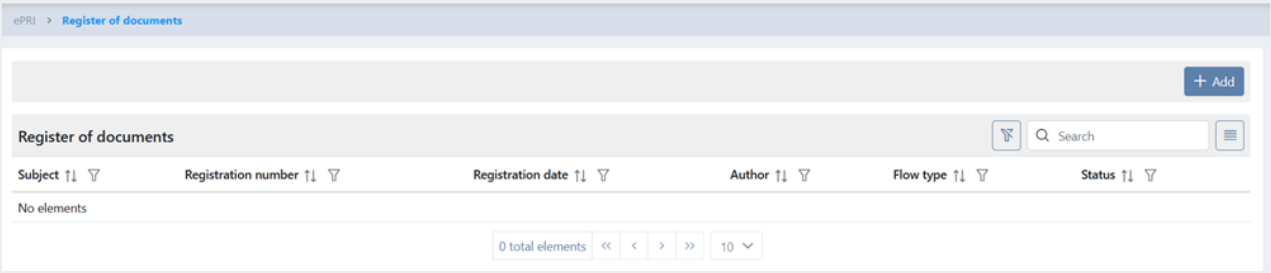

Figure 10. Table filters and sorts.

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.

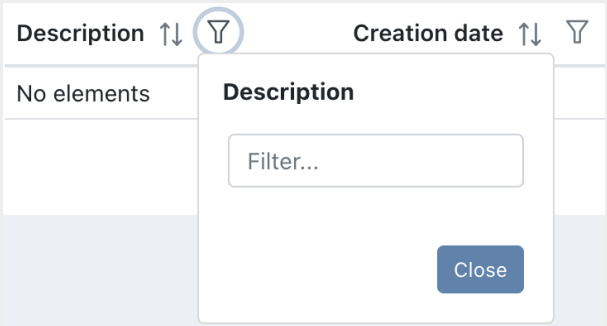

Figure 11. Filter example.

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.

	**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 ePRI 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).
- **Document Management Divisions**: section where t is possible to configure and manage the company document management divisions (Document Management Divisions).

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 ePRI service.
ACTIVATED	The user is inserted and the role is active: the user can access to the ePRI 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 ePRI 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

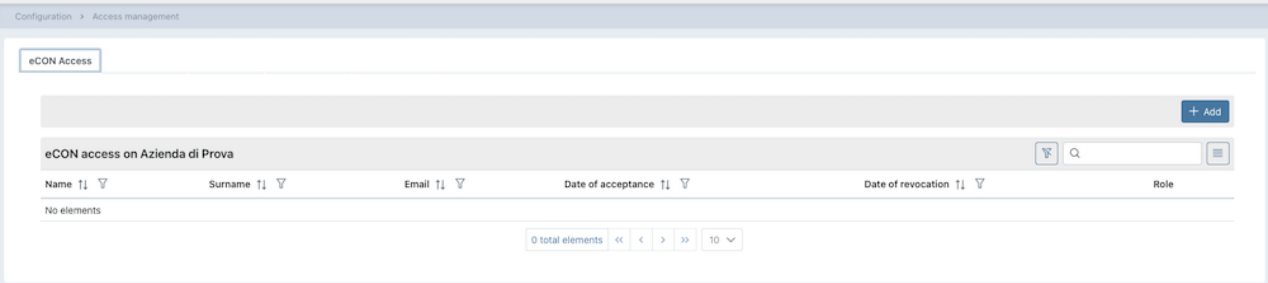

Figure 12. Users list.

The table below shows the available roles for the ePRI 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.

Description	Enabling
Utente del servizio (service user).	The user with this profile can access all the features of the service, **excluding** enabling new users.
Utente abilitato al caricamento dei pacchetti di versamento di precedente conservatore.	This profile is available exclusively following a commercial agreement. The user enabled with this profile will be able to upload, using the dedicated function, a Dissemination Information Packages from another preservation service provider.

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 and he be able to manage all documents, it is sufficient 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. ePRI service access management ePRI

In the "ePRI Access" section, in addition to the data listed above, the left side of the page displays the list of all Document Management Divisions (DMD) previously added for the company.
Role configurations can be defined at the company level, or at the level of a document management divisions.
To assign a specific role at a given level, select the desired level (company, document management divisions) from the left side of the screen (it will be highlighted in blue), and proceed with the role assignment as described below.

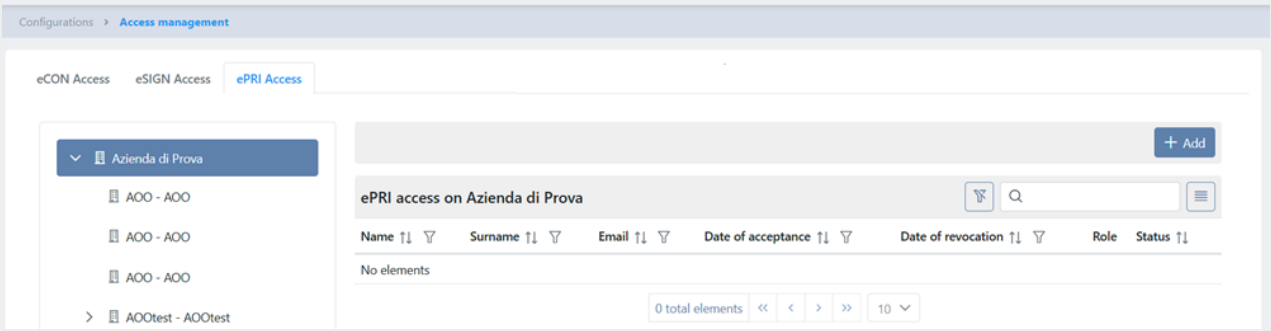

Figure 13. User list.

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

Description	Enabling
Amministratore del servizio ePRI (ePRI service manager)	The user enabled with this profile can access to all the functions of the ePRI service, including the change of the service configuration, enabling of new users, and assigning the corresponding profile.
Utente del servizio ePRI (ePRI user service)	The user enabled with this profile can access to all functions of the ePRI service but cannot enable new users.

Description	Enabling
Utente abilitato alla gestione delle registrazioni di protocollo (User enabled to manage register of documents)	The user enabled with this profile has access, for editing and data entry purposes, only to the functions related to the management of registrations. The user has access to “*Register of documents*”, “*Daily registration logs*” and “*Subjects*” pages.
Utente abilitato alla visualizzazione delle registrazioni di protocollo (User enabled to view register of documents)	The user enabled with this profile has read-only access to the functions related to the registrations management. He has access to the “*Register of documents*”, “*Daily registration logs*” and “*Subjects*" pages.
Utente abilitato alla gestione dei fascicoli (User enabled to manage Folders)	The user enabled with this profile has access, for editing and data entry, only to the functions related to the management of folders.
Utente abilitato alla visualizzazione dei fascicoli (User to view Folders)	The user enabled with this profile has read-only access to the functions related to folder management.
Utente abilitato alla gestione delle mail (User enabled to manage Emails)	The user enabled with this profile has access, for editing and data entry, only to the functions related to email management. He has access to “Email” and “Email Accounts” pages.
Utente abilitato alla visualizzazione delle mail (User enabled to view Emails)	The user enabled with this profile has read-only access to the functions related to email management. He has access to “Email” and “Email Accounts” pages.
Utente abilitato ad operare sul titolario di classificazione (User enabled to manage classification scheme)	The user enabled with this profile has access **exclusively** to the classification scheme and its management.
Utente abilitato a visualizzare il titolario di classificazione (User enabled to view Classification scheme)	The user enabled with this profile can assign values to the Classification scheme in the various services where it is available (e.g., eSIGN or ePLUS), to correctly apply the related metadata for proper preservation. The user is not authorized to view or manage the Classification scheme page.

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.

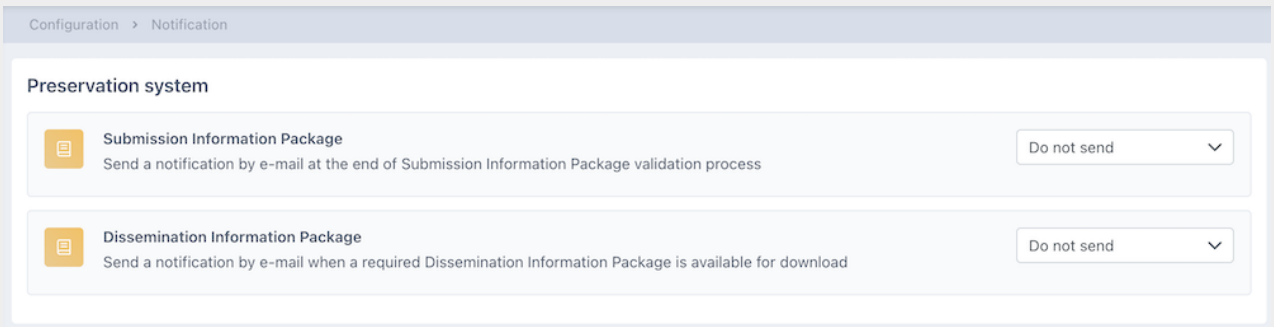

Figure 14. Notification

The system can send notifications:

- at the end of Submission Information Package validation process;
- when a required Dissemination Information Package is available for download.

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.

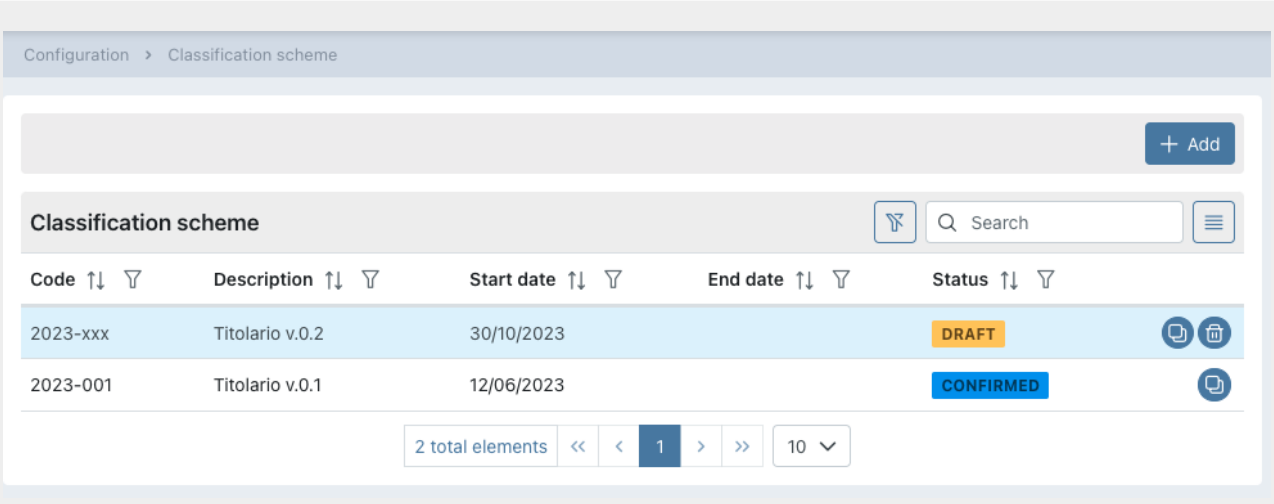

Figure 15. Classification scheme

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 the case that the Classification scheme is confirmed, it is not possible to modify its structure, it can only be applied to the eDOC document management service, only on the eCON preservation service, 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.

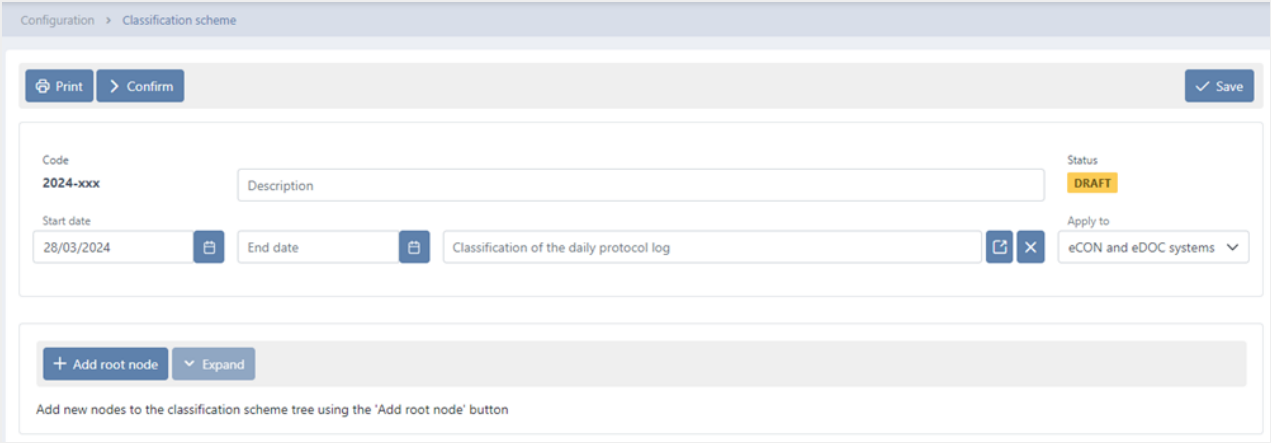

Figure 16. Adding a classification scheme.

During the creation phase, the service assigns an identification code to the classification scheme and a default description.
The default description is "`Classification scheme of <creation date>>`", while the code is will be composed as follows: `yyyy-xxx` where `yyyy` indicates the creation year and `xxx` the unique progressive creation number.
The creation year is immediately assigned during the creation phase and is visible right away.
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 registration 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 registration 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 registration 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.

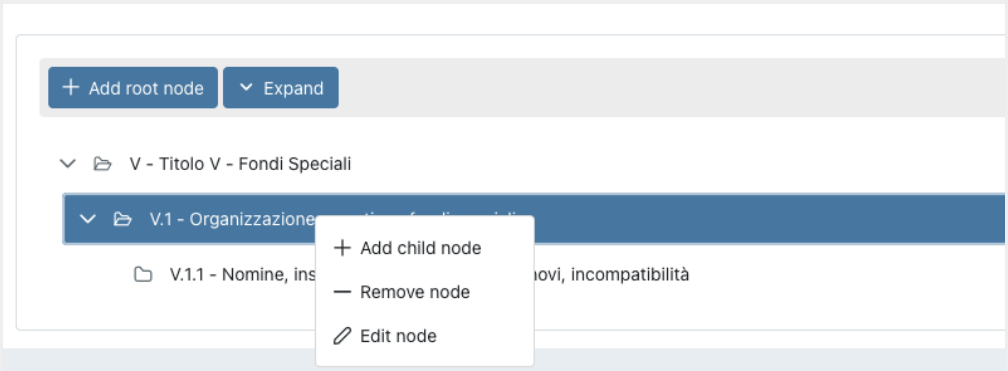

Figure 17. Example of classification scheme structure

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.

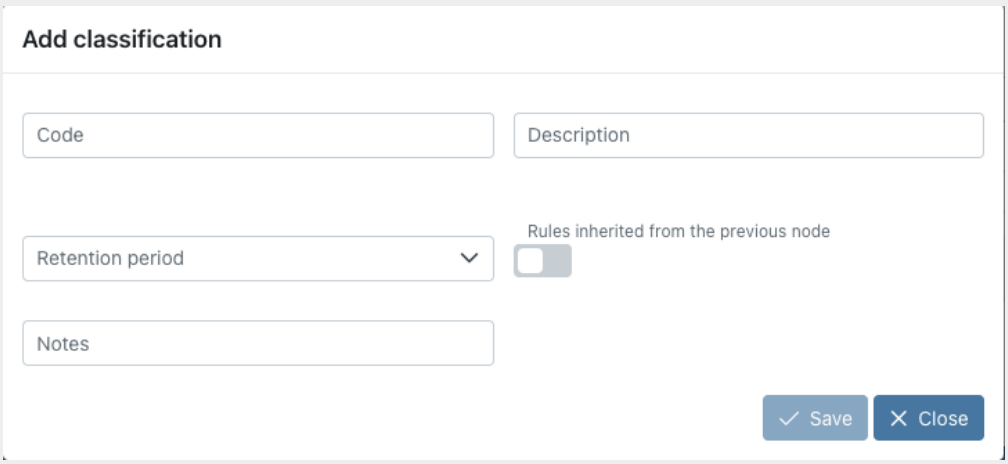

Figure 18. Entering a node.

To complete the entry, it is necessary to enter the code (which must be unique within the entire structure), the 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.
The option to inherit the retention rule from the parent node will, of course, not be available on the main nodes (root), as there is no parent node for these.

If nodes are added without specifying any retention rule, an alert icon will appear next to the node to quickly identify the node with the missing data.

The action of addition, modification, and deletion of a 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 the "**Delete**" button, it is possible to remove a classification scheme that is in draft state.

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. Document Management Divisions

As defined in Article 50 of the Testo Unico sulla Documentazione Amministrativa (TUDA), within the context of its legal system, each administration identifies the offices to be considered to coordinate document management in large document management divisions, 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 document management divisions are listed.

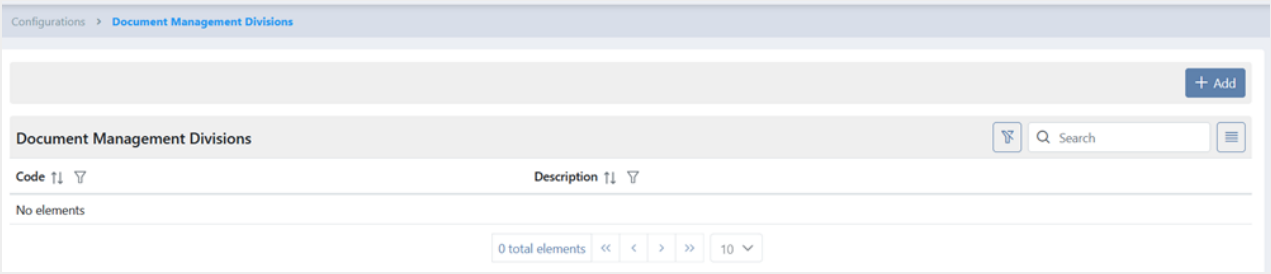

Figure 19. Document management divisions.

- **Code**: it is the unique code of the document management division assigned during add phase;
- **Description**: it is the description of the document management division assigned during add phase.

From this section it is possible:

- to sort the columns and filter the elements in the table;
- click on the individual row to open the management division detail page to modify it;
- to add a new organizational area by clicking on "**Add**".

5.5.1. Adding a document management division

By clicking on the "**Add**" button a new page opens where you can insert a new document management division.

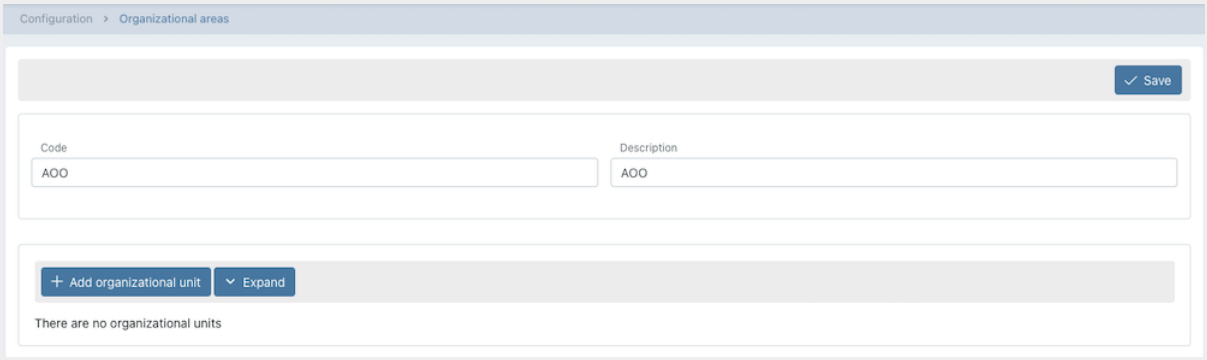

Figure 20. Adding a document management division.

In order to uniquely identify a document management divisions, 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 document management division click on the "**Add Document Management Unit**" button. The inserted organizational units have a tree structure.

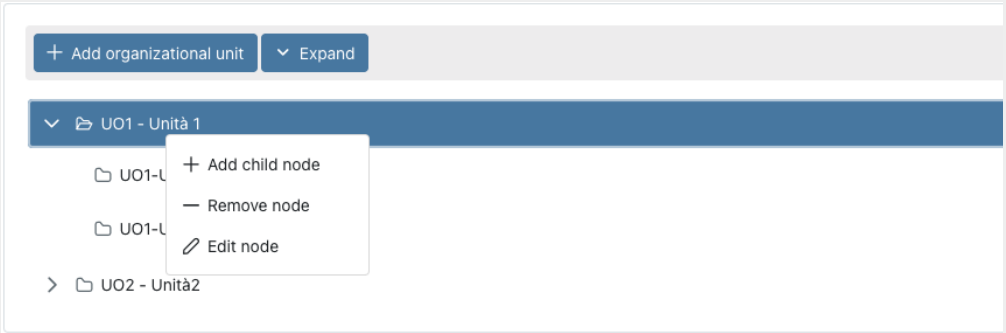

Figure 21. Example of organizational area structure.

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.

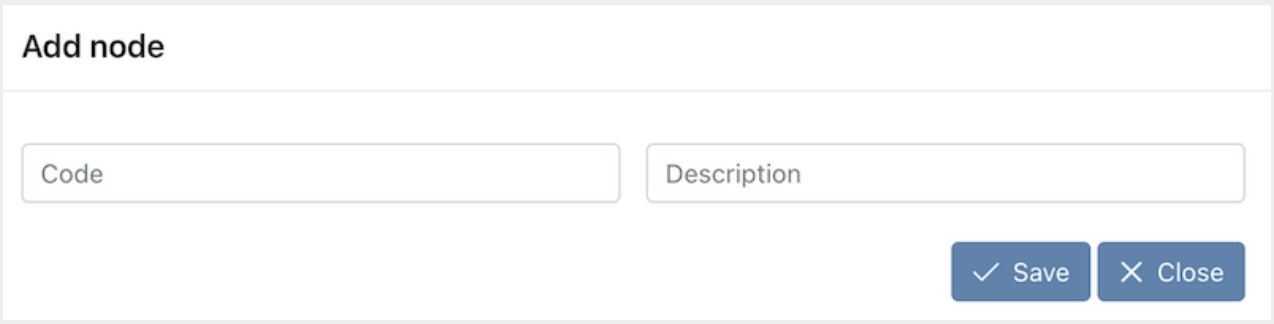

Figure 22. Adding Document Management Divisions.

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. ePRI - Register of documents

The ePRI service enables **the management of the electronic registration number for inbound, outbound, and internal documents, allowing the generation, management, and preservation of the dematerialized daily registration logs, digitally signed.**

The user will be able to:

- to manage documents to be registered;
- to manage received and sent emails (PEC or ordinary) and their registration;
- to manage the automatic creation of PEC-type Submission Information Packages containing sent and received email messages from an account, and their later archiving in the preservation system;
- to access the preservation system and to monitor the status of the submitted documents;
- to request Dissemination Information Packages (DIP) for the documents being searched;
- to download the requested Dissemination Information Packages;
- to access the document management system to check, search, view, and download documents.

Once logged into the Entaksi Console, to access the ePRI interface, select one of the available options from the "**ePRI**" items in the main menu: each option will open the corresponding page.

The **ePRI** menu includes:

- **Register of documents**: a list of all registration with the option to manually enter new ones (see Register of documents);
- **Daily registration logs**: a list of all generated daily registration logs (see Daily registration logs);
- **Email**: management of the received and sent messages from a previously configured email account with the option to register them automatically (see Email);
- **Folders**: management of registrations folders (see Folders);
- **Configurations**: this menu item provides access to additional configuration options required for proper service operation:
  - **Email accounts**: a list of all previously configured email accounts, with the ability to add new ones or disable existing ones (see Email accounts);
  - **Subjects**: the ability to define personal data for company reference subjects (see Subjects).

6.1. Register of documents

The Register of documents page contains a list of all registration created through the ePRI service.

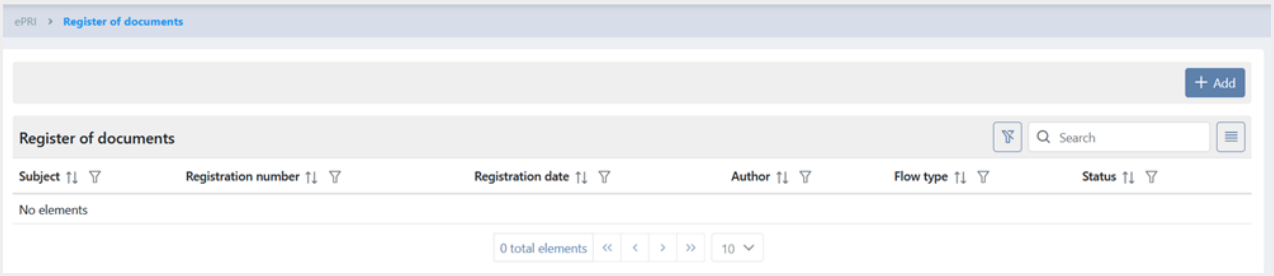

Figure 23. Register of documents.

Below is a brief description of the fields and filters available in the grid:

- **Subject**: contains the subject of the registration and it is added at the time of submission.
- **Registration number**: this is the unique registration number automatically assigned when the registration is confirmed. The number is composed as follows:
  `VAT number of the administration + DMD code + Year + Unique progressive 7-digit number`
  where:
  - `VAT number of the administration`: the VAT number of the administration for which the draft registration is being created;
  - `DMD code`: the code of the Document Management Divisions (DMD) selected during the registration process (this is a mandatory field). At the beginning displayed as `xxxxxxx`, it will be populated with the value entered during registration at the time of saving and will therefore be visible even while in draft status;
  - `Year`: the year in which the registration is carried out;
  - `Unique progressive 7-digit number`: a unique 7-digit progressive number for the registration, automatically assigned by the system based on the year and DMD added. At the beginning displayed as `xxxxxxxx` it will be automatically populated by the system upon confirmation of the registration;
- **Registration date**: the date and time when the registration was created;
- **Author**: the name of the user who created the registration;
- **Flow type**: it is the category of documents included in the registration;
- **Status**: it is the current progress state of the registration.

From this section, it is possible to:

- sort the columns and filter the items in the table as described in the Console tables chapter;
- delete any registrations in *Draft* status simply by clicking the button located on the right side of the row ;
- access the details of the digital registration log by clicking on the individual row. If the process status is *Draft*, it will be possible to modify the previously entered data. For all other status types, data modification is not allowed; however, the information will be available in read-only mode as descriptive details of the registration.
- new registrations can be added, if the user has the necessary permissions, by clicking the **Add** button.

The table below lists the possible values for the "*Flow type*" of the registration:

Value	Description
INBOUND	The register of documents refers to "inbound" documents, meaning documents received by the company from other organizations.
OUTBOUND	The register of documents refers to "outbound" documents, meaning documents sent by the company to other organizations.
INTERNAL	The register of documents refers to "internal" documents, meaning documents that are neither received nor sent, but are produced by the company for internal purposes.

The table below lists available values for the "*Status*" of registration:

Value	Description
DRAFT	The register of documents has been only saved. It will be possible to make changes to the data (except for the author and registration date), upload new files, delete previously uploaded ones, or delete the entire registration. The assigned registration number will be provisional and structured as follows: VAT number administration + DMDCode + Year + xxxxxxxx
RECORDED	The register of documents has been saved and confirmed. It will no longer be possible to modify the registration data, add/remove files, or delete the entire registration. The only permitted action will be to change its status to "Canceled". The assigned registration number will be provisional and structured as follows: VAT number administration + DMD Code + Year + Unique progressive number
CANCELED	The register of documents has been canceled.

6.1.1. Add a register of documents

Register of documents can be added in two different ways: manually or through email registration (see Email detail page).

Manual Registration

To add a registration manually, click the "**Add**" button located at the top right of the register of documents page; to edit a previously added registration in draft status, click on the corresponding row of the registration.

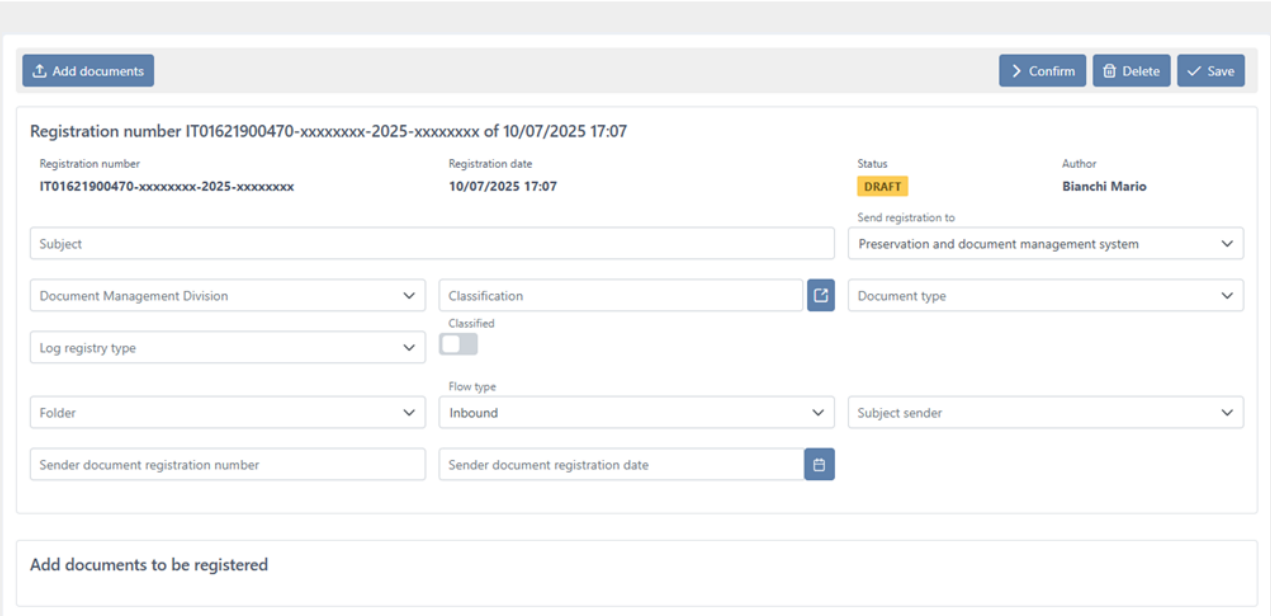

Figure 24. Add a register of documents.

During the creation or the editing of a registration, mandatory fields that are not correctly filled in will be highlighted in red: saving will only be possible once all required fields have been completed.
The registration date, author, and registration number are automatically assigned by the system and cannot be modified.

The data related to the classification (mandatory data) and the folder (optional data) are strictly connected: when a classification is selected, only folders with the same classification will be proposed.
If a folder is selected (without having previously selected the classification), the system will automatically populate the classification present on the folder.

To assign a classification scheme node, click the button located to the right of the corresponding field: the currently active classification scheme will be displayed (i.e., the one confirmed with a start date earlier than the current date and no end date present, or an end date later than the current date). If no elements are shown, a valid classification scheme must be added as explained in the paragraph Adding a classification scheme.
Select a node from the lowest level of the chosen branch and click the "**Confirm**" button: the documents included in the registration will be assigned to the selected classification.

By selecting one of the available actions for the "*Send registration to*" field, you can define the destination environment for the automatically generated Submission Information Package, which includes the attached documents and the digital registration log. The selectable options are:

- *Digital preservation system*: The generated Submission Information Package is sent **exclusively** to the eCON preservation service.
- *Document management system*: The generated Submission Information Package is sent **exclusively** to the eDOC document management service, and therefore the documents are not placed into the preservation system.
- *Preservation and document management system*: The generated Submission Information Package is sent to both the eCON preservation service and the eDOC document management service.

By selecting the flow type, additional data will be required:

- "*Inbound*" flow type: The subject sender (a mandatory field) will be required and must be selected from those previously added in the subject page (see Subjects). The sender's document registration number and registration date (optional fields) will also be requested.
- "*Outbound*" flow type: The subject receiver (a mandatory field) will be required and must be selected from those previously added in the subject page (see Subjects).
- "*Internal*" flow type: no additional data will be required.

By clicking the "**Add Documents**" button located at the top left, user can attach documents to the registration for preservation; the formats supported by the service are those listed in Allegato 2 of the AgID Guidelines.

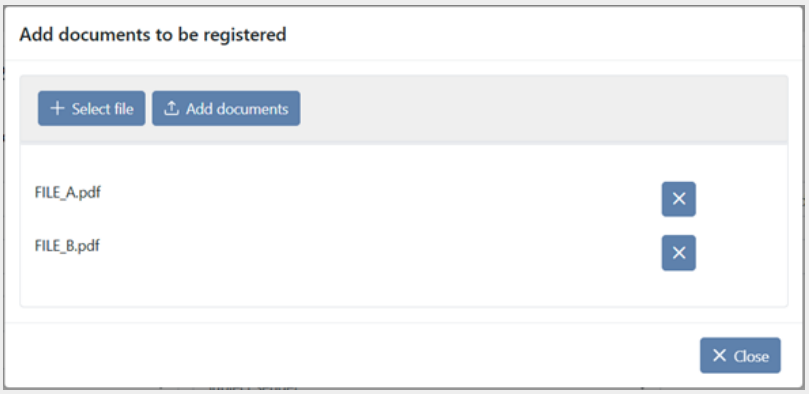

Figure 25. Add documents mask.

By clicking the "**Select file**" button, user can select one or more documents to upload.
By clicking the "**Add documents**" button, the previously uploaded files will be added to the registration.
By clicking the button before clicking "*Add documents*" button will remove the file from the list and it will not be uploaded.
By clicking the "**Close**" button will close the window. If "Close" button is clicked without previously clicking "*Add documents*", the selected files will **not** be uploaded and will not appear in the list of documents to be registered.

IMPORTANT: If the file name contains special characters (for example *ù*, *à*, :, /, \, etc.), it is recommended to rename the file by removing such characters, as the system will automatically remove them during the file upload process.

ATTENTION: Documents included in the registration must have an extension permitted by the preservation system.
For this reason, documents with the following extensions will not be accepted:
`.7z`; `.rar`; `.tar`; `.pptx`; `.xls`; `.gif`; `.tsd`; `.msg`.

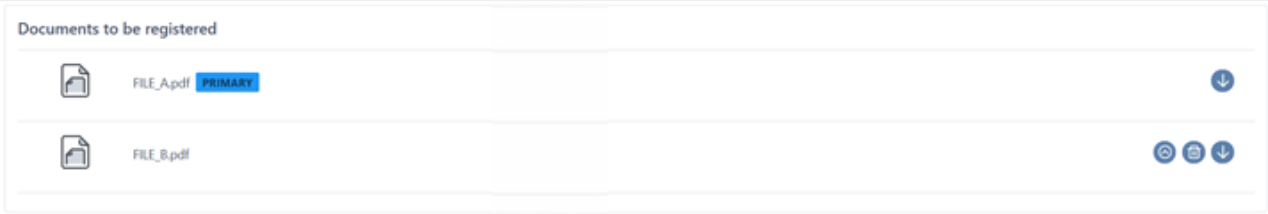

Figure 26. Document to be registered list.

The first uploaded document will be automatically designated as the "*Primary*" document.
If user wishes to designate another document as primary, simply click button located on the row, which is visible only when the registration is in "*Draft*" status.

By clicking on button, which is visible only when the registration is in "Draft" status, the file will be removed from the list and will not be included in the registration.

By clicking on button, it will be possible to download the individual file that is part of the registration.

Registration from Email

Registrations generated from emails can be of two different types: manual (individual or bulk) or automatic.

If the "*Register received message*" option has been activated in the email account configuration page (see Email accounts), a registration is automatically created for each email received and/or sent from the configured account.
Otherwise, the registration must be performed manually, either from the email detail page by clicking the button located at the top right, or by selecting one or more emails to be registered and confirming the action (see Email).

If the email is manually registered from the detail page by clicking the button , the registration will remain in draft status: it will need to be confirmed at a later stage.

In all the cases mentioned above, the registration will be automatically generated with the following data:

- the description is populated with the subject of the email;
- the Document Management Division, the Classification scheme, the document type, the log registry type, confidentiality option and its description, are automatically populated with the values set in the "*Default Values for registrations*" section of the email account configuration page;
- the flow type is automatically set to "*Inbound*" for received emails and "*Outbound*" for sent emails;
- the "Subject" field is automatically filled in with the data of the subject listed in the subject page whose email address matches that of the sender or receiver (see Subjects).
  If multiple subjects meet the above condition, the system selects the most recently added one.
  If no matching subjects are found, the system will create a new entry in the subjects page by extracting the data from the email address. Email addresses can be of two types: "subject name + email" or "email only".
  - For an address type "subject name + email". The service creates a subject type "Legal person" filling in the email and the company name fields, and automatically associating it with the registration. If the registration was not manually generated using the button and all mandatory fields are filled, it will be confirmed automatically;
  - for an address type "email". The service will refer to the settings saved in the email account configuration page for the "*Force registrations*" field (see Email accounts):
    1. *If enabled*: the registration is forced. Mandatory fields of the daily registration logs that are not available in the subject page such as the company name, will be populated with empty values, thereby validating the registration, which will be automatically confirmed if all required fields are present;
    2. *if disabled*: the registration will not be forced. If the daily registration logs is invalid, the registration will remain in draft status;
- the documents to be registered will be automatically included as specified in the email account configuration page under the "*include message attachments*" field (see Email accounts):
  - if enabled_: in addition to the *.eml* file of the email, which is automatically set as the primary document, all attachments from the original message will be included in the registration that have an allowed extension;
    If any attachments have a non-allowed extension, the registration will still be created but will remain in draft status.
  - *if disabled*: only the *.eml* file of the email, defined as the primary document, will be included in the registration.

If all the mandatory fields are correctly filled in, the registration will be automatically confirmed, changing its status to

"*Registered*" and a registration number will be automatically assigned.
Otherwise, the registration will remain in "*Draft*" status to allow for any corrections or modifications.

Unlike manual registration, it is **not** possible to delete the primary file (i.e., the *.eml* file) **nor** to set another file as primary (the button is not visible). However, it is possible to delete non-primary files by clicking the button, to download files by clicking the button, and add new files by clicking the "*Add Documents*" button located at the top right, proceeding as in manual registration.

Manual save and confirmation of draft registration

By clicking the "**Save**" button located at the top right, the registration is saved as a "*Draft*": no registration number will be assigned except for the default one (identified as xxxxxxxx) it is possible to make changes to the registration at any time, both to the data and the uploaded files (adding new ones or deleting previously uploaded ones), or delete the registration by clicking the "**Delete**" button. By clicking the "**Confirm**" button, the registration will be confirmed, the status will change from "*Draft*" to "*Registered*", and a unique registration number will be automatically assigned by the system, proceeding with the digital registration logs operation.

Confirmed registrations

A confirmed registration, with status "*Registered*", cannot be modified but only canceled.
To cancel a previously confirmed registration, open it in edit mode and click the "*Undo*" button located at the top right.

At the time of confirmation, the system automatically assigns the registration number, which is visible both in the Console and on the first page, top left, of the documents attached to the registration in *.pdf* format. (This information is not visible if the registration is in Draft or Canceled status.)

The digital registration log information associated with the document is contained in a downloadable *.xml* file, accessible by clicking the "**Download digital registration log**" button located at the top left of the page. The digital registration log will subsequently be preserved in the same Submission Information Package containing the files that make up the registration.

6.2. Daily registration logs

The **Daily registration logs** page contains a list of all the daily registration automatically processed by the service.
The register of documents will have a unique registration number assigned by the system, structured as follows:
`VAT number administration + DMD + Year + Unique progressive three-digit number`
where:

- `VAT number administration`: it is the VAT number of the administration for which the system is creating the daily registration log;
- `DMD`: it is the document management division associated with the documents registered during the registration process. Therefore, different registration with their own numbering will be generated for the various document management divisions;
- `Year`: it is the year in which the daily registration log is created;
- `Three-digit unique number`: it is the progressive three-digit unique number automatically assigned by the system based on the year and the Document Management Division (DMD).

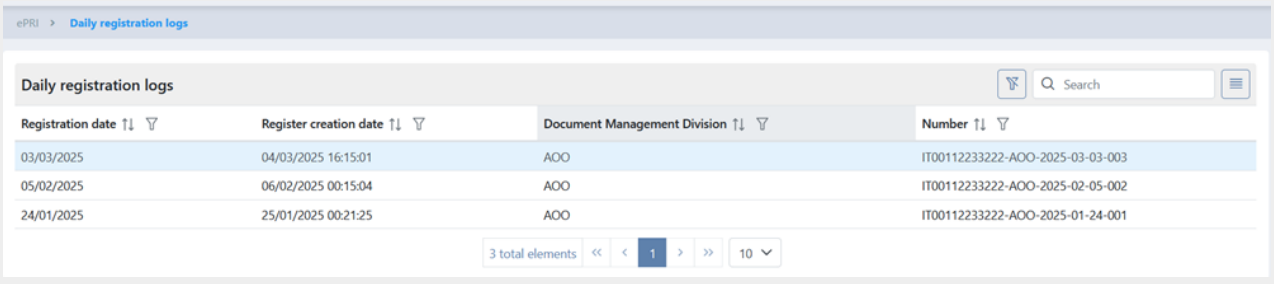

Figure 27. Daily registration logs list.

Below is a brief description of the fields present in the list:

- **Registration date**: it is the registration date that make up the daily registration logs;

- **Register creation date**: it is the creation date of the daily registration logs. If the register has been created but not yet closed and therefore not sent for preservation, the message "*Register creation date not available*" will be displayed;
- **Document Management Division**: it is the description of the document management division for the registration that make up the register;
- **Number**: it is the registration number automatically assigned by the system, as previously described, in the format: `VAT number administration + DMD + Year + Unique number assigned by the system`.

From this section, it is possible to:

- sort the columns and filter the items in the table as described in the Console tables chapter;
- view the details of a daily registration log by clicking on its row.

6.2.1. Daily registration logs detail page

By clicking on a registration row, you can view the detailed page of that daily registration log.

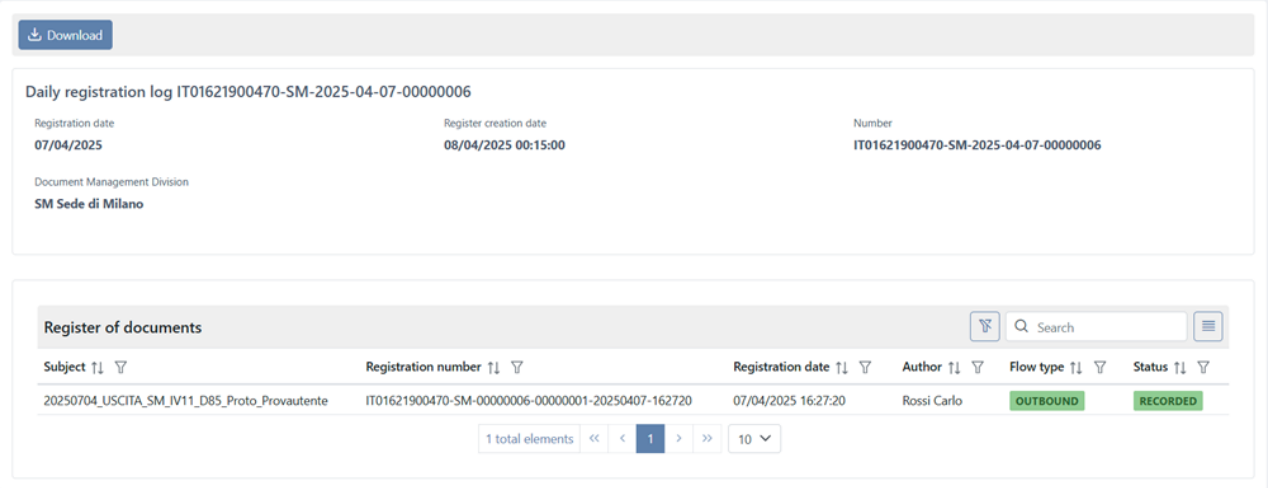

Figure 28. Daily registration log detail page.

This page is divided into two sections. The upper part displays the information that uniquely identifies the registration: Registration date, Register creation date, Number, and the Document Management Division.
The lower section lists all the registration that make up the daily registration log.

Below is a brief description of the fields present in the list:

- **Subject**: this is the subject of the registration added during the registration process;
- **Registration number**: this is the registration number with the following structure: `VAT number of the administration + DMD code + Year + Unique progressive number`;
- **Registration Date**: the date when the registration was added;
- **Author**: the author of the registration;
- **Flow type**: the flow type of the registration, which can be internal, inbound, or outbound (see Register of documents).
- **Status**: the status of the registration, which, once confirmed, can only be registered or canceled.

From this section, it is possible to:

- sort the columns and filter the items in the table as described in the Console tables chapter;
- view the details of the registration to display its structure and the documents it contains;
- download the register of document by clicking the "**Download**" button located at the top left of the page. The registration is a *.csv* file listing all registrations made during the day.

The following table presents the information and a brief explanation for each item.

Field	Description
Subject	Registration subject assigned during data entry.

Field	Description
Status	It refers to the current state of the registration, as part of a register, it can only assume the values "Registered" or "Canceled".
Registration number	It refers to the unique number assigned by the system during the confirmation of the registration, and is composed as follows:
Author	It refers to the author of the registration.
Registration date	It refers to the date on which the registration is confirmed.
Year	It refers to the year of registration.
Flow type	It refers to the flow type of registration. It can take the values "*Internal*", "*Inbound*", or "*Outbound*".
DMD (Document Management Division)	It refers to the document management division of the registration.
Log registry type	It refers to the log registry type of the registration, which it is an optional value and it may be left empty. If provided, it can take the value "accession list / separate register" or "ordinary register / emergency register".
Sender VAT number	This information is present exclusively in the case of an inbound flow. It refers to the VAT number of the sender added during registration and recorded in the subjects page.
Sender Tax code	This information is present exclusively in the case of an inbound flow. It refers to the Tax code of the sender added during registration and recorded in the subjects page.
Sender name	This information is present exclusively in the case of an inbound flow. It refers to the name of the sender added during registration and recorded in the subjects page.
Sender surname	This information is present exclusively in the case of an inbound flow. It refers to the surname of the sender added during registration and recorded in the subjects page.
Sender company name	This information is present exclusively in the case of an inbound flow. It refers to the company name of the sender added during registration and recorded in the subjects page.
Sender email	This information is only available in the case of an inbound flow. It represents the email address of the sender's reference subject, as added during the registration process and present in the subjects page.
Receiver VAT number	This information is present exclusively in the case of an outbound flow. It refers to the VAT number of the receiver added during registration and recorded in the subjects page.

Field	Description
Receiver Tax code	This information is present exclusively in the case of an outbound flow. It refers to the Tax code of the receiver added during registration and recorded in the subjects page.
Receiver name	This information is present exclusively in the case of an outbound flow. It refers to the name of the receiver added during registration and recorded in the subjects page.
Receiver surname	This information is present exclusively in the case of an outbound flow. It refers to the surname of the receiver added during registration and recorded in the subjects page.
Receiver company name	This information is present exclusively in the case of an outbound flow. It refers to the company name of the receiver added during registration and recorded in the subjects page.
Receiver email	This information is only available in the case of an outbound flow. It represents the email address of the receiver's reference subject, as added during the registration process and present in the subjects page.
Sender registration date	This information is present exclusively in the case of an inbound flow. It refers to the date of the sender document added during registration.
Sender registration number	This information is present exclusively in the case of an inbound flow. It refers to the registration number of the sender document added during registration.
Classification scheme	It represents the classification scheme code added during the registration process.
Category	It represents the classification scheme category code added during the registration process.
Class	It represents the classification scheme class code added during the registration process.
Sub-class	It represents the classification scheme sub-class code added during the registration process.

6.3. Email

In this section, user can view all the email messages automatically downloaded in the Console from previously configured and enabled email accounts (see Email accounts).

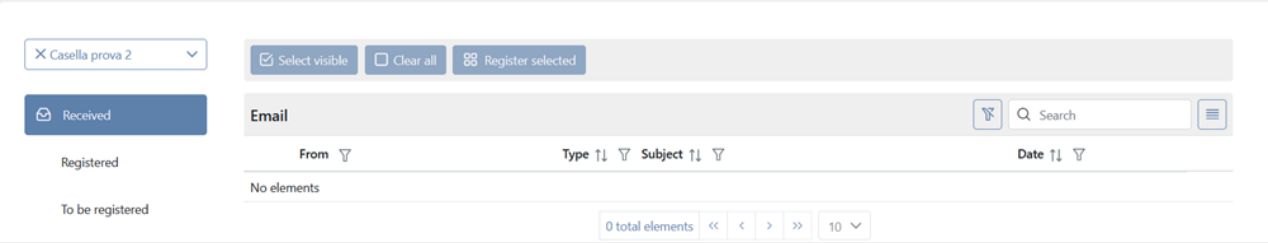

Figure 29. Email list.

The page is divided into two sections.
On the left side, user can select the email account for which he wants to view the messages, along with the message categories being managed: received messages (to be registered, registered), sent messages (to be registered, registered), and the trash, on the right side, the downloaded messages from the selected account are displayed in a list, filtered by the selected type.

At the top left of the list, all previously configured accounts are shown: by selecting the desired account, **only** the sent, received, or deleted messages downloaded in the Console from that specific mailbox will be displayed in the right section.

The icon to the left of the mailbox refers to a certified account, while a different icon indicates that the account has been disabled. Even if disabled, the account will always remain visible in the list of available accounts in order to view messages downloaded before the account was disabled.

Once the desired account is selected from the available list, it is possible to view the messages managed by that mailbox namely, received and sent messages (including those registered and to be registered in the Console), as well as deleted ones: by selecting the message type (highlighted in blue), all related emails will be displayed in the right section of the page.

	The messages downloaded from the configured email account are **exclusively** those located in the "*INBOX*" folder: any messages contained in other folders or subfolders are not downloaded.

Below are the detailed characteristics of each section.

"*Received*" section

By clicking on this section, all received messages downloaded in the Console from the previously selected mailbox are displayed in the list on the right.

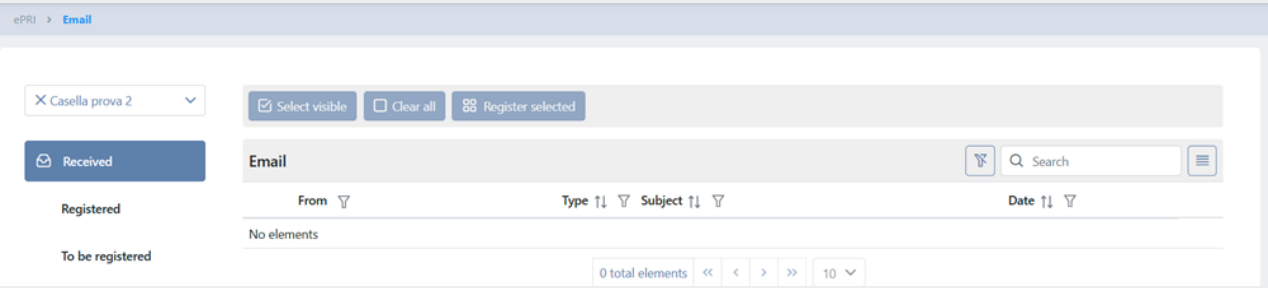

Figure 30. Received email.

The information displayed in the list is as follows:

- **From**: sender's address of the received message;
- **Type**: type of the received message. The different types and their descriptions are listed in the table below;
- **Subject**: subject of the message. If the original email contains attachments, an icon is displayed;
- **Date**: date and time the message was received.

Exclusively for unregistered messages, a button is available in the row that, when clicked, removes the corresponding message from the list, and it will no longer be downloaded from the email account but will remain visible in the "Trash" section.

Exclusively for original registered messages, there is a button in the row that, when clicked, opens the registration related

to the email.

Exclusively for messages automatically archived via Submission Information Package (SIP) of the PEC type, once enabled and configured in the Email archiving section of the email account page,a button is available in row which, when clicked, will display the details page of the corresponding submitted SIP.

The following table lists the different types of available messages.

Table 3. Message types list

Message type	Icon	Description
Accepted		Acceptance Notification of an email received.
Not accepted		Non-Acceptance Notification of an email received.
Taking charge		Email taking charge notification.
Delivery Successful		Delivery confirmation notification.
Certified email		The received email was sent from a certified email account.
Delivery error		Delivery failure notification for the received email.
Notice of delivery error		Pre-delivery failure warning notification for the received email.
Virus detection		Detection of a virus in the received email.
Ordinary email		The received email was sent from a ordinary email, non-certified email account.

From this section, it is possible to simultaneously register multiple email messages: the selectable messages are exclusively those of certified or ordinary mail types that have not been previously registered or that are registered in draft status.
Messages can be selected manually (by ticking them individually) or automatically by clicking the "**Select Visible**" button (in which case only the selectable messages displayed on the current page will be ticked).
Clicking the "**Clear all**" button will uncheck all previously selected messages, regardless of the page they are on.
By clicking the "**Register selected**" button, all selected messages will be automatically registered following the procedures described in the *Automatic registration from email* section of the Add a register of documents paragraph.

Upon confirming the bulk registration, a summary window will be displayed showing detailed information about the outcome of the operation: the total number of messages to be registered, the total number of messages successfully registered without errors, and the total number of messages registered with errors and therefore saved as drafts, in this latter case, by clicking the "**Export error details**" button, it is possible to download a *.csv* file listing all messages registered as drafts along with the detected anomalies.

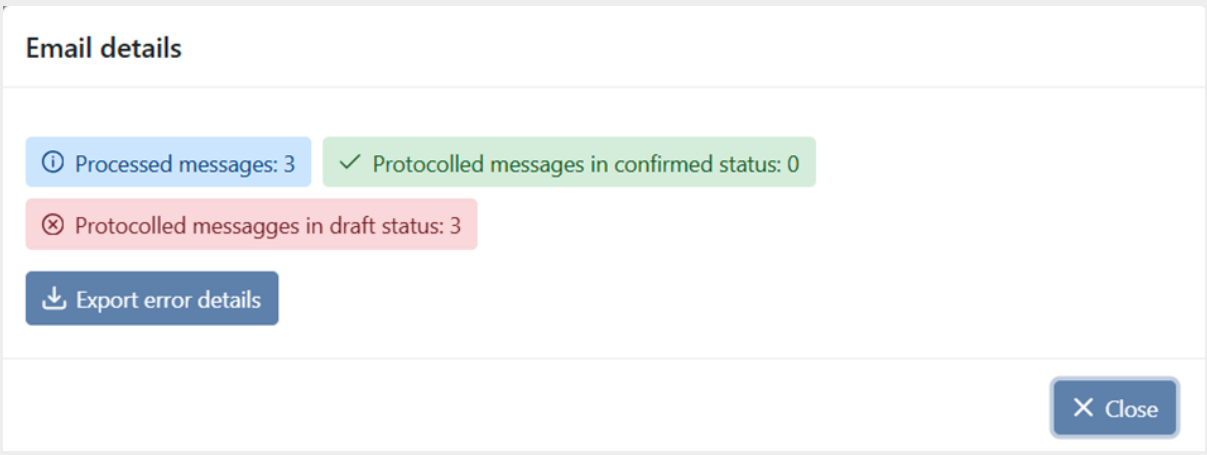

Figure 31. Email details.

By clicking on a single row in the list, you can view the details of the selected email (see Email detail page).

"*Registered*" section

By clicking on this section, all received email messages, excluding notifications, downloaded from the selected mailbox and previously registered in the Console, are displayed in the list on the right.

In the message list of this section, the same information already described in "*Received Email Messages*" and includes the filterable column "*Status*", which shows the status of the related registration, this status can take on the values already described in the Register of documents paragraph.

These messages **cannot** be deleted as they have already been registered; therefore, the button will not be visible in the row.
To open the corresponding registration, simply click the button located on the right side of the row.
The button will be visible exclusively for messages archived through the creation of a PEC-type Submission Information Package (SIP); by clicking it, the detail page of the corresponding SIP will be displayed.

Exclusively messages that have been registered but are in draft status can be re-registered in bulk by selecting them and clicking the "**Register selected**" button.
For faster registration, it is recommended to filter the list by the registration status "Draft" and then proceed with selection and bulk registration.

Clicking on a row in the list allows to view the details of the selected email (see Email detail page).

"*To be registered*" section

By clicking on this section, all received email messages, excluding notifications, that have been downloaded from the selected mailbox and not yet registered in the Console are displayed in the list on the right.

The message list in this section displays the same information already described in "*Received Email Messages*".

The button is not visible, the emails have not yet been registered, clicking the button deletes the corresponding message from the list and prevents it from being downloaded again from the email account but the message will then be visible in the "**Trash**" section.
The button will be visible exclusively for messages archived through the creation of a PEC-type Submission Information Package (SIP); by clicking it, the detail page of the corresponding SIP will be displayed.

As these messages are yet to be registered, it is possible to proceed with bulk registration as described in the "*Received*" section by selecting the relevant emails and clicking the "**Register selected**" button.

By clicking on a single row in the list, user can view the details of the selected email (see Email detail page).

"*Sent*" section

By clicking on this section, all sent messages downloaded into the Console from the previously selected mailbox are displayed in the list on the right.

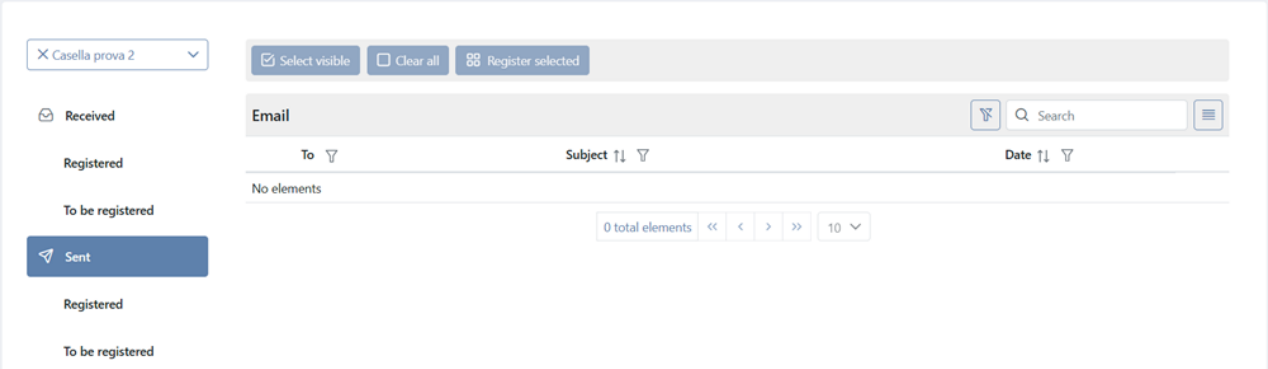

Figure 32. Sent messages.

The information displayed in the list is as follows:

- **To**: Email address(es) of the receiver of the sent message;
- **Subject**: Email subject. If the email contains attachments, an icon is displayed:
- **Date**: the date and time the email was sent.

Exclusively for unregistered messages, a button is present in the row that, when clicked, deletes the corresponding message from the list. The message will no longer be downloaded from the email account but will be visible in the "**Trash**" section.

Exclusively for registered messages, there is a button in the row that, when clicked, opens the registration related to the email.

Exclusively for messages automatically archived via Submission Information Package (SIP) of the PEC type, once enabled and configured in the *Email archiving* section of the mail account page,a button is available in row which, when clicked, will display the details page of the corresponding submitted SIP.

Clicking on a row in the list allows to view the details of the selected email (see Email detail page).

"*Registered*" section

By clicking on this section, all sent email messages, excluding notifications, downloaded from the selected mailbox and previously registered in the Console are displayed in the list on the right.

The message list in this section displays the same information already described in "*Sent Email Messages*" and includes the filterable column "*Status*" which shows the status of the related registration, this status can take the values already described in the Register of documents paragraph.

These messages cannot be deleted as they have already been registered, therefore, the button will not be visible in the row.
To open the corresponding registration, simply click the located on the right side of the row.
The button will be visible exclusively for messages archived through the creation of a PEC-type Submission Information Package (SIP); by clicking it, the detail page of the corresponding SIP will be displayed.

Exclusively messages that have been registered but are in draft status can be re-registered in bulk by selecting them and clicking the "**Register selected**" button.
For faster registration, it is recommended to filter the list by the registration status "Draft" and then proceed with selection and bulk registration.

Clicking on a single row in the list allows user to view the details of the selected email (see Email detail page).

"*To be registered*" section

By clicking on this section, all sent email messages, excluding notifications, downloaded from the selected mailbox and previously registered in the Console are displayed in the list on the right.

The message list in this section displays the same information already described in "*Sent Email Messages*".

The button is not visible, because the emails have not been registered, and clicking the button the corresponding message is removed from the list and will no longer be downloaded from the email account, but it will be visible in the "**Trash**" section.

The button will be visible exclusively for messages archived through the creation of a PEC-type Submission Information Package (SIP); by clicking it, the detail page of the corresponding SIP will be displayed.

As these messages are yet to be registered, it is possible to proceed with bulk registration as described in the "*Received*" section by selecting the relevant emails and clicking the "**Register selected**" button.

Clicking on a single row in the list allows you to view the details of the selected email(see Email detail page).

"*Trash*" section

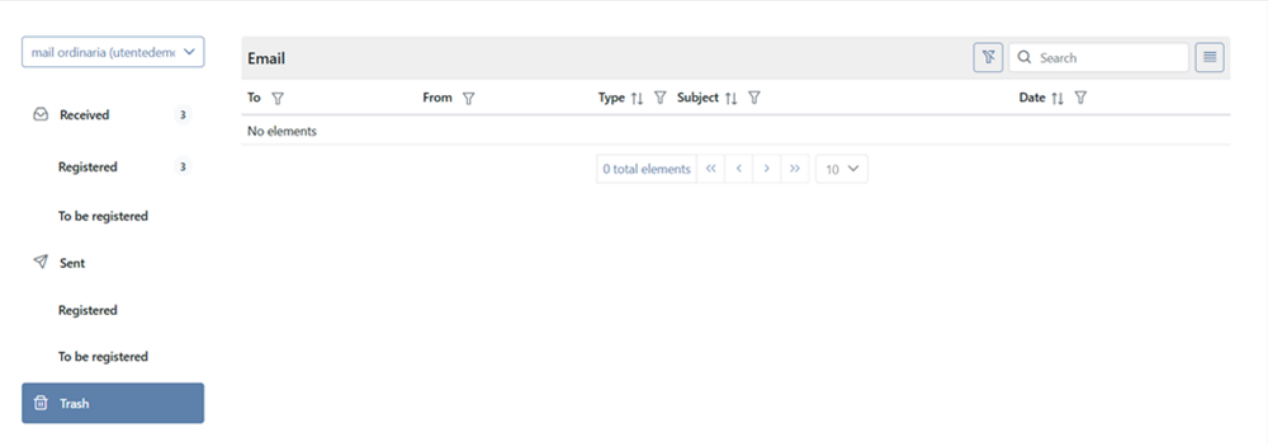

Figure 33. Trash emails.

By clicking on this section, all previously deleted sent or received messages are displayed in the list on the right.

The information displayed in the list is as follows:

- **To**: address of the receiver or receivers of the message;
- **From**: address of the message sender;
- **Type**: Message type. The types and their descriptions are the same as those listed in the "*Received*" section;
- **Subject**: subject of the email. If the email contains attachments, an icon is displayed;
- **Date**: the date and time the email was sent or received.

By clicking the button the emails will be restored to their respective folders, either Sent or Received messages. The button will be visible exclusively for messages archived through the creation of a PEC-type Submission Information Package (SIP); by clicking it, the detail page of the corresponding SIP will be displayed.

Clicking on a single row in the list allows user to view the details of the selected email (see Email detail page).

6.3.1. Email detail page

Clicking on the row of a message (sent, received, or deleted) user can access the detail page.

Received message detail page

The detail page of a received message, regardless of its type (registered or to be registered), is divided into two sections: a top section and a central section.

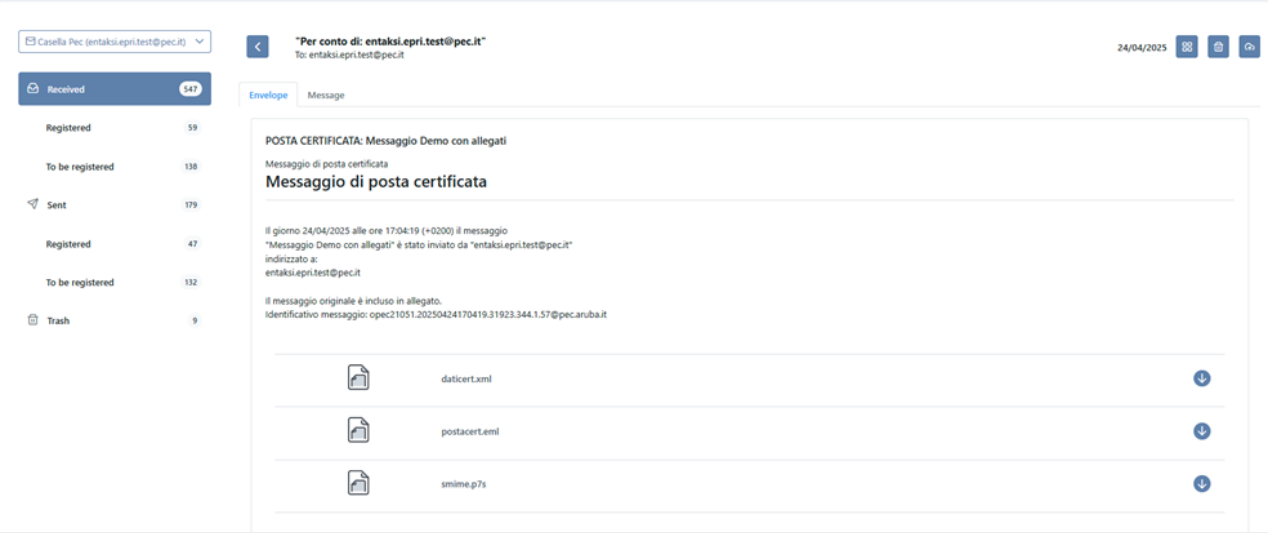

Figure 34. Received message detail.

In the upper-left section, the sender and receiver information is displayed, and by clicking the button it is possible to return to the main page, on the right are shown the date and time of message received, and by clicking the button , visible only for ordinary and certified emails (not for notifications), it is possible to manually register the message (see Add a register of documents section "*Registration from Email*").
If the message has already been previously registered, the button is not visible; instead, a different button is shown, which, when clicked, displays the page with the corresponding registration of documents.

For messages that have not been previously registered, a button is visible which, when clicked, deletes the message and prevents it from being downloaded again from the email account, however, the message remains visible in the "**Trash**" section.

The button is visible **exclusively** for messages that have been automatically preserved through PEC-type Submission Information Packages (SIP), and when clicked, it displays the detail page of the corresponding submitted information packaged.

Additionally, a section is displayed below, containing main information related to the registration itself, including the registration number, registration date, author, and registration status.

In the case of Certified Email (PEC) messages, the central section is further divided into two additional parts: "*Envelope*" and "*Message*".

When a certified email account receives a message containing text and an attachment, the information is included in the file "*postacert.eml*", along with two additional files: "*daticert.xml*" and "*smime.p7s*".
The *Envelope* section summarizes the information related to the original received email and contains the three attachments described earlier.
By clicking the button , on the right side of each attachment, it is possible to download the file.
This section is present in all types of received messages.

The *Message* section, present **exclusively** when the displayed message is a *Certified Email* (PEC) type, shows the email text along with any attachments.
By clicking the button , on the right side of each attachment, it is possible to download the file.

Sent message detail page

The sent email detail page is divided into two sections: one at the top and one in the center.

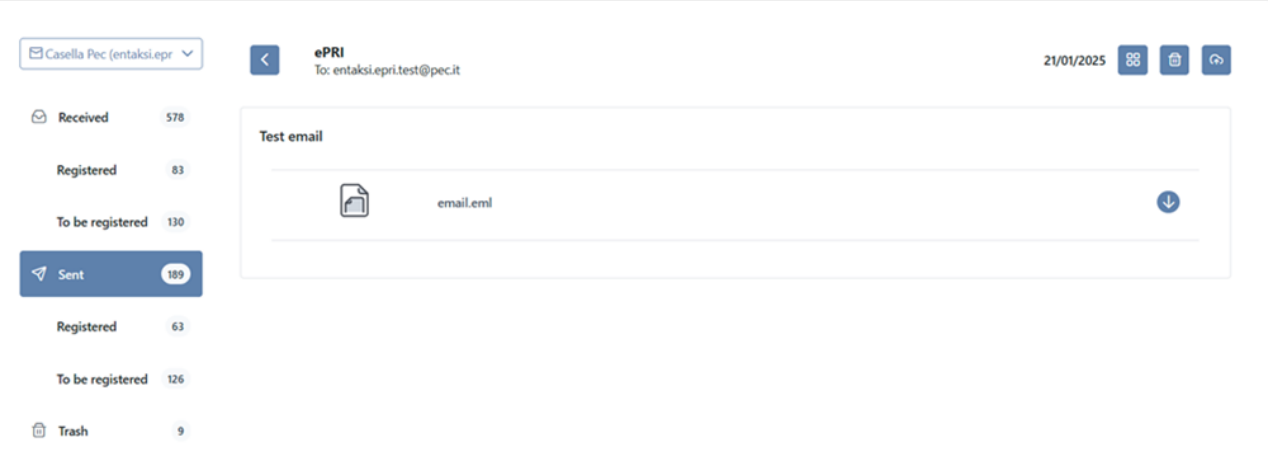

Figure 35. Sent message detail.

In the upper-left section, the sender and receiver information is displayed, and by clicking the button it is possible to return to the main page, on the right are shown the date and time of message received , and by clicking the button it is possible to register the message (see. Add a register of documents section "*Registration from Email*").

If the message has already been previously registered, the button is not visible; instead, a different button is shown, which, when clicked, displays the page with the corresponding registration of documents.

For messages that have not been previously registered, a button is visible which, when clicked, deletes the message and prevents it from being downloaded again from the email account, however, the message remains visible in the "**Trash**" section.

The button is visible **exclusively** for messages that have been automatically preserved through PEC-type Submission Information Packages (SIP), and when clicked, it displays the detail page of the corresponding submitted information packaged.

Additionally, a section is displayed below, containing main information related to the registration itself, including the registration number, registration date, author, and registration status.

The central section displays the text of the sent email along with any attachments.
By clicking the button , on the right side of each attachment, it is possible to download the file.

Trash message detail page

The detail page displayed is the same as the one previously described for both sent and received messages.
Divided into two sections, the upper-left section displays the sender and receiver information, and by clicking the button, it is possible to return to the main page, on the right, the date and time the message was sent are shown.

By clicking the button the messages will be restored to their respective folders, either sent or received.

The button is visible **exclusively** for messages that have been automatically preserved through PEC-type Submission Information Packages (SIP), and when clicked, it displays the detail page of the corresponding submitted information packaged.

In the case of Certified Email (PEC) messages, the central section is further divided into two additional parts: "*Envelope*" and "*Message*". For sent emails, the original message text is displayed along with any attachments.
All files can be downloaded by clicking the button .

6.4. Folders

On the **Folders** page, all folders entered into the system are displayed in a list.

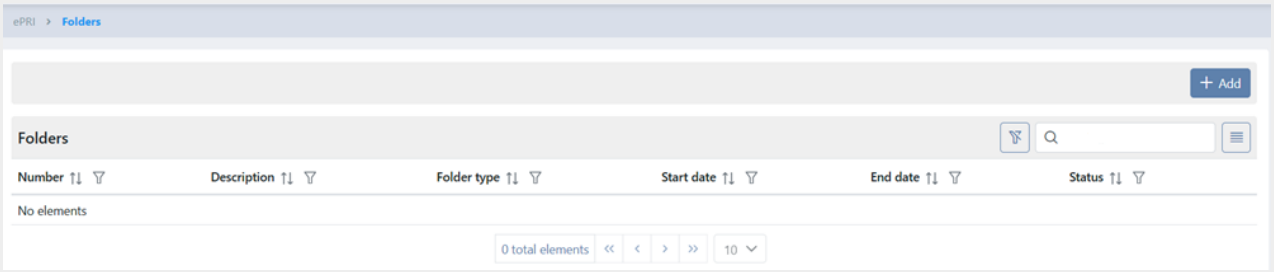

Figure 36. Folders.

Below is a brief description of the fields and filters available in the list:

- **Number**: the unique number automatically assigned by the system when a new folder is saved, in the format `producer code + document management division code + classification code + year + unique progressive number`;
- **Description**: the subject of the folder;
- **Folder type**: the type of folder that can be selected from the available options in the system, namely: *Affair*, *Activity*, *Natural person*, *Legal entity*, *Administrative Procedure*;
- **Start date**: the start date of the folder's validity;
- **End date**: the end date of the folder's validity. This is filled in only if the folder is in "Closed" status;
- **Status**: the status of the folder, which can take on the values listed in the following table.

Table 4. Status list.

Status	Description
OPEN	The folder can be modified (by accessing the detail page) or deleted (by clicking the button in row or the dedicated button on the detail page).
CLOSED	The folder cannot be modified or deleted. When accessing the detail page, the data is displayed in read-only mode.

From this section, it is possible to:

- sort columns and filter the items in the table, as described in the Console tables chapter;
- access the folder details by clicking on the individual row;
- add new folders, if authorised, by clicking the "**Add**" button located at the top right.

6.4.1. Folder detail page

To add a new folder, click the "**Add**" button located at the top right while to view or modify a previously added folder, just click on the row of the folder of interest.
In both cases, the folder's detail page will be displayed, which is divided into two sections: a header section where all the information related to the folder is shown, and a lower section where all the register of documents included in the folder are listed.

Add and update a folder

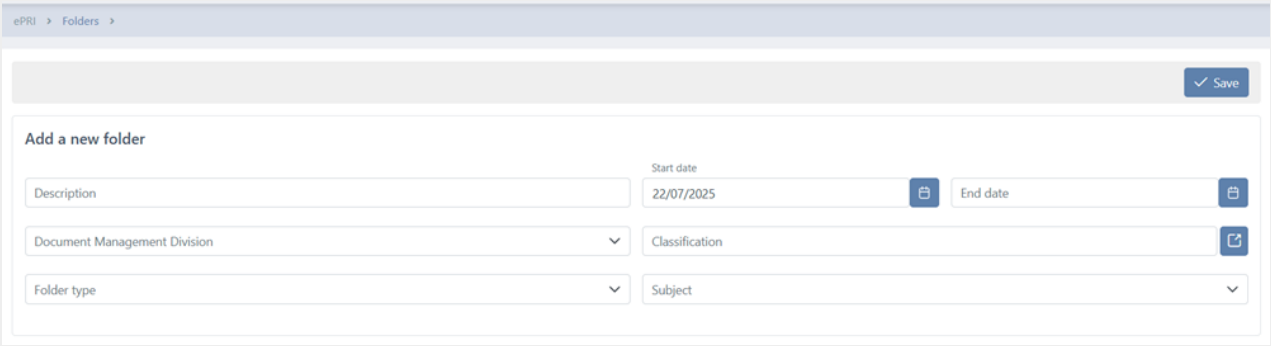

Figure 37. Add folder.

The required data are:

- **Description**: the subject of the folder, a free-text description used to uniquely identify the folder. Mandatory field;
- **Start date**: the start date of the folder's validity. Mandatory data. During creation, the system will propose the current date, which can be modified to a past date if necessary. It is not possible to enter a folder with a start date in the future;
- **End date**: the end date of the folder's validity. It is not possible to enter an end date in the future. The user can only input past dates or the current date of insertion;
- **Document management division**: the document management division assigned to the folder. Mandatory data;
- **Classification**: the classification assigned to the folder. Mandatory field;
- **Folder type**: the type of folder, selectable from those available in the system, namely *Affair*, *Activity*, *Natural Person*, *Legal Entity*, *Administrative Procedure*. Optional field;
- **Subject**: the subject related to the folder. Mandatory data only if the folder type is specified as "*Natural person*" or "*Legal entity*".

By clicking the "**Save**" button located at the top right, the new added folder will be saved, if all mandatory fields have been correctly filled in.

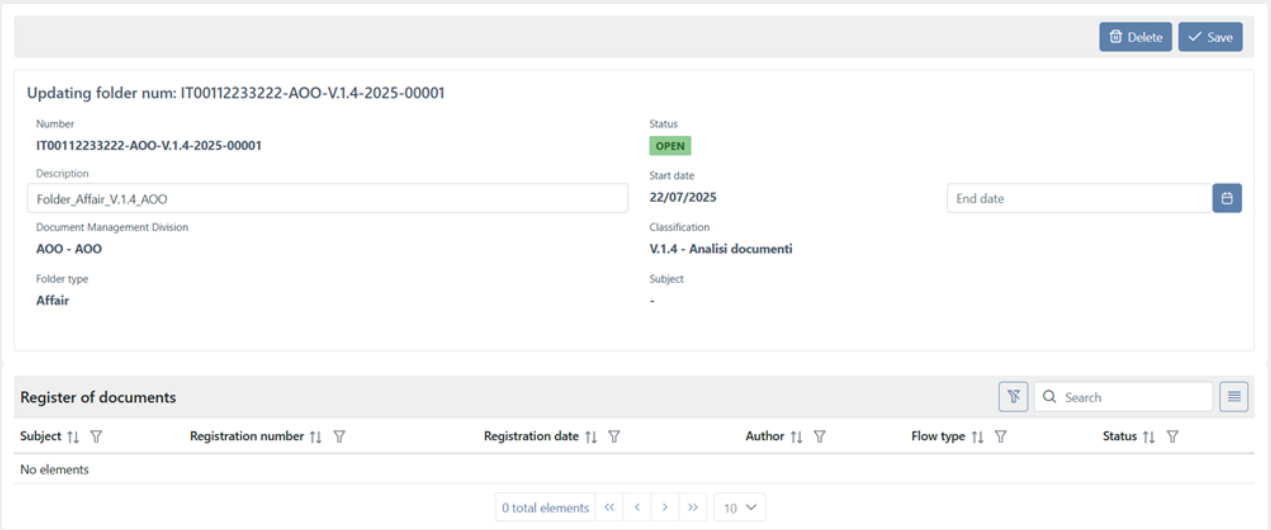

Figure 38. Updating folder.

The system will automatically assign a unique, non-editable number composed as follows `producer code + document management division code + classification code + year + unique progressive number`, where:

- `producer code`: corresponds to the VAT number of the company;
- `document management division code`: corresponds to the code of the document management division added during registration;

- `classification code`: corresponds to the code of the classification schedule added during registration;
- `Year`: the year of the folder's start validity, took out from the value added in the "*Start date*" field during registration;
- `unique progressive number`: A unique 5-digit progressive number assigned automatically by the system, based on the producer code, DMD code, classification code, and year.

Without an end date, the folder is in "*Open*" status.
If the folder is in "*Open*" status, its description can be modified, an end date can be added, or it can be deleted.
If the folder is in "*Closed*" status, it can no longer be deleted, and the data will be displayed in read-only mode, meaning it cannot be modified.

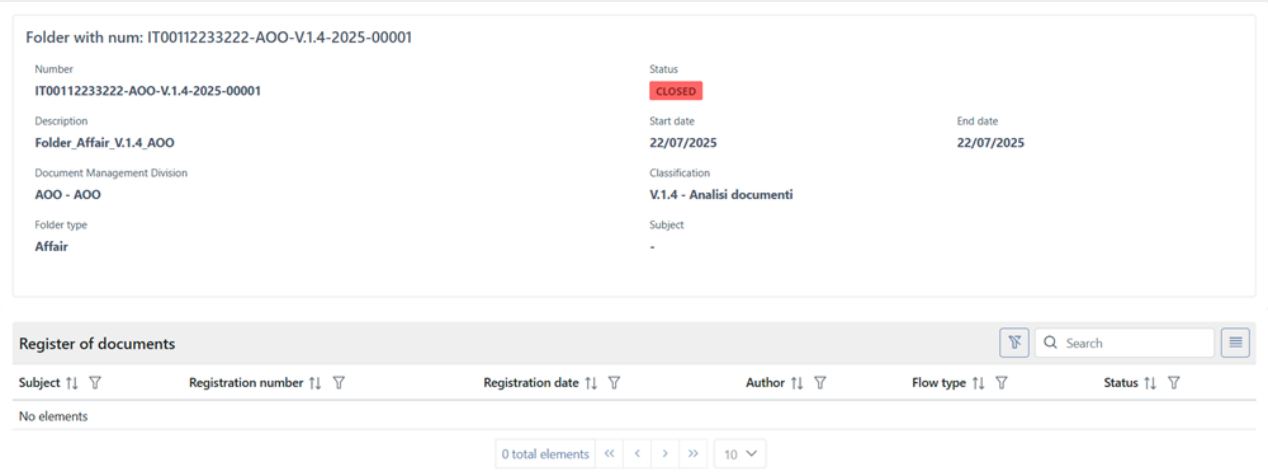

Figure 39. Close folder.

Register of documents included in a folder

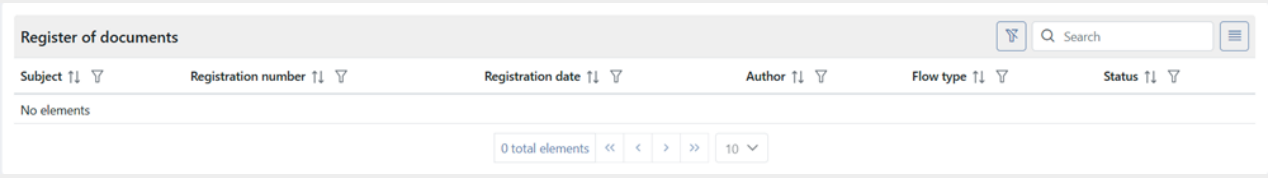

Figure 40. Register of documents

In this section, all register of documents included in the folder are displayed.
Below is a brief description of the fields present in the list:

- **Subject**: the subject of the registration, which is assigned during the registration process;
- **Registration number**: the registration number with the structure
  `VAT number of the administration + DMDcode + Year + xxxxxxxx` for draft registration, or
  `VAT number of the administration + DMDcode + Year + Unique progressive number` for confirmed or canceled registration;
- **Registration date**: the date when the registration was registered;
- **Author**: the author of the registration;
- **Flow type**: the flow type of the registration, which can be *internal*, *inbound*, or *outbound* (see Register of documents)
- **Status**: the status of the registration, which can be draft, registered, or canceled (see Register of documents)

From this section, it is possibile to:

- sort the columns and filter the items in the table, as described in the Console tables chapter;
- view the details of the registration to examine its structure and the documents contained in it by clicking on the row of the registration of interest.

6.5. Configurations

By clicking the "Configurations" menu, you can set up configurations for the correct display and input of data managed by the ePRI service.

Specifically, in the "*Email accounts*" section, user can configure one or more email accounts from different providers (both PEC and non-PEC) for viewing and managing emails on the "*Email*" page.
In the "*Subjects*" section, user can enter the relevant company subjects.

6.5.1. Email accounts

On the **Email accounts** page, all email accounts configured in the system are displayed in a list.

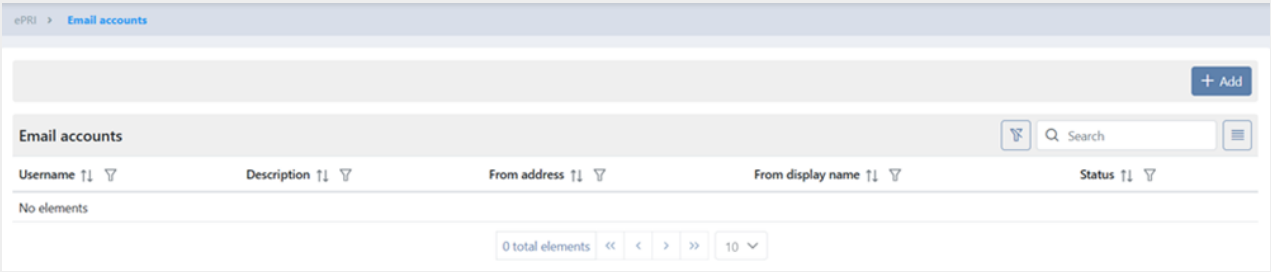

Figure 41. Email account list.

Below is a brief description of the fields and filters available in the list:

- **Username**: the username entered in case of the account authentication setup;
- **Description**: the description provided in the corresponding field during account configuration;
- **From address**: the email address entered in the relevant field during account configuration;
- **From display name**: the sender's name entered in the appropriate field during account setup;
- **Status**: the status can be either "*Enabled*" or "*Disabled*". If *Enabled*, the email account is active, and sent and/or received emails will be downloaded into the Console and displayed on the "*Email*" page, if *Disabled*, the email account is no longer active, and sent and/or received emails will no longer be automatically downloaded into the Console; only the emails downloaded before the deactivation will remain visible.

From this section, it is possible to:

- sort columns and filter items in the table, as described in the Console tables chapter;
- access email account details page by clicking on an individual row;
- add new accounts, if authorised, by clicking the "Add" button.

Adding or updating an Email Account

By clicking the "**Add**" button at the top right of the email accounts list on the *Email Accounts* page, the system will display a secondary page where the user can configure and enable email accounts for the automatic download of sent and/or received emails into the Console, to proceed with their registration.

By clicking the "**Save**" button at the top right will save the entered or updated data.

To update previously entered data, click on the desired account in the list, make the necessary changes, and save.

The *Email accounts* page is divided into sections to facilitate both data entry and data display.

Email account

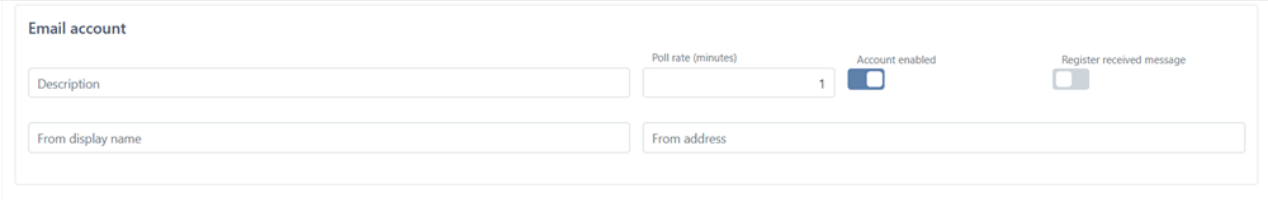

Figure 42. Email account description.

In this section, user can enter the general information related to the account, such as the account description, the sender, and the sender's email address.
The description and the sender's email address are the descriptive details displayed in the accounts list in the left section of the Email page.

The *poll rate* indicates how often (in minutes) the service should download messages from the mailbox.

The "*Account enabled*" field specifies whether the mailbox is active or not: by default, a new mailbox is automatically enabled (the checkbox is set to *true*).

If user wish to disable an account, simply uncheck the box and save: the disabled account will appear with an icon ✕ in the list of available accounts on the *Email* page.

Mail server

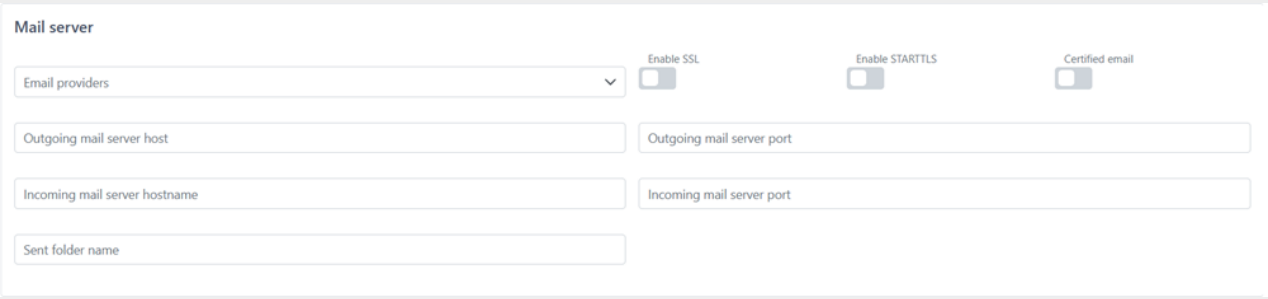

Figure 43. Mail server section.

In this section, user can correctly configure the mail server used to automatically download all sent and received messages.
To simplify the setup, user can select one of the available providers from the "*Email Providers*" list: the default settings for the selected provider will be filled in automatically.

If the selected server is a certified email (PEC) server, the account will be marked with a specific icon ✉ on the *Email* page.

Authentication

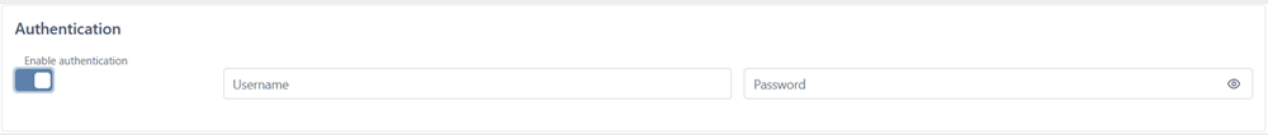

Figure 44. Mail authentication section.

If authentication is required to access the server specified in the previous section, user must check the "*Enable authentication*" field (which is disabled by default) and enter the username and password credentials.

Email archiving

Figure 45. Mail archiving section.

By enabling the "*Send to preservation system*" field (disabled by default), emails will be **automatically** archived on a weekly schedule through the creation of a *PEC*-type Submission Information Package, which will include all related *.eml* files.
To complete the automation configuration, it is necessary to specify the starting date from which the sent or received emails will be included in a PEC submission information package, the frequency at which the submission information packages should be created, the classification scheme under which the emails should be archived, in order to correctly populate the index of the PEC Submission Information Package.

Register of documents configurations

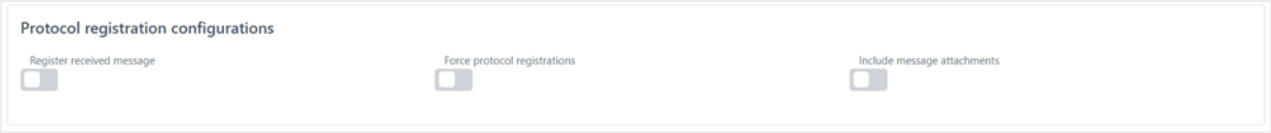

Figure 46. Automatic registration.

The "*Register received message*" field, if checked, activates the automatic email registration process as described in the chapter Register of documents, under the section "*Registration from Email*".

The "*Force registrations*" field, if checked, enables the "forced" registration in cases where the sender's or receiver's email address is of the "email only" type (or did not report the information of the displayed name), the registration will be confirmed even if the mandatory subject information in the daily digital registration is missing, and those fields will be displayed with empty values (see Register of documents).

The "*Include message attachments*" field, if checked, enables the automatic inclusion of email attachments during the registration process: in addition to the *.eml* file, the registration will also include the attachments.
If this option is not enabled, registrations generated from emails will include only the *.eml* file, regardless of the presence of attachments in the original mail.

Default value for registrations

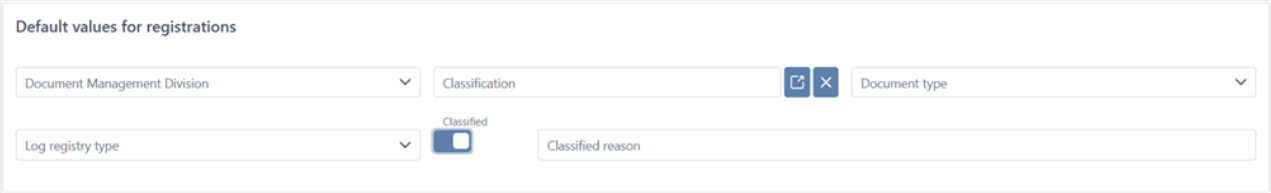

Figure 47. Default values for registrations section.

In this section, user can set default values to simplify the registration process from emails: the data entered in this section will be automatically included in registration created from emails, whether manually or automatically, as described in the Register of documents paragraph.

To select a node from the classification scheme, click the button  located to the right of the corresponding field: the currently active classification scheme will be displayed (i.e., the one confirmed with a start date earlier than the current date and no end date added, or an end date later than the current date). If no items are displayed, you must enter a valid classification scheme as explained in the Adding a classification scheme section.
Select a node at the last level of the chosen branch and click the "**Confirm**" button.

If user wishes to delete a previously entered value, click the corresponding button  .
The data related to the classification (mandatory data) and the folder (optional data) are strictly connected: when a

classification is selected, only folders with the same classification will be proposed.
If a folder is selected (without having previously selected the classification), the system will automatically populate the classification present on the folder.

The confidentiality option is disabled by default: to enable it, click the field and, if necessary, enter the confidentiality description (this field is mandatory for a registration marked as confidential).

All the fields in this section are intended for registration and can be partially filled in: in such cases, the remaining fields must be completed manually during the registration process.
If the "*Register received message*" option is active, the registrations created will remain in draft status until all required fields are completed.

6.6. Subjects

In this section, user can view, add, and edit the company's subjects, which are displayed in a list.

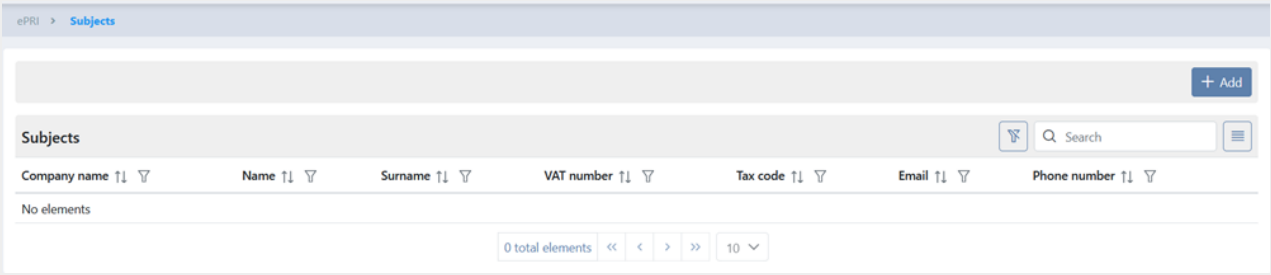

Figure 48. Company's subjects list.

Below a brief description of the fields displayed in the list.

- **Description**: a short description assigned to the subject during data entry;
- **First name**: the subject's first name;
- **Last name**: the subject's last name;
- **VAT Number**: the subjets's VAT identification number;
- **Tax Code**: the subject's personal tax code;
- **Email**: the subject's email address;
- **Phone number**: the subject's phone number.

From this section, user can:

- sort columns and filter the items in the table, as described in the Console tables chapter;
- access the subjects details by clicking on a specific row;
- add new subjects by clicking the "**Add**" button.

To add a new subject, user must select a type from the available options, "*Foreign administration*", "*Italian administration*", "*Natural person*", or "*Legal person*": the mandatory fields required to save data entry depend on the selected subject type.
A uniqueness check prevents saving multiple subjects with the same email address.
Additionally, it is possible to associate a contact with a subject by selecting them from the list provided by the service; the subjects included in this list are exclusively those saved in the system as natural persons.

Click the "**Save**" button to save the data entry and the newly added subject will then appear in the subjects list.
To delete a subject, click the button on the corresponding row in the list.

7. eCON - Preservation

Once logged into the Entaksi Console, to access the interface of ePRI service you can click on the dashboard button "**Preservation**", so the "**Submission Information Packages**" page opens, or you can select one of the submenu items of the "**eCON**" main menu: each item opens the respective page.

The "**eCON**" menu contains:

- **Uploading SIP**: in this section it is possible to manually upload .zip SIP generated by other systems procedures (Uploading

SIP).

- **SIP list**: the list of all the information packages ready for storage (SIP) with the related identification data. See chapter SIP List for the description of the list items.
- **AIP list**: the list of Archival Information Packages (AIP) stored in the system with the related identification data. See chapter AIP List for the description of the list items.
- **Search and request documents**: it allows you to search stored documents and request DIP(s).
- **Search and document collections**: the list of the last researches made on the system (Search and document collections).
- **DIP list**: the list of all the required DIP packages. See chapter DIP list for the description of the list items.

7.1. Preservation process

The process of IT document preservation consists of several phases, involving the Producer, the Company, and any third-parties Users.

All documents submitted to the preservation system must be distinguished by a set of mandatory metadata defined by the AgID Linee Guida (Guidelines).
The metadata managed by the system apply to various entities managed, documentary units, and archived files, making possible the search and storage of archives according to the minimum set defined in Allegato 5 of AgID "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" which the system can extend this with an additional metadata model according to the different documentary types.
Metadata can be linked to the described object and subsequently stored in two ways: as (*embedded*) metadata, recorded in index files at the file or documentary unit level, or as (*external*) objects, always referenced in the index but stored in separate files. Entaksi used *embedded* metadata until July 8, 2024, when the new archival index with *external* metadata was implemented.

The following provides an overview of the general framework of the preservation process, describing the various stages that documents go through, from submission to permanent preservation.

7.1.1. Methods of acquiring submission packages

The **Submission Information Packages** (SIP) containing the documents to be preserved and uploaded into the system as described in the Uploading SIP are subjected to a validation process that checks their integrity and a backup, where the packages are stored until the documents are included in an archival package.
All operations performed on the SIP are recorded and stored in the system through an operations log.

7.1.2. Acceptance of submission packages and generation of the confirmation of receipt

If the checks on the received Submission Information Packages are successful, the documentary units contained in them are transferred to the temporary area for the creation of Archival Information Packages.
At the end of this operation, the system prepares the data for generating the confirmation of document receipt (i.e., for the creation of a Confirmation of Receipt).
The **Confirmation of Receipt** (Rapporto di versamento, (RDV) in italian) is automatically generated and relates to a specific SIP, uniquely identified by the Preservation System.
The confirmation of receipt is an XML file containing the index of the SIP it references, along with information processed during validation, it includes data that determines the immutability of the archival units it contains, such as the hash of each file within the SIP.

The time reference containing the acceptance date of the Submission Information Package is represented by the ISO 8601 format in the element /rdv/dataElaborazione.
The Confirmation of Receipt is digitally signed by the Preservation Service Manager.

The processing and digital signature of the confirmation of receipt and the document archiving activities are recorded in the log of operations related to the acquisition of the SIP.

The Confirmation of receipt is kept for the entire preservation period of the documents within the SIP, based on the document with the longest retention period.

7.1.3. Preparation and management of archival information packages

The documentary units of a successfully verified SIP are placed in the archival register identified during validation, in a temporary area dedicated to the creation of a new AIP.

The creation of the **Archival Information Package** (AIP) involves reviewing the contents of the temporary areas of each archival register, assembling the archival information package index, applying the digital signature of the Preservation Service Manager and a timestamp, and including it in the AIP.
The various phases include:

- identification of the previous Archival Information Package;
- preliminary verification for the creation of Archival Information Packages;
- closure of the Archival Information Package.

The identification of the previous AIP involves locating the last closed package within the same archival register.
If there are no PDAs in the register, the new package will be numbered 1; otherwise, the package number will be incremented by one from the previous package.

7.1.4. Preparation and management of the dissemination information package for exhibition purposes

The system allows the user to search for and extract preserved objects display or dissemination of the same through **Dissemination Information Packages** (DIP).

The Dissemination Information Package is made available as a ZIP file containing:

- a dissemination index digitally signed by the Preservation Service Manager;
- the documentary units corresponding to the selection criteria;
- the set of preservation evidence.

7.2. Uploading SIP

If you want to upload an already formed SIP, you can use the "Uploading SIP" function in the eCON menu.

With ePRI it is also possible to upload .zip files produced by other software as long as they have a layout compliant with current legislation.

The SIP must be a file in .zip format, with the possibility of choosing between the types of specific "Format".

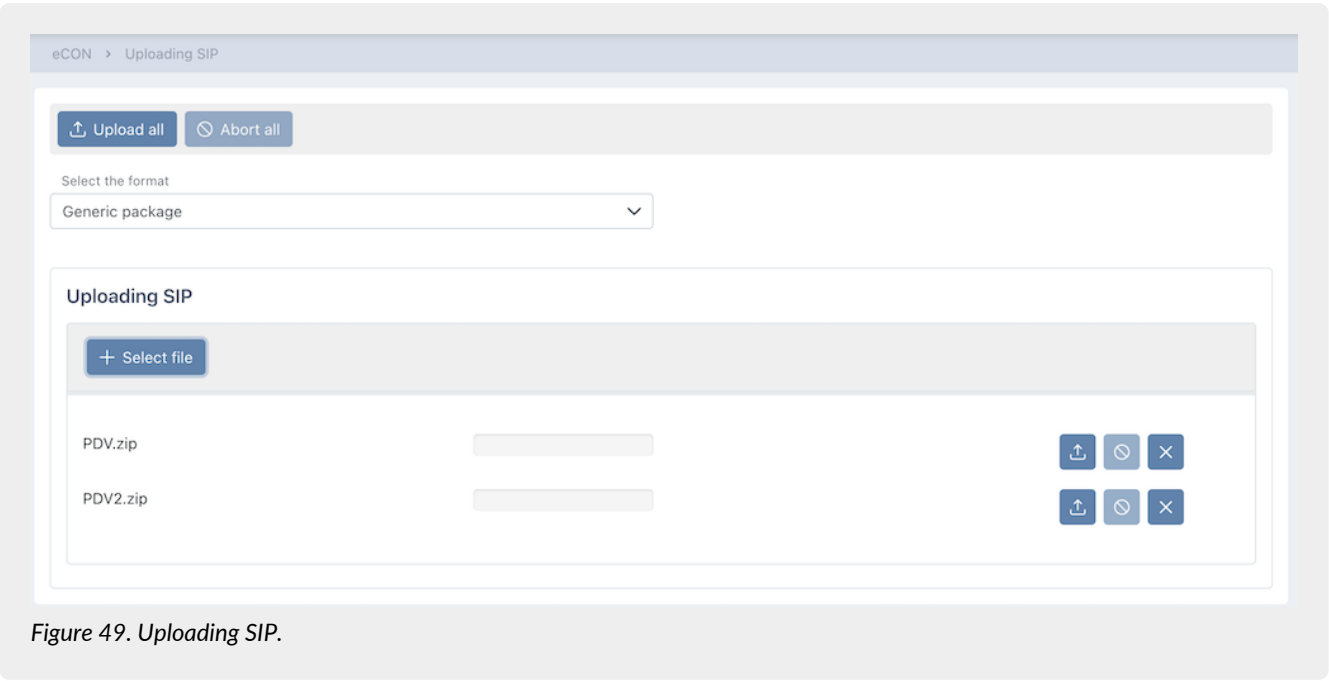

Figure 49. Uploading SIP.

Technical specifications of the .zip file format and of index types are described in the manual "UM 20150928 eDoc API User

Manual" available on the site at the following link:
https://www.entaksi.eu/pdf/docs/doc_services/UM_20150928_Manuale_utente_eDoc_API.pdf.

To upload the package:

- select the format of document you wish to upload;
- click on the "**Select file**" button and select one or more packages, or simply drag them into the section;
- by clicking on "**Upload all**" all the packages in the section are imported into the system at the same time;
- by clicking on "**Abort all**" the previously started import is aborted: in any case, the files already successfully uploaded are not aborted and they are present in the system;
- by clicking the keys in the single file row:
  - : **only** the relative file is uploaded;
  - : the import of the single file is aborted, but only if it is still in progress and not completed;
  - : the single file is removed from the list.

The "**Previous preservation system package**" option, which is **exclusively** active only after a commercial agreement for each individual company, allows you to upload a Submission Information Packages from another preservation system.

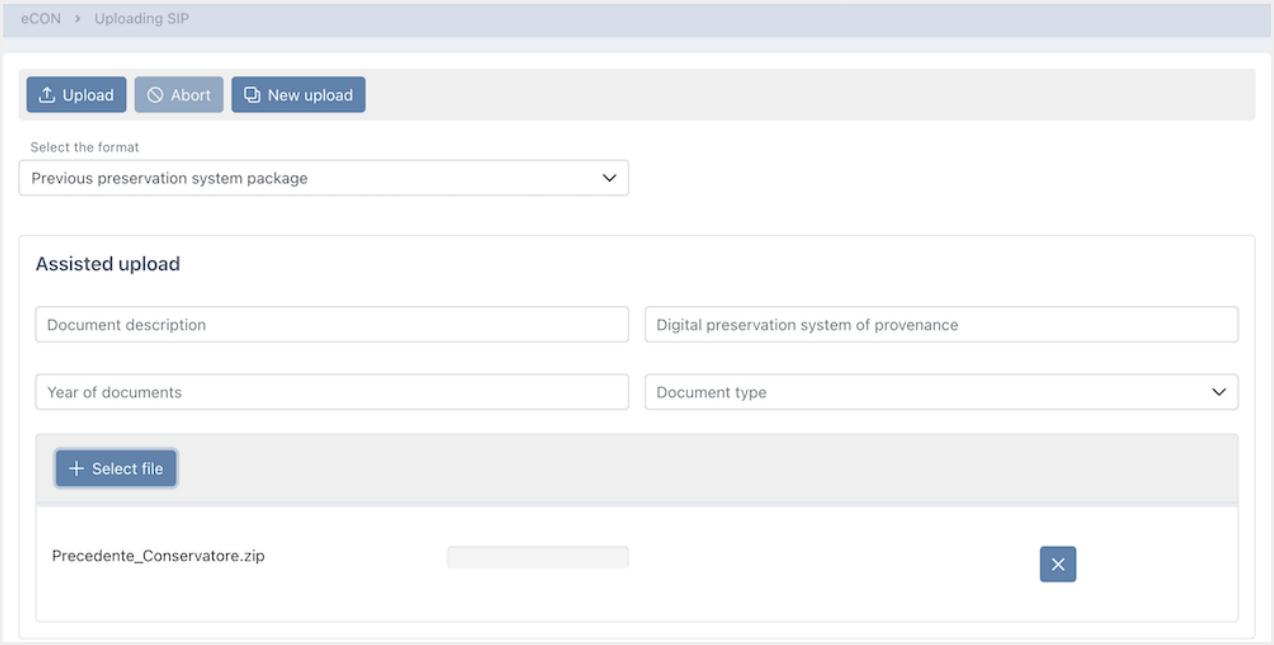

Figure 50. Previous preservation system package upload

This function allows you to load any file from a previous preservation system by indicating the items: "Document description", "Digital preservation system of provenance", "Year of documents". In order to enter the file, click on the "**Select file**" button or drag the file directly into the section.

By clicking on the button the file will remove and you will be able to select another file.
By clicking on the "**Upload**" button the files will import into the system and by clicking on the "**Abort**" button the import will abort only if it has not already finished.
By clicking on the "**New upload**" button, the page will initialize again to allow you to enter another package.

7.2.1. Metadata

Metadata is an attribute that describes the documents content. It is declared in the SIP index, and it can be:

- automatically set by the system;
- manually entered by the user;
- derived from integration procedures with other software via API.

Metadata is a fundamental part of the archived documentation, as the system allows the search of documents only by querying its values in the SIP index.

The following table shows the correspondence between metadata and search keys, and their description. The search functions are described in the chapter Search and request documents .

Table 5. Research metadata.

Search key	Metadata	Obligatory	Description
Dublin Core			
Abstract	`terms:abstract`	No	Summary of document content: for some document types, in the absence of metadata specifications, may contain information about the content that you deem necessary for the search of the document.
Access Rights	`terms:accessRights`	No	Indicates the access rights to the document.
Contributor	`terms:contributor`	No	In the dossiers produced by Public Administration entities, it indicates (in one or more occurrences) the IPA code of the administration participating in the proceeding according to the `IPA:<code>` syntax.
Creator	`terms:creator`	No	In the dossiers produced by Public Administration entities, indicate the IPA code of the administration in charge of the proceeding according to the `IPA:<code>` syntax.
Date	`terms:date`	Yes	Signature date of the document.
Date Accepted	`terms:dateAccepted`	No	In received documents, it is the posting date of the document.
Date Submitted	`terms:dateSubmitted`	No	In sent documents, it is the date the document was sent.
Description	`terms:description`	No	Extended description of the document.
Extent	`terms:extent`	Yes	Document size (e.g. 2345 bytes).. Automatically valued.
Format	`terms:format`	Yes	The *mime type* format of the LUL. For PDF it is always the same as "application/pdf". With "analogico" value, it indicates that the document treated was previously analog, and it was converted to a PDF/A and digital signed when the SIP has been created.
Has part	`terms:hasPart`	No	The URN code of the document unit in addition to the unit documentary of the described document. It can be repeated many times. When it is applied to a dossier, each term indicates one of the documentary units contained in the dossier.
Identifier	`terms:identifier`	Yes	Document ID in the preservation system.

Search key	Metadata	Obligatory	Description
Is Part Of	`terms:isPartOf`	No	URN code of the document unit containing the described file.
Is Referenced By	`terms:isReferencedBy`	No	Document URN.
Medium	`terms:medium`	No	The *mime type* format of the container used for the document, for example `application/pkcs7-mime` for files included in a digitally signed PKCS#7 envelope.
Provenance	`terms:provenance`	No	The Dublin Core `terms:provenance` metadata containing the URN of the unit is applied to the documents for which the previous archiving proof is archived.
Publisher	`terms:publisher`	No	Descriptive metadata which contains the previuos preservation system information.
References	`terms:references`	No	The URN code of the sub-document it refers to.
Replaces	`terms:replaces`	No	It indicates the name of the document to correct in case of modification (metadata `modification:number` with value greater than 1). It contains the 20-character eCON document identifier or the file name in the SIP.
Source	`terms:source`	Yes	URN code of the file described according to the syntax of the provenance SIP. In the Archival Information Packages metadata contains the URN of the Submission Information Packages from which the documents come from, repeated for each involved Submission Information Packages. It is automatically set on archiving.
Subject	`terms:subject`	Yes	Summary string that contains the type, month, year, surname and first name of the document subject. Eg: "Payroll March 2017 ROSSI MARIO".
Title	`terms:title`	Yes	Filename.
Type	`terms:type`	Yes	The type of documents contained in readable terms.
Document			
Document year	`documento:anno`	Yes	The reference year of the document, extracted from the date. Automatically valued.

Search key	Metadata	Obligatory	Description
Document aoo	`documento:aoo`	No	Organizational area. With reference to the producer, it identifies the organizational area to which the document belongs in case of multiple document streams.
Document class	`documento:classe`	No	If present, it is the class code of the document classification.
Document preservation	`documento:conservazione`	Yes	Document preservation time. It is automatically valued by the system according to the document type.
Document date	`documento:data`	Yes	Date of the document.
Document start date	`documento:datainizio`	No	Starting date of the document reference period (only for documents that have a reference period).
Document protocol date	`documento:dataprotocollo`	No	Value used to indicate the protocol date assigned during the reception in the received documents.
Document registration date	`documento:dataregistrazione`	No	Date of entry in the VAT registe.
Document end date	`documento:datatermine`	No	Document end date. See "Document start date".
Class description	`documento:descrizioneclasse`	No	It is the class description document.
Subclass description	`documento:descrizionesottoclasse`	No	It is the subclass description document.
Title description	`documento:descrizionetitolo`	No	It is the title description.
Classification scheme description	`documento:descrizionetitolario`	No	It is the classification scheme description
Document flow	`documento:flusso`	Yes	It indicates the document flow, and it can assume the following values: - U = in exit - E = in entrance - I = Internal. It is automatically valued.

Search key	Metadata	Obligatory	Description
Document format	`documento:formato`	Yes	It indicates the document format as defined by Annex 2 of the "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" ("Guidelines on the creation, management and preservation of IT documents").
Document training	`documento:formazione`	Yes	It indicates the document creation process, and it is valued with one of the following letters: a) creation through the use of software tools that ensure the production of documents in the formats provided for in Annex 2 of the Guidelines; b) acquisition of an IT document electronically or on IT support, acquisition of the copy by image on computer support of an analogical document, acquisition of the IT copy of an analog document; c)storage on computer support in digital format of the information resulting from IT transactions or processes or from the electronic presentation of data through forms made available to the user; d) generation or grouping, even automatically, of a set of data or records, coming from one or more databases, also belonging to several interoperable subjects, in accordance with a predetermined logical structure and memorized in static form.
Document Number	`documento:numero`	No	Progressive number of the document, if any.
Lot position	`documento:posizionelotto`	No	The index of the position of the document described within the archived container file (only if the archived file is a format that can contain multiple documents).
Document dossier number	`documento:pratica`	No	If available, it indicates the dossier number of the document.
Document 'prima nota'	`documento:primanota`	No	In received documents, it indicates the registration protocol assigned in the 'prima nota'.
Document protocol	`documento:protocollo`	No	Value available to indicate the protocol number assigned during reception in the received documents

Search key	Metadata	Obligatory	Description
Document registration	`documento:registrazione`	No	Indicates the number assigned to the submitted document. In the received documents indicate the protocol assigned in the VAT register. In environmental documents, it indicates the number assigned to the Registro Carico e Scarico Rifiuti.
Document sectional	`documento:sezionale`	Yes	Sectional of the document, if not present it acquires the empty value "_default".
Document sub-class	`documento:sottoclasse`	No	If present, it is the sub-class code of the document classification.
Document type	`documento:tipo`	Yes	Document type, selectable from the list of documents provided by the system.
Document classification scheme	`documento:titolario`	No	If present, it is the code of the classification scheme.
Document category	`documento:titolo`	No	If present, it is the category code of the document classification.
Document type registry	`documento:tipoRegistro`	No	If present it can be: - Nessuno (Nothing) - Protocollo Ordinario/Protocollo Emergenza (Ordinary register/Emergency register) - Repertorio/Registro (Repertoire/Register).
Modify			
Modify author	`modifica:autore`	No	It corresponds to the author (or producer) of the correction.
Modify date	`modifica:data`	No	It corresponds to the date and time of the modified document.
Modify number	`modifica:numero`	No	It is the version number of the document.
Modify type	`modifica:tipo`	No	Indicates the type of modification made to the document and can assume the following values: - Annullamento (Annulment) - Rettifica (Correction) - Integrazione (Integration) - Annotazione (Annotation).
Verify			
Certified digital copy of physical documents	`verifica:conforme`	Yes	It indicates whether the document is a certified replacement, value "vero" (true) or "falso" (false).

Search key	Metadata	Obligatory	Description
Digital signature	`verifica:firma`	Sì	It indicates whether the document is digitally signed, value "vero" (true) or "falso" (false).
Digital timestamp	`verifica:marca`	Sì	It indicates whether the document is digitally marked, value "vero" (true) or "falso" (false).
Electronic seal	`verifica:sigillo`	Sì	It indicates whether the document è digitally sealed, value "vero" (true) or "falso" (false).
Intermediary			
Intermediary Tax Code	`intermediario:codicefiscale`	No	Intermediary Tax Code (mandatory if the tax ID is not indicated).
Intermediary surname	`intermediario:cognome`	No	Intermediary surname (in case of a natural person).
Intermediary tax ID	`intermediario:idfiscale`	No	Tax identifier composed of the country code and the VAT number of the third party intermediary (mandatory if the tax code is not indicated).
Intermediary name	`intermediario:nome`	No	Intermediary name (in case of a natural person).
Intermediary Company name	`intermediario:ragionesociale`	No	Intermediary Company name (in case of a legal person).
Intermediary type	`intermediario:tipo`	No	Intermediary type, it can have the following values: - PF for Natural Person - PG for Legal Person - PAI for Italian Public Administrations - PAE for Foreign Public Administrations.
Intermediary code	`intermediario:codice`	No	Code assigned to the intermediary
Sender			
Sender tax code	`mittente:codicefiscale`	Yes	Sender Tax Code (mandatory if the tax ID is not indicated).
Sender surname	`mittente:cognome`	Yes	Sender surname (mandatory in case of natural person).
Sender tax ID	`mittente:idfiscale`	Yes	Tax identifier composed of the country code and the VAT number of the sender (mandatory if the tax code is not indicated).
Sender name	`mittente:nome`	Yes	Sender name (mandatory in case of natural person).
Sender PEC	`mittente:pec`	No	Sender PEC.

Search key	Metadata	Obligatory	Description
Sender Company name	`mittente:ragionesociale`	Yes	Sender Company name (mandatory in case of a legal person)
Sender type	`mittente:tipo`	Yes	Sender type, it can have the following values: - PF for Natural Person - PG for Legal Person - PAI for Italian Public Administrations - PAE for Foreign Public Administrations.
Sender code	`mittente:codice`	No	Code assigned to the sender
Producer			
Producer tax code	`produttore:codicefiscale`	Yes	Producer Tax Code (mandatory if the tax ID is not indicated).
Producer surname	`produttore:cognome`	Yes	Producer surname (mandatory in case of natural person).
Producer tax ID	`produttore:idfiscale`	Yes	Tax identifier composed of the country code and the VAT number of the producer (mandatory if the tax code is not indicated).
Producer name	`produttore:nome`	Yes	Producer name (mandatory in case of natural person).
Producer Company name	`produttore:ragionesociale`	Yes	Producer Company name (in case of a legal person).
Producer Type	`produttore:tipo`	Yes	Producer type, it can have the following values: - PF for Natural Person - PG for Legal Person - PAI for Italian Public Administrations - PAE for Foreign Public Administrations.
Producer code	`produttore:codice`	No	Code assigned to the producer
Recipient			
Recipient tax code	`destinatario:codicefiscale`	Yes	Recipient Tax Code (mandatory if the tax ID is not indicated).
Recipient surname	`destinatario:cognome`	Yes	Recipient surname (mandatory in case of natural person).
Recipient tax ID	`destinatario:idfiscale`	Yes	Tax identifier composed of the country code and the VAT number of the recipient (mandatory if the tax code is not indicated).
Recipient name	`destinatario:nome`	Yes	Recipient name (mandatory in case of natural person).

Search key	Metadata	Obligatory	Description
Recipient PEC	`destinatario:pec`	Yes	Recipient PEC.
Recipient Company name	`destinatario:ragionesociale`	Yes	Producer Company name (in case of a legal person).
Recipient type	`destinatario:tipo`	Yes	Recipient type, it can have the following values: - PF for Natural Person - PG for Legal Person - PAI for Italian Public Administrations - PAE for Foreign Public Administrations.
Recipient code	`destinatario:codice`	No	Code assigned to the recipient
Fixity			
XML canonical form	`fixity:canonicalXML`	No	It is valid only for files in XML format. It is "true" if the file has been reduced to a canonical form before calculating the digest.
Base64 digest	`fixity:messageDigest`	Yes	The Base64 representation of the file digest calculated according to a given algorithm.
Digest algorithm	`fixity:messageDigestAlgorithm`	Yes	The algorithm by which the file digest was calculated.
Digest originator	`fixity:messageDigestOriginator`	Yes	The application that calculated the file digest (this is "edoc" if the digest is calculated from preservation system).
Folder			
Identifier	`fascicolo:identificativo`	Yes	Complete unique folder number.
Progressive	`fascicolo:progressivo`	Yes	Unique progressive numeric part of the folder number.
Type	`fascicolo:tipologia`	Yes	Folder type. It can take the following values: - Affair; - Activity; - Natural person; - Legal entity; - Administrative Procedure.
Subject	`fascicolo:oggetto`	Yes	Folder's description
Subject company name	`fascicolo:ragionesocialesoggetto`	No	Subject company name related to the folder (in case of legal entity).
Subject name	`fascicolo:nomesoggetto`	No	Subject's name related to the folder (in case of natural person).

Search key	Metadata	Obligatory	Description
Subject surname	`fascicolo:cognomesoggetto`	No	Subject's surname related to the folder (in case of natural person).
Subject tax ID	`fascicolo:idfiscalesoggetto`	No	Tax identifier composed of the country code and the VAT number of the subject.
Subject tax code	`fascicolo:codicefiscalesoggetto`	No	Subject's tax code.
Subject type	`fascicolo:tiposoggetto`	No	Subject type, it can take the following values: - PF for Natural Person; - PG for Legal Person; - PAI for Italian Public Administrations; - PAE for Foreign Public Administrations.
Folder start date	`fascicolo:dataapertura`	Yes	Folder starting date.
Folder end date	`fascicolo:datachiusura`	No	If present, it represents the folder ending date.

For other SIPs examples please refer to our website: https://www.entaksi.eu/en/entaksi-solution-spa-english/.

7.3. SIP List

By accessing the list of **Submission Information Package (SIP)** present in the system, it is possible to monitor the status of the SIPs.

The SIP consists of a .zip file containing the documents belonging to one or more documentary units to upload into the preservation system, and an index file in XML format.

SIPs can be uploaded from three different sources:

- automatic loading by external procedures;
- manual loading by the user;
- other service modules.

The Preservation System defines a series of different SIP formats which determine the validation method for the package. These formats can be of general use or agreed with the individual producer to contain specific requirements related to the desired metadata set.

The Preservation System receives the documents sent by the producer through a REST services, and the connection and the authentication are guaranteed by a HTTPS protocol.

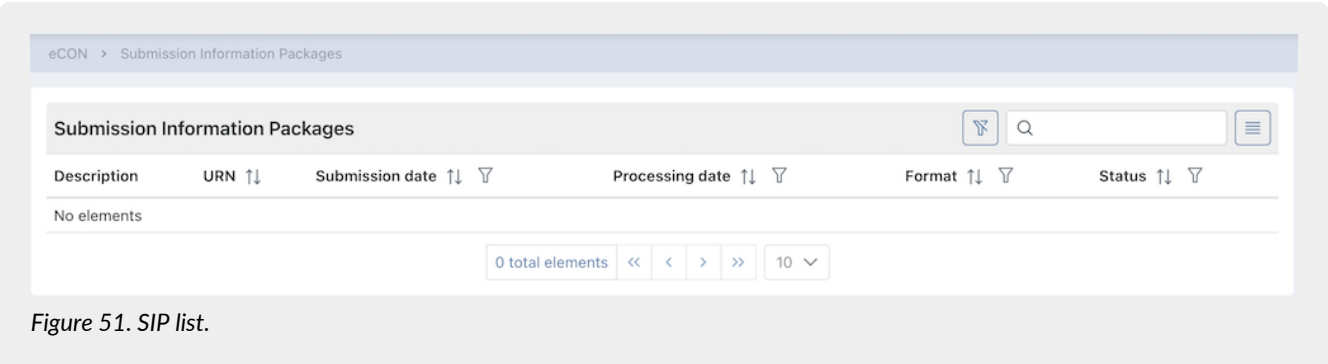

Figure 51. SIP list.

The list shows the following information:

- **Description**: a item that contains the description as reported in the "Subject" field for generic and analogue packages if

valued (otherwise it will report only "Generic package"), or a description associated with the document type;
- **URN**: the unique identification of the payment package;
- **Upload date**: the date / time when the SIP was loaded;
- **Processing date**: the date / time when the SIP was processed;
- **Format**: the format in which the SIP was received.;
- **Status**: the status in which the package is located at a given moment. It can take the following values:
  - "Initial status";
  - "Under construction";
  - "Processing";
  - "Processed";
  - "Signing in progress";
  - "Archived";
  - "Accepted";
  - "Rejected";
  - "SIP verification".

The states of interest to the user are shown in the following table. The other states listed previously are mostly service states, through which the SIP transits for only a few seconds.

State	Description
BUILDING	The package remains in this state from the submission until the end of the month, when the associated management cycle is closed and the package is archived. Once it has been closed and submitted, the Confirmation of receipt is issued.
REFUSED	the SIP validation is not successful, the package has problems and it must be reloaded. All the rejected SIPs are periodically deleted from the system with an automatic procedure.
ELABORATO	the validation has been successful, the SIP has no problems and it is ready for the preservation of the documents it contains.
ACCEPTED	the SIP contents are put into preservation.

From this section it is possible:

- to sort columns and filter the elements present in the table as described in the chapter Console tables;
- to access the detail page of the submission package where its information is shown.

The SIP detail page is divided into two sections.

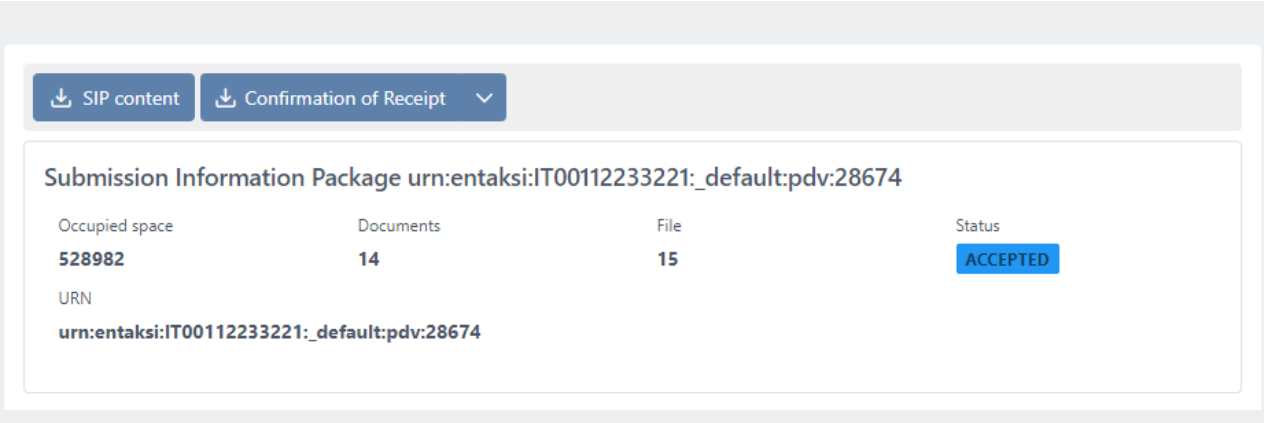

Figure 52. SIP details.

In the top section, in addition to the title of the package (such as the progressive number assigned by the system) the following information is present: the space occupied by the package, the documents and the number of files that make up the package, the status of the package and its URN.
By clicking on the "**SIP content**" button user can download the SIP ZIP file of the selected package.

By clicking the "**Deposit receipt**" button user can download the SIP deposit receipt: clicking on the arrow to the right open a menu from which user can choose the file type (.xml or .pdf) that wants to download by simply clicking on it.
In the section below "**Confirmation of receipt**", the data relating to the receipt is present.
For packages containing more than 10000 documents, the confirmation of receipt is displayed in a condensed format; the full version is available exclusively by downloading the relevant document.

The **Confirmation of receipt** (Rapporto di versamento, RDV, in italian) is an XML file that contains the SIP index it refers to, along with information processed during validation and details ensuring the immutability of the archival units contained, this includes the hash of each file in the SIP (see Acceptance of submission packages and generation of the confirmation of receipt).
The Confirmation of Receipt is digitally signed by the Preservation Service Manager with an XAdES BT level signature, which consists of a digital signature with an embedded timestamp, in compliance with the ETSI EN 319 132-1 standard - "Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures". This signature provides additional assurance that the submission process is completed within the legal deadlines.
The cryptographic certificates used in the signing process and for applying timestamps are issued internally by Entaksi Solutions SpA - Irish Branch, registered on the EU Trust List.
Entaksi may also use backup Certification Authority that are part of the European Union Trusted List (EUTL) under eIDAS.

7.4. AIP List

In the "AIP List" section it is possible to view the list of SIPs brought into preservation as AIPs (Archival Information Package) after SIPs have been closed. In order to form an AIP and to make effective the preservation status, it is necessary to apply a signature and a time-stamp.

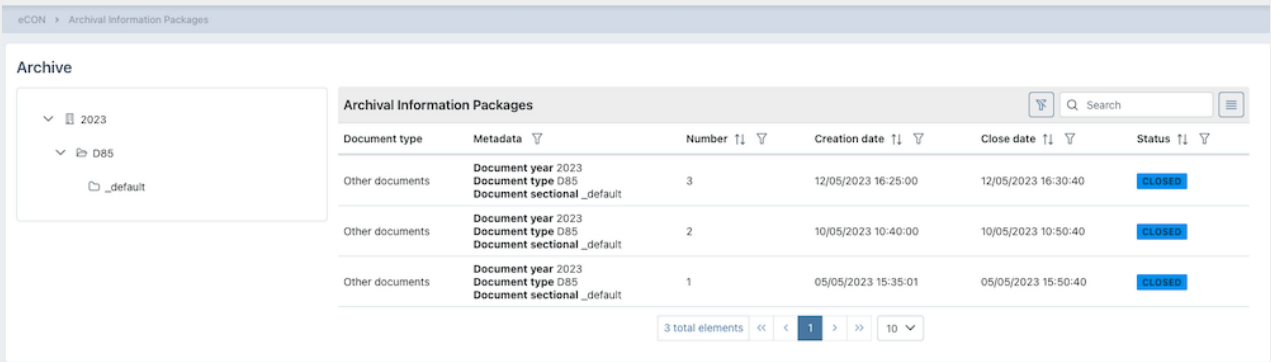

Figure 53. AIP list

The structure of the metadata for the archive log used by the company is shown on the left side.
By clicking on nodes, the list on the right will be automatically filtered by the selected node. This node appears highlighted.
To remove the selection from the node, it is necessary to click twice (double click) on the node. The node will no longer be highlighted and the list on the right will no longer be filtered.

The list shows the following information:

- **Document**: the extended description of the document type;
- **Metadata**: it's the metadata with which the company has organized its document preservation;
- **Number**;
- **Status**: the status in which the package is located at a given moment. It can take the following values:
  - "To be processed";
  - "Processed";
  - "To sign";
  - "Signing in progress";

- "Signed";
- "Closed".

The states of interest to the user are shown in the following table. The other states listed previously are mostly service states, through which the AIP transits for only a few seconds.

State	Description
ELABORATO	the index has been created, the AIP has no problems and is ready for storing the documents it contains.
CLOSED	the AIP is in preservation.

From this section it is possible:

- to sort columns and filter the elements present in the table as described in the chapter Console tables;
- to access the detail page of the archival package where the AIP information is shown.

Refused packages are periodically deleted from the system through an automated procedure.

The Archival Information Package (AIP) is a logical entity that contains the documentary units from one or more SIPs and an index file that is digitally signed and timestamped by the Preservation Service Manager using the *XAdES B-LTA* signature defined by the standard ETSI EN 319 132-1 - "Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures". This signature, which consists of a digital signature with an embedded timestamp and the inclusion of all materials necessary for verifying long-term validity, also meets the requirements for Long-Term Preservation according to the ETSI TS 119 511 standard - "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" (see Preparation and management of archival information packages).

This index file is the proof of the preservation of the archival units contained.

The AIP index is an XML format file which describes, for each of the documentary units contained, information including the unique identifier assigned according to the URN code, and, for each file, a digital fingerprint (hash) and the algorithm with which this fingerprint was calculated.

The Archival Information index allows you to check the integrity of each individual file, regardless of all the other files stored in the same block. In fact, it will be sufficient to be in possession of the file to be able to execute the hash algorithm on its content and to compare the recalculated fingerprint with the string shown in the index.

The solution adopted by Entaksi uses the UNI 11386:2020 standard - Support for Interoperability in the Preservation and Recovery of digital Objects (original: Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali), also called SinCRO, for the format of the AIP index.

Within the DIAM/SC11 (Management of archival documents) subcommittee of the Italian National Unification Body (Ente Nazionale Italiano di Unificazione, UNI), a special working group called SInCRO defined the structure of the data set to support the preservation process, by identifying the necessary elements for the creation of a Preservation Index ("closing file").

The implementation of this index, of which SInCRO has described both the semantics and the articulation, allows you to use a shared data structure and achieve a satisfactory degree of interoperability in the migration processes from a preservation system to another, through the adoption of a specially developed XML Schema.

The AIP index scheme defined in the UNI 11386 standard includes four "extension" points, where the preservation manager can insert additional information according to a customized scheme. Entaksi uses these additional information:

- **Additional information on the package description** (`SelfDescription/MoreInfo`). This section contains the references to the SIP from which the AIP data come.
- **Additional information on the contents of the package** (`VdC / MoreInfo`). This section lists the metadata in the archival package.
- **Additional information on the individual archival units** (`FileGroup / MoreInfo`). This section contains the metadata of the archival unit(s).
- **Additional information on individual files** (`File / MoreInfo`). This section shows the metadata of the individual archive unit file.

In the "AIP List" section by selecting an AIP from the list, it is possible to view the detail where are shown both general information about the package itself, such as the structure of the archival register, creation and processing dates, number, and status, either the list of documentary units contained in it, divided by number, title and description.

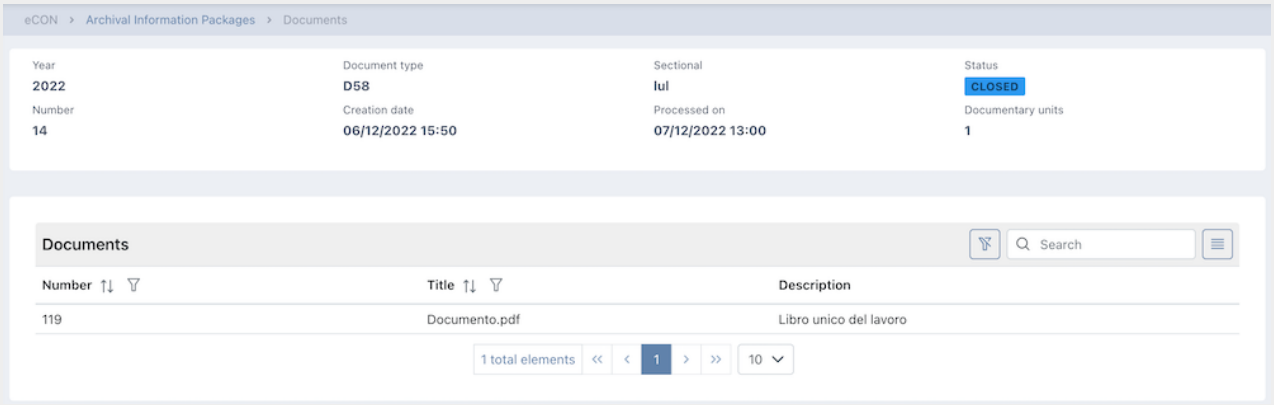

Figure 54. AIP detail

If it is necessary to deepen the content, by clicking on each documentary unit, it is possible to view the search keys indexed by the system (metadata) and how they have been set.

7.5. Search and request documents

Through "**Search and request documents**", using the predefined searching metadata and setting the value to be assigned to the key it is possible to set up the general search within all the preserved documents for the company and to request DIPs.

The search title automatically suggested by the system is the value `"Ricerca del <data creazione>"`, however, it can be modified by entering the desired text in the 'Search Title' field.

To perform a search, it is necessary to set predicates, a search criterion, and a value.
Research keys are made up of metadata in documents. All search items correspond to the metadata as listed in the chapter Metadata.

To combine several search terms (for example: "equal" in the case of text searches, "greater" and "lesser" if looking for a range, such as for dates).
The value, on the other hand, can be entered manually or selected from a list provided by the system (in case the selected metadata includes predefined values).

The system allows users to create even complex searches by entering multiple criteria and combining them with each other.

If user want to perform a search using a single key (i.e., a single metadata field) but with multiple values at the same time, simply select the metadata of interest and the criterion, then click the button located + on the same row: an additional row will be displayed to allow the entry of another value.

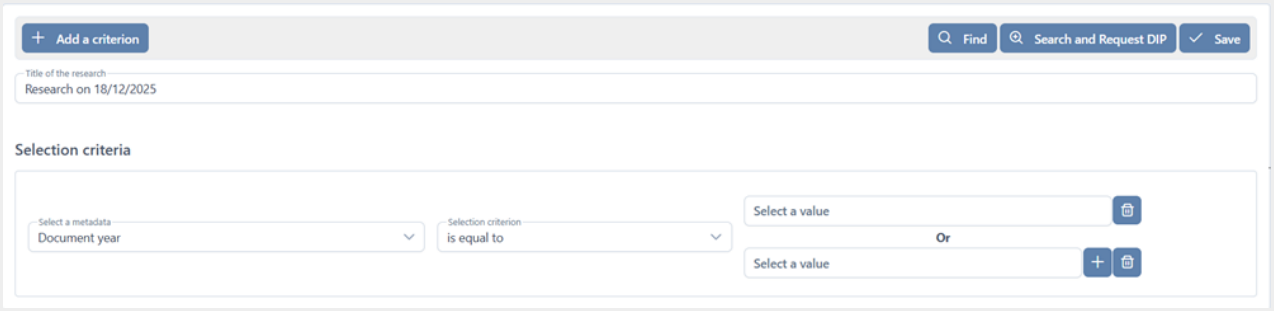

Figure 55. Ricerca valori multipli.

By entering multiple values, the system will search for all documents where the selected metadata field contains any of the entered values.

To combine multiple search keys, click the "**Add a Criterion**" button: a second row will appear where user can enter additional criteria.

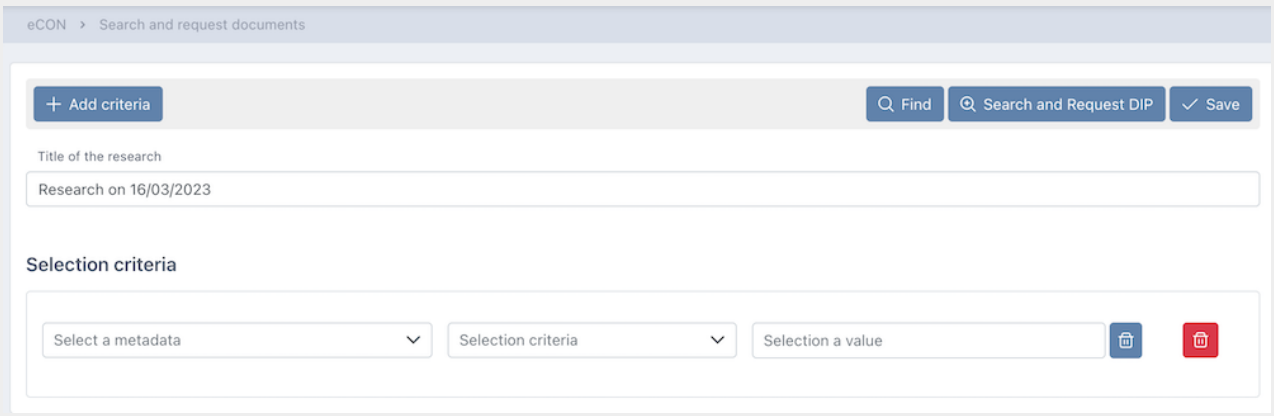

Figure 56. Search and request documents.

In this case, the system will search for all documents that **simultaneously** contain all the required information for each individual search key (metadata).

To delete a value entered in a row because it is incorrect, click the corresponding button .

To delete the entire added search section, click the corresponding button. .

The "**Save**" button allows to save the search terms without executing the search;
the "**Search**" button executes the search, which will be saved in the system and displayed on the "*Searches and document collections*" page;
the "**Search and Request PDD**" button executes the search and automatically requests a Dissemination Information Package (DIP) containing the requested documents.

7.5.1. Search and request documents using a list of values separated by the character

As explained in Search and request documents paragraph, in order to search multiple values, you have to manually add new criterion lines and manually enter each individual value.
If you want to perform a filter for a large number of values, this operation could be very long and hardworking.

For this reason, Entaksi has developed a simultaneous multiple selection function by inserting a list of values separated by the character #.

This selection methodology can be used for any search criteria.

Suppose, for example, that you want to perform a multiple search for recipients
MARCO VERDI;MARIO BIANCHI;MARIO ROSSI.

Then, you have to select "Recipient name" as metadata, set the search criterion "is equal to" and enter the list structured as follows inside the value box:

```
MARCO VERDI#MARIO BIANCHI#MARIO ROSSI
```

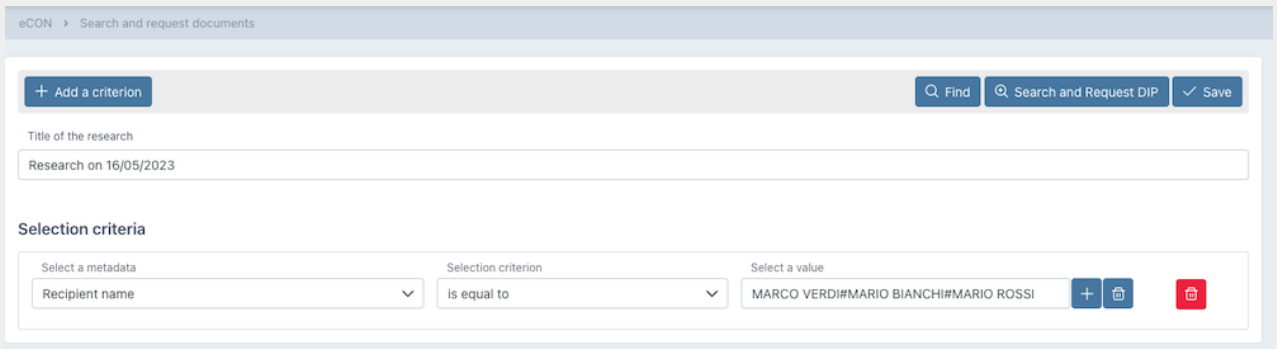

Figure 57. Name entry via value list.

By pressing the "Enter" key on the keyboard, the names are automatically included in the search with the "or" option:

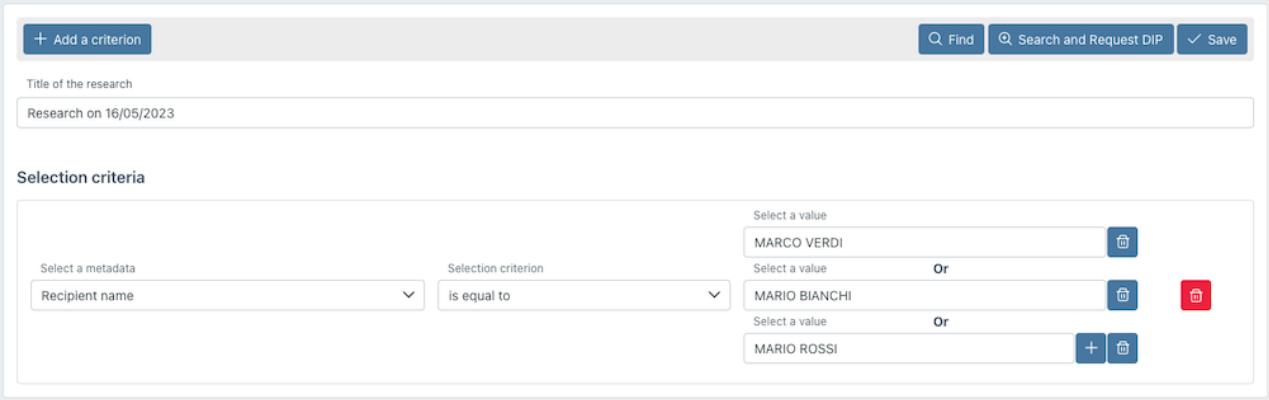

Figure 58. Multiple values search.

The table below lists the various types of criteria of a list of values with separator.

Type of criterion	**Example list of values**
String type	`MARCO VERDI#MARIO BIANCHI#MARIO ROSSI`
Numeric type	`2022#2023`
Date type	`06-12-2022#07-12-2022`
Date time type	`06-12-2022 14:16#07-12-2022 14:16`
List type	`D01#D02#D03`

If you want to replicate a criterion of a previously performed search, you can copy the list of values.
In this case you have to enter the DIP detail page (see DIP list) or a previously performed search detail page (see Search and document collections), to click on "copy criteria" button  next to the criterion you want to reproduce, and to paste the copied string into the corresponding criterion of the new search.

7.5.2. Interoperability DIPs

Interoperability DIPs are those containing all the AIPs within the preservation system, aimed to transferring the data to another preservation system.

They are available only if the service has been ceased by the company, for six months from the ceasing date.
Interoperability DIPs can be obtained with the following procedure:

1 . In the "Search and request documents" function Search and request documents (available on our application: https://entaksi.eu/console), **leave all the data selection fields blank** and click on the "Search and Request DIP" button. In this way, the research will return all AIP preserved for the reference company, and so the interoperability DIP(s) will correctly form.

NOTE: Data selection process is an activity that may take some time to complete, it depends on the system data traffic and on the size of the DIP(s) to be created.

2 . The user can monitor the progress of the search on the "*Searches and document collections*" page by checking its status, visible in the last column of the page.

3 . The search process is complete when its status shows **PDD ready**. By clicking on the search, the detail page will be displayed, listing all the requested documents and allowing the PDD to be downloaded.

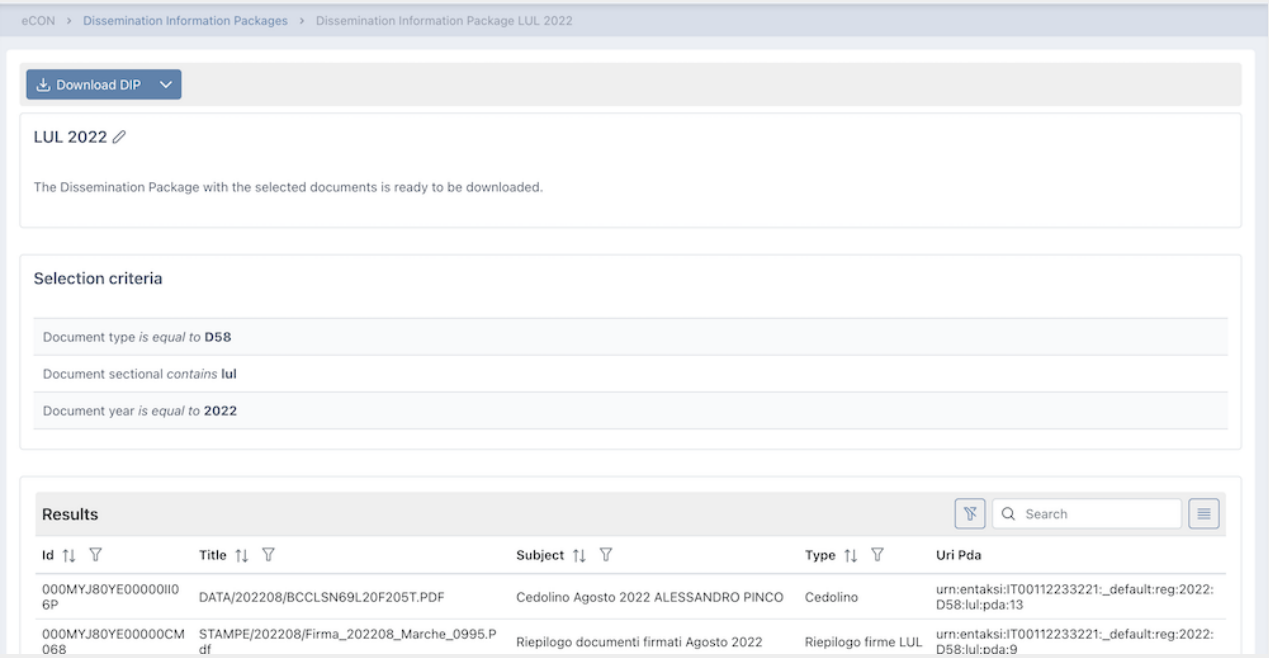

Figure 59. Interoperability DIPs creation.

4 . The search result thus carried out includes the list of all the AIPs in the preservation system. Now you can click on "Download DIP" button to get all the company documents to send to another preservation system. There may be one or more DIPs: it depends on the number of documents (each DIP includes about 900 signed documents and indexes).

As creating, also downloading DIP(s) is a process that may take some time to complete.

Created DIPs are ready to be submitted to the new preservation system, following the indications defined by the new preservation manager.

NOTE: Please consider that there may be some SIPs still to be "closed" and to be prcessed into AIPs in the preservation system.
The closing process takes place on a defined basis, approximately monthly: it is recommended to carry out the interoperability procedure described above after having checked in the SIP List section in the Console that all the AIP have been correctly created.

NOTE: If the company contract with Entaksi is not ceased, the procedure will give an error message, as at least one term must be entered in the search menu for an active company.

7.6. Search and document collections

In the "Search and document collections" section, a list of all the saved searches is shown.

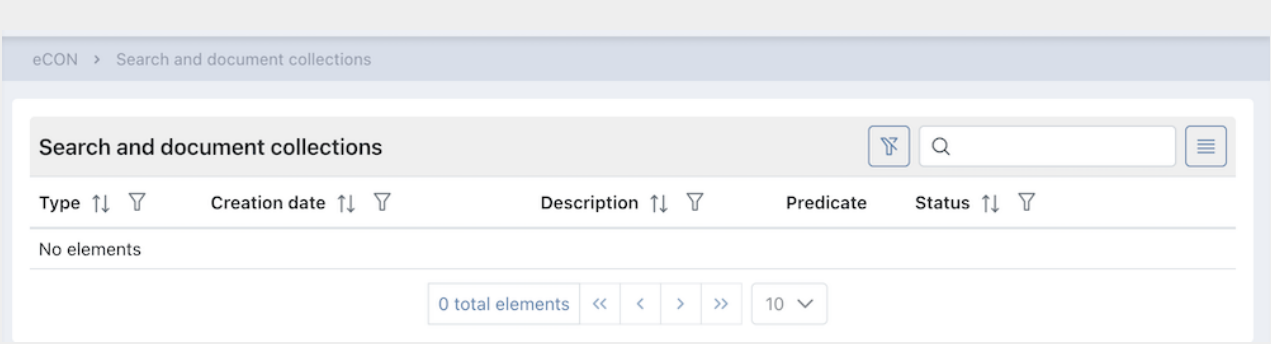

Figure 60. Search and document collections

The items listed are:

- **Type**: type of extraction. It can assume the values of "Search" or "Collection";
- **Creation date**: it is the date the search was started;
- **Description**: it is the title of the search;
- **Predicates**: they are the criteria entered during the search creation phase (Search and request documents)
- **Status**: it is the state the search. It can have the following values:
  - "Draft";
  - "Saved";
  - "Search in progress";
  - "Results available";
  - "DIP requested";
  - "DIP under construction";
  - "Enable";
  - "DIP ready";
  - "DIP to delete";
  - "DIP deleted";

Among these, the statuses the more interesting are:

State	Description
DRAFT	it means that the search made in Search and request documents has simply been saved.
SEARCH IN PROGRESS	your requested search is being processed.
NO RESULT	the search has been completed and returned no results; no documents matching the specified criteria were found.
RESULTS AVAILABLE	the search has been completed. To view the results, simply click on a row to open the detail page.
DIP READY	the requested DIP is available for download.

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 the case of a "Search" type with a "Draft" status, entering the detail page you can modify and / or complete the search requiring a DIP.

In the case of "Search" type with "Results available" status, entering the detail page you can see the results of the research.

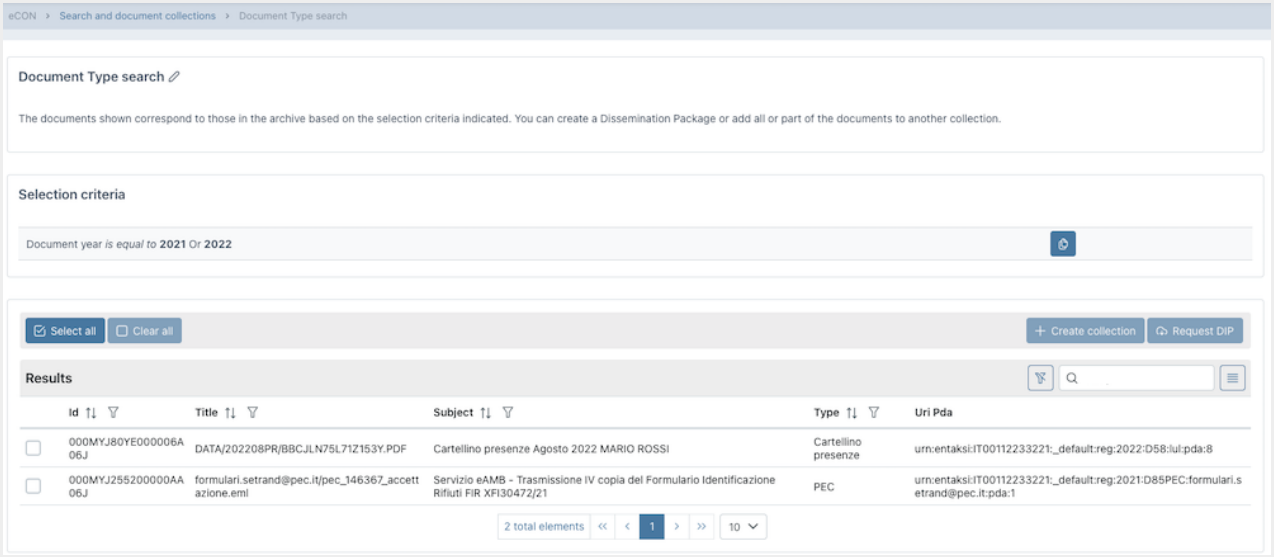

Figure 61. Detail search and document collections.

In the first section, the search title is shown and you can change it by clicking on next to the title.

In the central section, the selection criteria previously carried out are listed. By clicking on next to the criterion, you can copy its list of values.
You can create a new search by copying the list as explained in Search and request documents using a list of values separated by the character .pdf

The documents that meet the extraction criteria are listed in the bottom section.

You can select the elements individually in the list or all by clicking the buttons on the left. By clicking on "**Select all**" all listed items are selected, by clicking "**Clear all**" all listed items are deselected.

The right buttons are enabled only if some item is selected. By clicking them, you can:

- to request a DIP by clicking on "**Request DIP**": the request will be present in the list of "Search and document collections" page;
- to create a collection by clicking on "**Create collection**". In this case, a new form opens from and you can decide to create a new collection by entering its description or merge the selected items into an existing one by selecting it from the list of existing collections. By clicking on "**Save**", the chosen option is executed.

Exactly as in the case of a Search in "Results available" status, entering into the detail page of a collection in "Active" status, by selecting all or part of the items, you can request a DIP, create a new collection or add them to an existing one.

If the search is in "DIP ready" status, you can enter in the DIP detail page.

7.7. DIP list

The section dedicated to **Dissemination Information Packages (DIP)** allows to view all the DIPs requested through the search functions previously described.

You can search and extract documents stored in the system, for the purpose of consulting them or distributing them through this specific information package.

Based on the selection criteria of the documents, the preservation system provides a Dissemination Package in .zip format, that includes:

- a DIP index called "*PIndex.xml*", digitally signed by the Preservation Service Manager with an *XAdES B-T* level signature, which consists of a digital signature with an embedded timestamp, in compliance with the ETSI EN 319 132-1 standard - "Electronic Signatures and Infrastructures (ESI) - XAdES digital signatures - Part 1: Building blocks and XAdES baseline

signatures.
The cryptographic certificates used in the signing process and for applying timestamps are issued internally by Entaksi Solutions SpA - Irish Branch, registered on the EU Trust List. Entaksi may also use backup Certification Authority that are part of the European Union Trusted List (EUTL) under eIDAS.
The index also serves as the dissemination report, containing the index of all requested archival packages.

- the documentary units within the archive, corresponding to the selection criteria organized according to their respective AIPs, which may correspond to one or more folders within the ZIP file, named according to the AIP's urn (e.g., urn_entaksi_IT01234567890__default_reg_2022_D85_man_pda_9);
- any signature validation reports;
- the set of preservation proofs for the selected documentary units (the signed indices of the provenance AIPs).

DIPs can contain parts, one or more AIP. Their download is available for one year, then an automatic deletion will be operated.

The DIP's index uses the same SinCRO format used by the AIP's index, including the MoreInfo tags definitions defined for that format.

DIPs are tracked by the System, as they constitute an authentic and signed copy of the documents contained in the AIPs. Their download is available to the user for six months before automatic disposal.

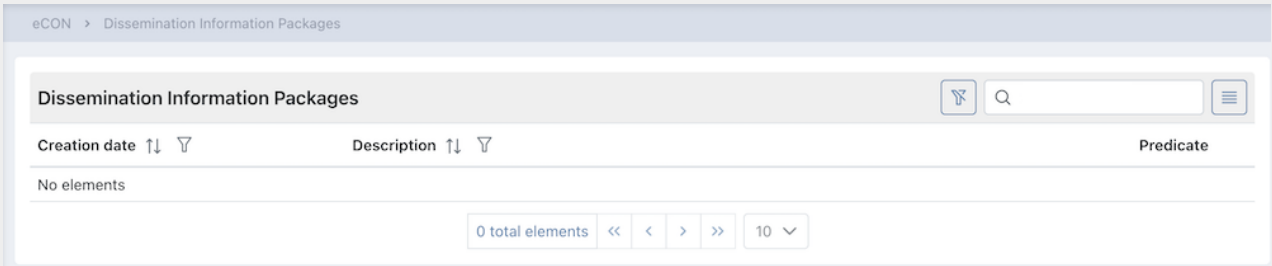

Figure 62. DIP List

The DIPs are displayed in a list where you can see the creation date, the description of the package and the values entered during the search.

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.

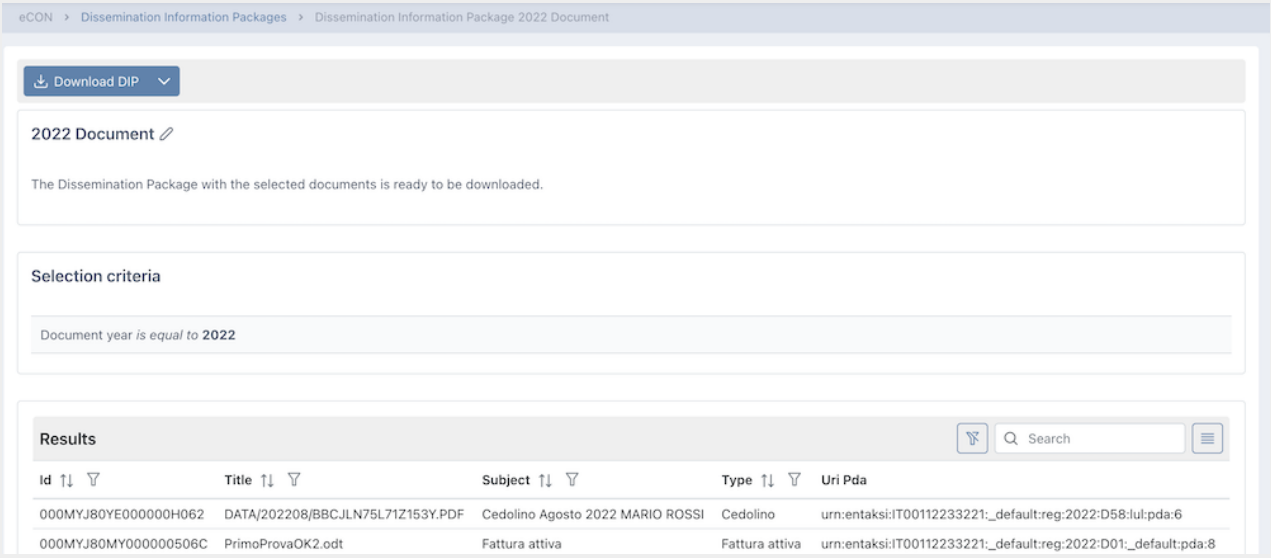

Figure 63. DIP detail.

In the lower part of the page, all the DIP documents are shown in a list.

In the top section, in addition to showing the general information of the package such as the year, document type, sectional, number and the creation date, you can download the DIP .zip file by clicking on "**Download DIP**".

Each DIP contains a maximum number of documents (about 900). For this reason, a search can produce one or more .zip files. In this case, assuming a number equal to n of created PDD files, by clicking on "**Download DIP**" all the n files produced are downloaded at the same time.

In order to download only one file, open the pull-down menu of the button and click on the desired file.

The selection criteria are displayed in the central section.
By clicking on the icon  next to each selection criterion, the list of values with the criterion separator will be copied, a new search can then be created by inserting the copied list as shown in Search and request documents

Back to the top.

8. eDOC - Entaksi document management system

The "eDOC" button on the Console menu bar allows the user to access the eDOC Document Management System. This section consent to consult the documents uploaded through the ePRI service on this specific customized Enterprise Content Management system.

The section allows the user to view the organization of the document archive and to search for specific documents in the structure, through an advanced metadata search system.

The documents included in the preservation system are automatically published on this management system based on Alfresco Community Edition, which allows the user to view and download work copies of the legally preserved documents.

Through this DMS it is possible to look up the documents for internal office management purpose only Please consider that to obtain documents with legal value, in according to what established by the D.P.C.M. 03/12/2013, it is necessary to follow the procedure described in the chapter Search and request documents. **Only DIPs, signed and time-stamp marked, match with the legal definition of normative valid documents**.

DIPs contain one or more AIP, and meet the preservation requirements for digital documents in case it is necessary to show them to a supervisory authority or to third-parties.

Therefore, through the same **Entaksi Console** access point it is possible to check both the status of the preservation system and access the management system in which the documents are published.

The same credentials used to access the Console work on the DMS.

The DMS shows a control panel containing the list of libraries (data areas) to which the user has access.
Each library corresponds to a company and will contain only the documents published for that company.

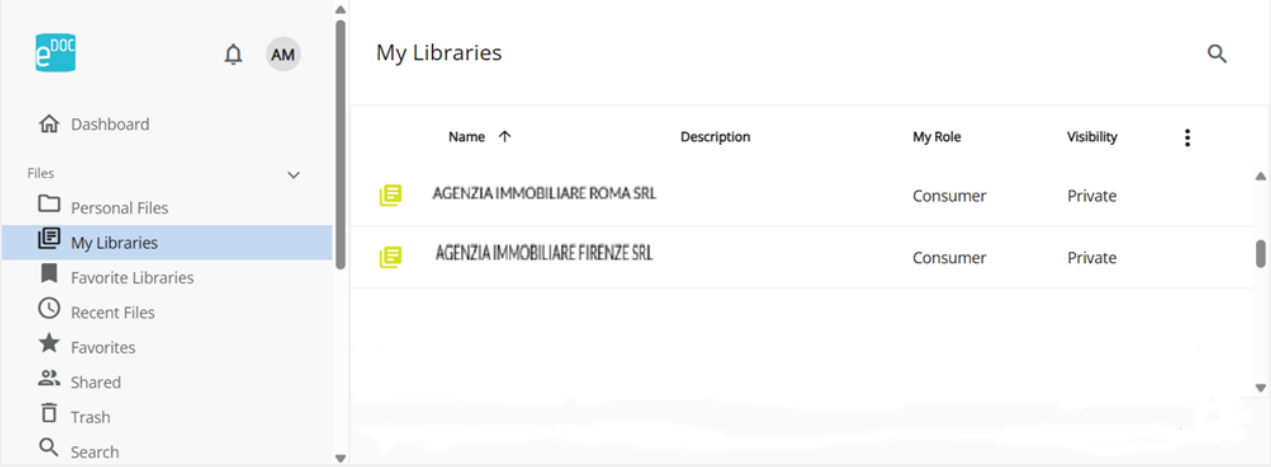

Figure 64. Libraries.

By clicking on the desired library, user access to the company's documents, which are organized into folders with the same structure configured for the Archiving Information Package register.

In the case of the ePRI service, since the archiving register is configured based on an applied classification scheme, the structure wil be as follows, for example:

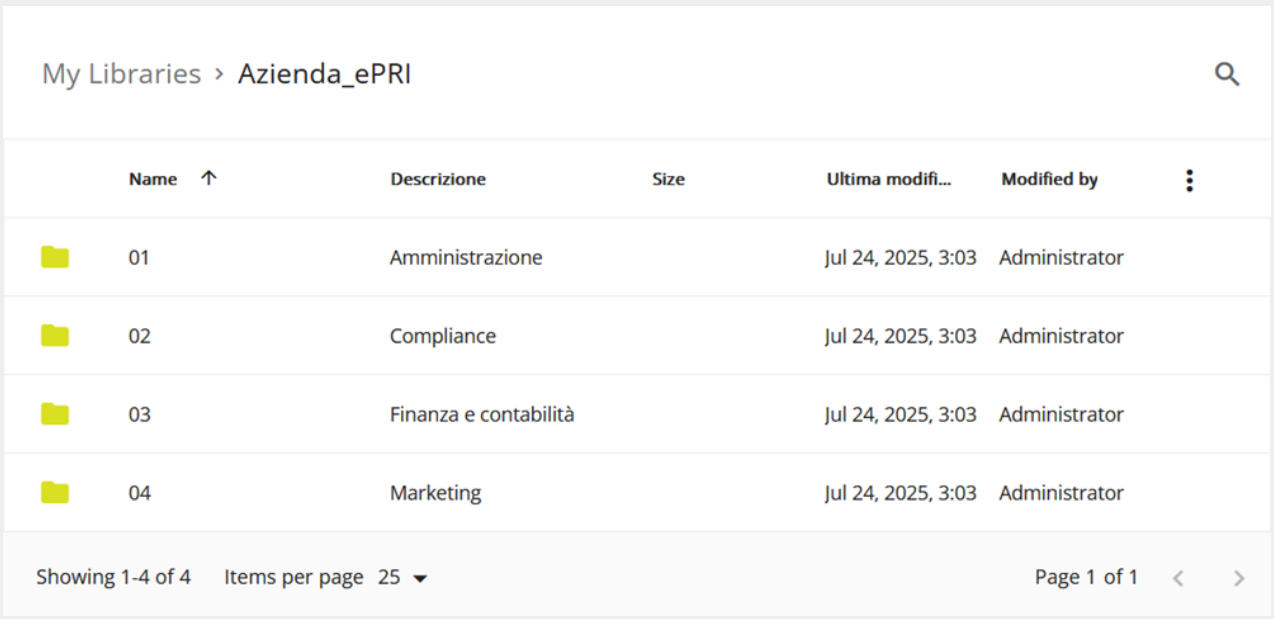

Figure 65. Structure.

By right-clicking on each folder, user can download it: a *.zip* file containing all the data in the folder will be downloaded, maintaining the same structure.
The folders are navigable by clicking on them: at the top of the page, a quick navigation menu is displayed, allowing user to return to previous pages.

Inside the folders, the categorization is available according to the required structure, and user can view and consult the documents. When opening a single document, in addition to viewing its content in the center, user can:

- click the button to enter full screen mode;
- click the button to share the file;
- click the button to download the file;
- click the button to print the document;
- click the button to view the document details.

Figure 66. Document details.

By clicking the "More Information" button, all metadata related to the document will be displayed in the left side menu.

By clicking the button ✕ in the top-left corner, the open document will be closed and the previous page will be reloaded.

8.1. Research

Documents can be located in the document management system using the search function, accessible by clicking on the "Search" option in the left side menu on the home page.
The search page is divided into two sections: on the right side, a complete list of documents stored in the libraries is displayed; on the left side, user can set filter criteria to accurately select and download the desired files.

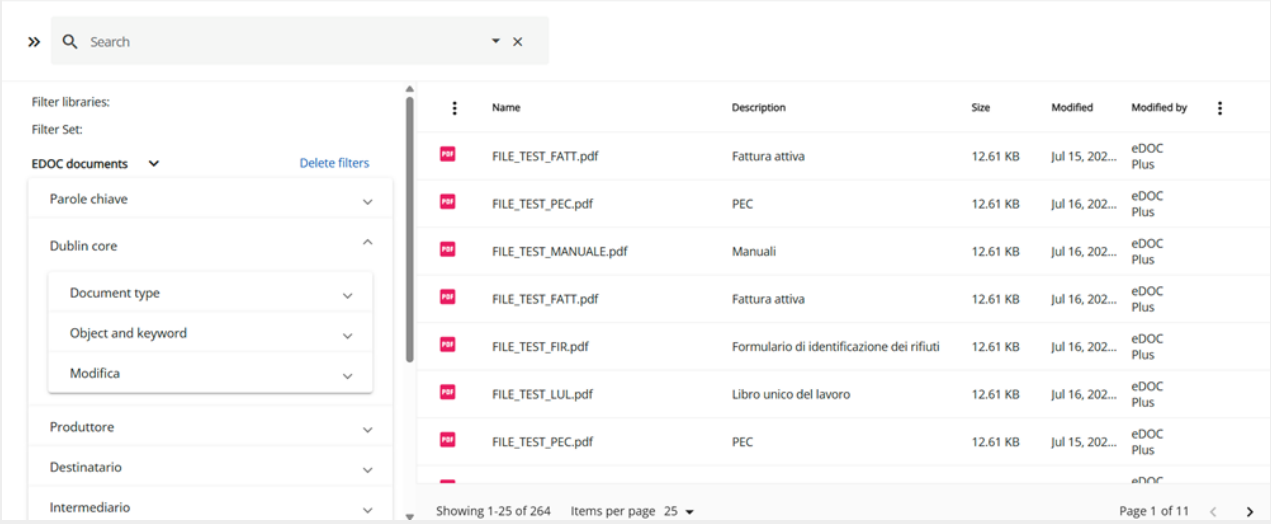

Figure 67. Search page.

Search is available by default across all enabled libraries. If user is authorized for multiple companies and wishes to search in a specific one, select the relevant library from the list: the search data and files will automatically be filtered based on the selected library.

User can also perform a search using "keywords" or by querying predefined fields of individual metadata: to view the list of available fields, click the ⌄ button to expand the dropdown menus and select one or more metadata fields of interest.

The available fields are organized into different sections based on their corresponding metadata:

- **Dublin Core section**
  - Document type.
  - Object and Keyword.
  - Modification date, with values from - to.
- **Produttore (Producer) section**
  - Tax identifier.
  - Tax identifier code.
  - Name.
  - Surname.
  - Company name.
- **Destinatario (Recipient) section**
  - Tax identifier.
  - Tax identifier code.
  - Name.
  - Surname.
  - Company name.
  - REM
- **Intermediario (Intermediary) section**
  - Tax identifier.

    - Tax identifier code.
    - Name.
    - Surname.
    - Company name.
- **Mittente (Sender) section**
    - Tax identifier.
    - Tax identifier code.
    - Name.
    - Surname.
    - Company name.
- **Document section**
    - Year.
    - Document typology.
    - Sectional.
    - Date, with values from - to.
    - Start date, with values from - to.
    - End date, with values from - to.
    - Registration date, with values from - to.
    - Registration.
    - Protocol date, with values from - to.
    - Protocol.
    - Lot location.
    - Classification scheme.
    - Category.
    - Class.
    - Sub-class.
- **Fattura (Invoice) section**
    - Receipt code.
    - Recipient description.
    - Expiration date.
    - Amount.
    - CIG Code.
    - CUP Code.
    - Signer.
    - SdI identifier.
    - Result.
    - Number.
- **PEC section**
    - Message description.
    - PEC mailbox manager.
    - Message identifier (provider).
    - Message identifier.
- **LUL section**
    - Type.
    - Cost center.
    - Employee ID.
    - Employee level.
    - Employee position.
    - Employee establishment.
- **FIR section**
    - Number.
    - Copy number.

- Recipient PEC.

- **Folder**
  - Folder identifier.
  - Folder sequence number.
  - Folder type.
  - Folder subject.
  - Company name of the folder subject.
  - First name of the folder subject.
  - Last name of the folder subject.
  - Fiscal ID of the folder subject.
  - Tax code of the folder subject.
  - Folder start date.
  - Folder subject type.
  - Folder end date.
- **Contract**
  - Legal nature of the contract party.
  - Segment of the contract party.
  - Contract end date.
  - Contract request date.
  - Contract execution date.
  - Contract agreed amount.
  - Contract disbursed amount.

The values available for each metadata field are those stored in the document management system.
By clicking the icon next to an individual metadata field, a list opens showing the **values** present in the metadata of the published documents, with the number of related documents displayed in parentheses.

By **selecting** and **deselecting** items in the list, it is possible to search for the desired documents; options can be selected in both single-selection and multi-selection modes.
If the list contains many values, to facilitate identification and subsequent selection, it is possible to search for a specific value among those available using the search box located below the metadata field name.

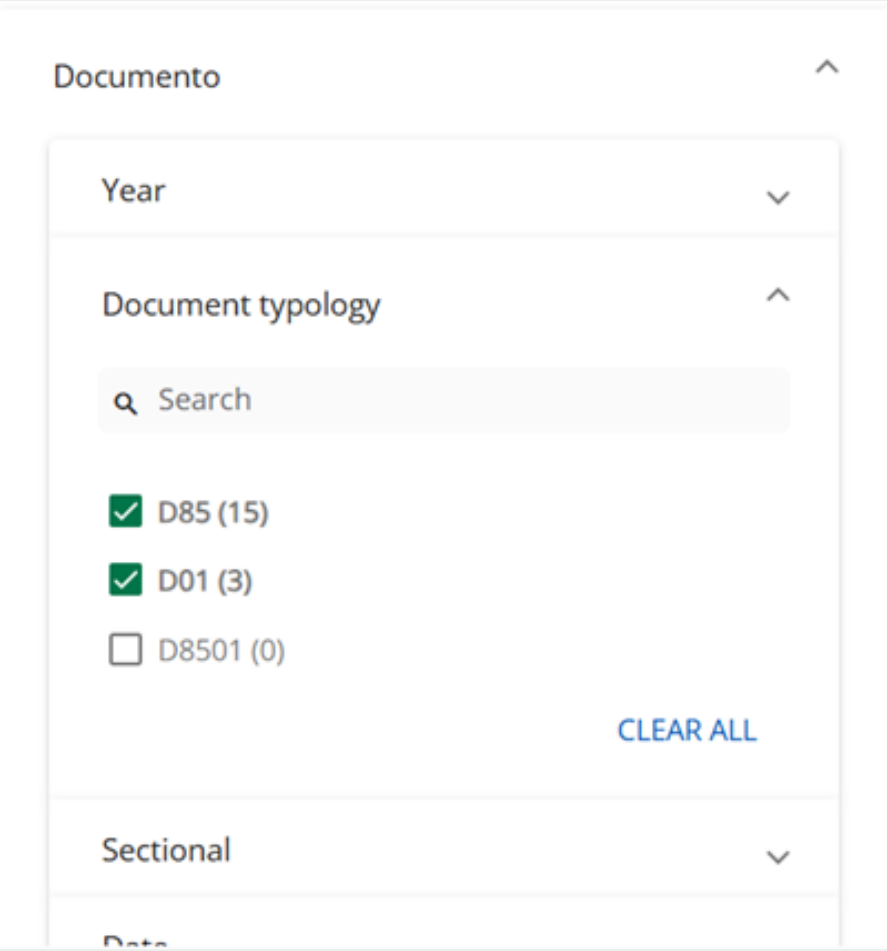

Figure 68. Filter value selection – Metadata.

The **list of documents** filtered according to the selected criteria will be displayed on the right-hand side of the search panel; from this grid, using the function buttons at the top or by right-clicking on an individual document, it is possible to:

1. **share** the document via link
2. **download** the selected document to a folder on your device
3. **preview** the document
4. **view** the document details
5. **mark** the document as a favorite
6. **copy** the document
7. **manage** document versions
8. **create** a process (workflow)

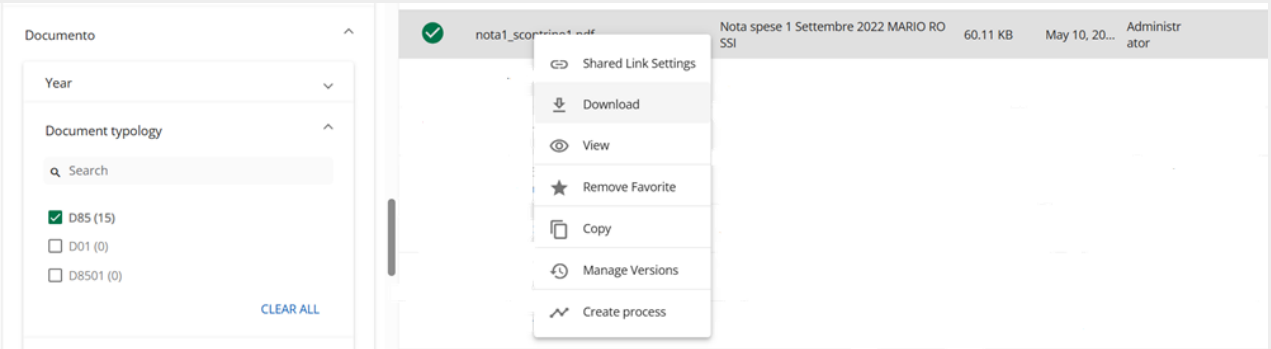

Figure 69. Filter value selection – results.

If the value of the relevant metadata does not immediately appear in the list, it can be searched for using the dedicated search field.
For each metadata value, the number of files containing it is shown (the number displayed to the left of the value in parentheses).

To filter documents by a metadata value, click on the value itself; a green check mark will appear to highlight the selection, and the system will automatically perform a search on the relevant files (displayed on the right).
As a result, all other metadata, along with their subsequently selectable values, will also be automatically filtered.

The available values for each metadata field are those present in the document management system.
If the desired metadata value does not immediately appear in the list, it can be searched using the dedicated search box.
For each metadata value, the number of files containing it is displayed (number shown to the left of the value in parentheses).
To filter documents by a specific metadata value, click on the value itself, a green checkmark will appear to indicate the selection, and the system will automatically perform a search on the relevant files (shown on the right), and, as a result, all metadata and their selectable values will also be filtered.

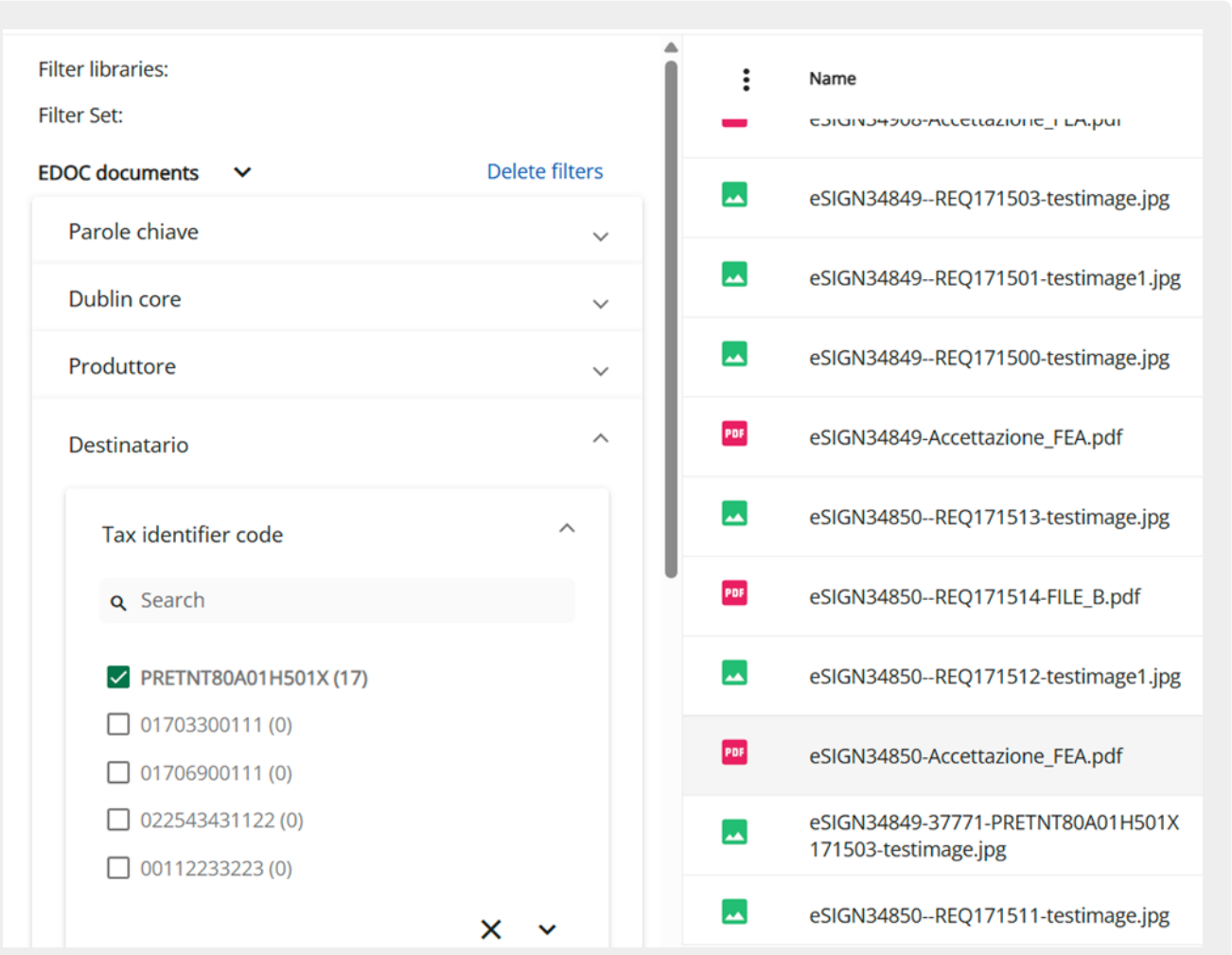

Figure 70. Filtering by the Recipient Tax Code metadata.

To remove all applied filters at once, click on "Delete filters".
To remove a single filter, click on the value again: the green checkmark will disappear, and the files and metadata with their respective values will no longer be filtered.

8.2. Smart Folders

The "**Smart Folders**" purpose is to logically group files stored in the eDOC document management service, even if they are located in different positions in the archive, into a single organized view.
This allows users to quickly identify documents with common characteristics without needing to know or navigate the physical folder structure.

As described in the previous chapters, the files stored in eDOC and uploaded through the Entaksi services are characterized by the presence of metadata, that is, descriptive attributes essential for the identification, classification, and retrieval of documents in the system (see the Research chapter).

Smart Folders are based on these metadata, leveraging their characteristics to group files and define how they are displayed in a smart folder.

For example, by setting a metadata containing a subject's tax code as the aggregation criterion, it is possible to create a Smart Folder for each individual.
When accessing one of these folders, the system will automatically perform a dynamic search in eDOC and display all documents that share the same metadata, that is, all documents related to that individual, regardless of their physical location in the document archive.

The sub-folder structure displayed in a Smart Folder reflects the structure configured when the document was published through the Entaksi services, ensuring continuity and consistency during browsing.

Identifying Smart Folders

To make them easier to identify in the document management system, Smart Folders are marked with a specific icon ( ), which distinguishes them from regular folders.

Advantages of using Smart Folders

In summary, activating Smart Folders allows user to:

- to locate documents based on their content and metadata, rather than their physical location in the archive;
- to define one or more aggregation criteria based on metadata;
- to create dynamic browsing structures in the form of folder trees, adaptable to different operational needs and business contexts;
- to view the same documents according to multiple organizational logics, without duplicating files.

Activating the service

Requests to activate Smart Folders, along with the indication of which metadata should be used as aggregation criteria, must be sent to Entaksi via email at: helpdesk@entaksi.eu.

Back to the top.

9. eMAN - Digital preservation manual

The "Guidelines on the creation, management and preservation of IT documents" published by AgID on 10/09/2020, on chapter 4.5, define the "digital preservation manager":

"In Public Administration, the digital preservation manager:
a. he is a role provided for in the organization chart of the owner of the object of conservation;
b. he is a manager or an internal officer formally designed and in possession of suitable legal, archival and IT skills;
c. he can be the responsible of the document management or the coordinator of the document management (if he s appointed).

For subjects other than the Public Administration, a person external the organization can be the digital preservation manager. He must have suitable legal, IT and archival skills and he must be different from the Digital Preservation Provider, in order to ensure the function of the owner of the object of preservation with respect to the system of storage".

From an operational point to view, the digital preservation manager must carry out the activities listed in chapter 4.5 from point a) to point m):

"a. he defines the preservation policies and functional requirements of the preservation system according to current legislation and international standards for the specific documents stored (IT documents, IT aggregations, IT archive);
b. he manages the preservation process and guarantees compliance with the law over time;
c. he generates and signs the preservation report, according to the procedures set out in the digital preservation manual;
d. he generates and signs the DIP with digital or electronic signatures in the cases provided by the digital preservation manual;
e. he monitors the correct functionality of the preservation system;
f. with a frequency not exceeding 5 years, he carries out a periodic check of the integrity and legibility of IT documents and all the document aggregations in the archives;
g. in order to ensure the preservation and the access to electronic documents, he adopts measures to detect any degradation of the preservation and to restore correct functionality;
h. he duplicates the IT documents in relation to the evolution of the technological context, in accordance with the digital preservation manual;
i. he prepares the necessary measures for the physical and logical security of the preservation system as foreseen by par. 4.11;
j. in the appropriate cases, he ensures the presence of a public official, guaranteeing him the necessary assistance and resources for carrying out his activities;
k. he ensures the necessary assistance and resources for the performance of verification and surveillance activities by the competent subject required by current regulations;
l. he provides to send IT documents, IT aggregations and IT archives, and all the tools which guarantee its consultation to the Central State Archives and to the territorially competent state archives, according to the deadlines set by art. 41, paragraph 1 of the Code of cultural heritage;
m. he prepares the digital preservation manual and he takes care of its periodic updating in case of regulatory, organizational, procedural or technological changes."

All the activities listed in letters a) to l), which include technical monitoring, the generation of the payment report, the definition of security and technical policies for the maintenance of the preservation system, and others, can be delegated to the Preserver.

The only non-delegable activity, which therefore remains in the hands of the digital preservation manager, is the one relating to point m), that is **the creation and the maintenance of the digital preservation manual according to the criteria defined by the Guidelines**.

Since the digital preservation manual is a must for PA and private individuals, Entaksi provides a **specific service through which it is possible to obtain a manual that is already conformed to the Guidelines**, containing the description of the preservation processes already used. It will also be kept constantly updated with respect to changes in legislation and methods of the preservation service.

When the manual has been digitally signed by the digital preservation manager, it will be stored through the Entaksi conservation service.

9.1. Digital preservation manuals

In order to access to the interface to create the digital preservation manual, you can enter in Entaksi Console and click on the dashboard button "**Digital Preservation Manual**" or click on the top menu item "**Digital Preservation Manual**" and choose one

of the submenus.

The **Digital preservation manuals** section contains a list of all the manuals created with the service.

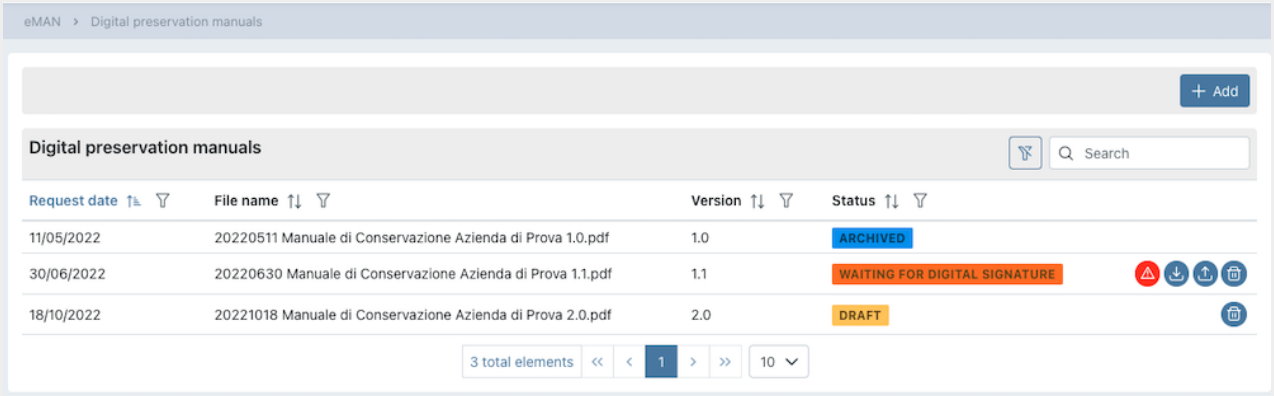

Figure 71. Digital preservation manual

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

- **Request date**: it is the date of the manual's request. This data is editable only as long as the status of the manual is in "Draft".
- **File name**: it is the name of the manual. It isn't editable and t is automatically crated by the system.
- **Version**: it is the version of the manual. This data is editable as long as the status of the manual is in "Draft".
- **Status**: it is the status of the manual.

From here it is possible :

- to sort the columns and to filter the elements in the grid;
- to access to the detail of the digital preservation manual by clicking twice on the single line in order to make any changes to the data. It is possible only in the case the manual's status is in "Draft";
- to remove an unsigned manual by clicking on the icon ;
- to download e to upload the manual by clicking on the icons and ;
- to insert new manuals by clicking on the "**Add**" button.

The table below shows the states available when processing the manual:

Valore	Descrizione
DRAFT	The manual is created but not required. In this state it is still possible to make any changes to the request date and to the version of the manual or to delete it.
WAITING DATA	The Digital preservation manual was requested, but since the details of the company contact person and the digital preservation manager are missing, the system has not started the generation process. The Digital preservation manual will be automatically created only when the information regarding the digital preservation manager and the contact company person is set up, and the status will change to "*Processing*".
PROCESSING	The manual was requested and the system starts the process of its creating.
WAITING FOR DIGITAL SIGNATURE	The manual has been created, but it must be digitally signed to be validated. In this state it is not possible to change the request date and version, but it is can be deleted.

Valore	Descrizione
PROCESSING	Final state of processing: the manual was created and digitally signed, it is therefore compliant with regulations and ready to be downloaded.
ARCHIVED	Archiving status successful: the manual was entered in the preservation system thanks to the automatic generation of a SIP, which has been validated and automatically sent for storage.
ARCHIVING ERROR	Archiving status with errors. This state could be caused because the SIP's automatic creation with the manual inside went in error, or the created SIP has not been validated and therefore refused for preservation.

The digital preservation manual processing workflow is as follows:

1. Create a new digital preservation manual's request in draft status and then start it. (see Digital preservation manual request)
2. Wait for the manual to be created and the changing of the status from "*Processing*" to "*Waiting for digital signature*".
3. When the status changes into "*Waiting for digital signature*", in case the automatic signature certificate issued by Entaksi is not available, you can download the digital manual, check it and sign it in a digitally way and upload it again using the upload button.
4. When the state change from "*Waiting for digital signature*" into "*Processing*", it will be possible to download the digitally signed preservation manual.
5. The service automatically creates a SIP (approximately weekly) and sends it in the preservation system. If the SIP is accepted, the status of the manual changes automatically in "*Archived*", otherwise, the status of the manual will be "*Archiving Error*".

9.1.1. Digital preservation manual request

In this section it is possible to create a new digital preservation manual request and to start it. It is possible to make changes, exclusively if its status is in "*Draft*".

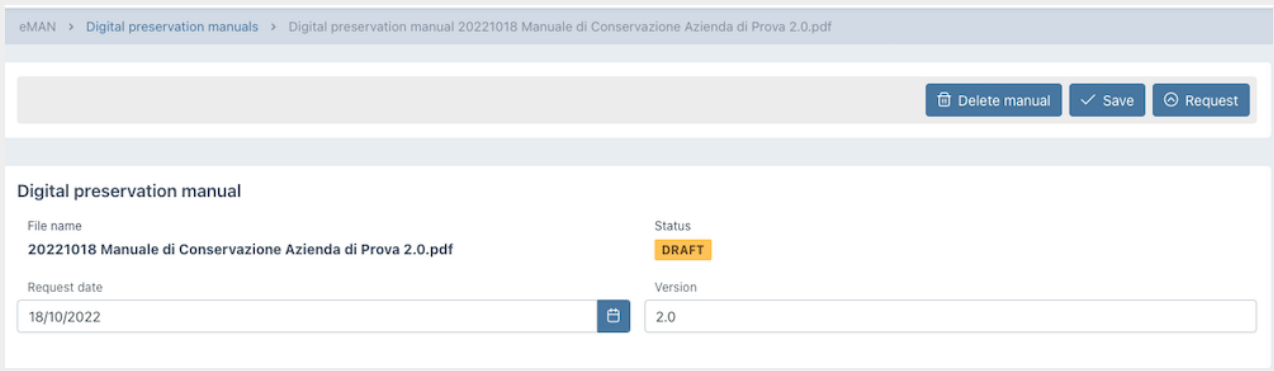

Figure 72. Digital preservation manual's request

The default state is "draft" and it is not possible to modify it.

The name of the file is automatically generated by the system, it can not be modified and it is made up as follows:
`"yyyymmdd" + "Manuale conservazione" + "Company name" + "Version" + ".pdf"`
Where:

- "yyyymmdd": it is the year, the months and the day of the request of the manual;
- "Manuale conservazione": it is a wording automatically inserted by the system;
- "Company name": it is the name of the company for which you are creating the manual;
- "Version": it is the version of the manual. The system automatically proposes the following number of the last created one;

- ".pdf": it is the file extension.

Assuming the first digital preservation manual is being created in 2021-06-07 for the ROSSi SRL company, the following name will be automatically proposed:

"20210607 Manuale conservazione ROSSI SRL 1.0.pdf"

The values of the request date and the version number can be changed, remaining, however, congruent (consecutive) with the date and version of the last manual.

By clicking on the top buttons:

- "**Delete manual**": the manual will be deleted;
- "**Save**": all changes made to the manual will be saved;
- "**Request**": the current manual processing will begin. It will **not** be possible to start a new request if there isn't a digital preservation manager for the specified date. It means that the role end date of the digital preservation manager (if it exists) must be higher than the request date of the manual (chapter Digital preservation managers)

It would be possible to come back to the digital preservation manuals list by clicking on the breadcrumb on the top "Digital preservation manuals".

9.2. Configurations

By clicking on the menu item "Configurations", a submenu is opened and by clicking on the respective item it is possible to check, modify and insert the personal data of the **Digital presentation managers** and of the **Company contact person** and the logo that is automatically shown in the digital preservation manual.

9.2.1. Digital preservation managers

In the **Digital preservation managers** section all the inserted preservation managers are shown in a list.

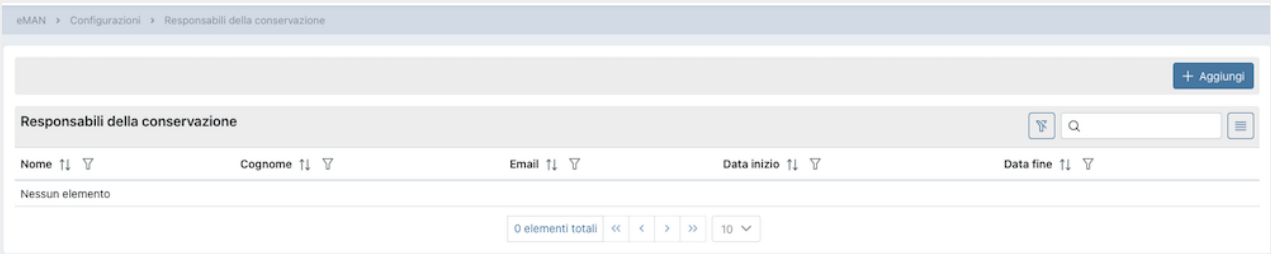

Figure 73. Digital preservation managers

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

- **Name**: the digital preservation manager's name;
- **Surname**: the digital preservation manager's surname;
- **Start date**: the digital preservation manager's role start date;
- **End date**: the digital preservation manager's role end date.

Thanks to the start and the end date of the role, it is possible to have the historian of the digital preservation managers.

From here it is possible:

- to sort the columns and to filter the elements in the list;
- to access the detail page by clicking twice on the single row in order to make any changes.
- to insert new managers by clicking on "**Add**".

9.2.2. Adding digital preservation managers

In this section it is possible to add new digital preservation managers. It is not possible to delete an inserted digital preservation manager.

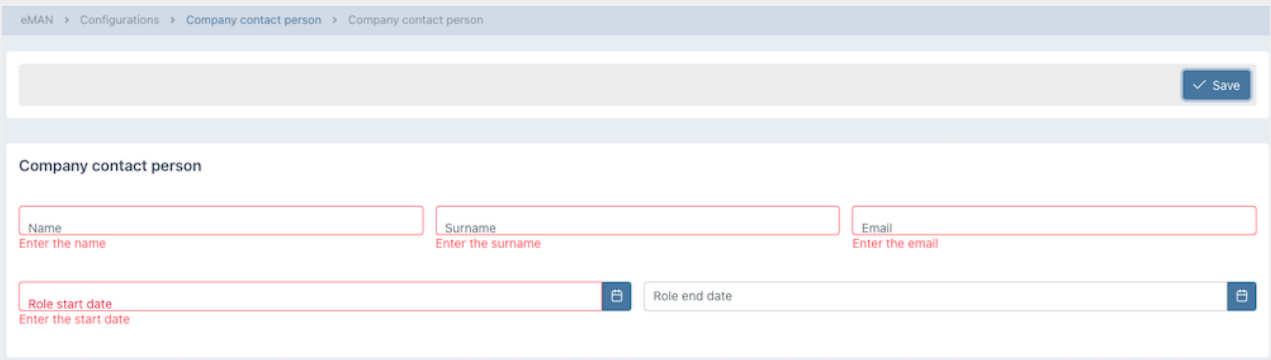

Figure 74. Adding digital preservation managers.

It is necessary to insert the following data:

- **Name**: it is the digital preservation manager's name. It is a mandatory item.
- **Surname**: ist is the digital preservation manager's surname. It is a mandatory item.
- **Email**: ist is the digital preservation manager's e-mail. It is a mandatory item.
- **Role start date**: it is the digital preservation manager's role start date. It is a mandatory item.
- **Role end date**: it is the digital preservation manager's role end date. if it is not inserted it indicates that the role is active until a date to be determined.

The mandatory items are shown in red and it is not possible to save until they are correctly entered.

All the entered data is saved by clicking the "**Save**" button.

It would be possible to come back to the digital preservation managers' list by clicking on the breadcrumb on the top "Digital preservation managers".

9.2.3. Company contact person

In the **Company contact person** section all the inserted company contact people are shown in a list.

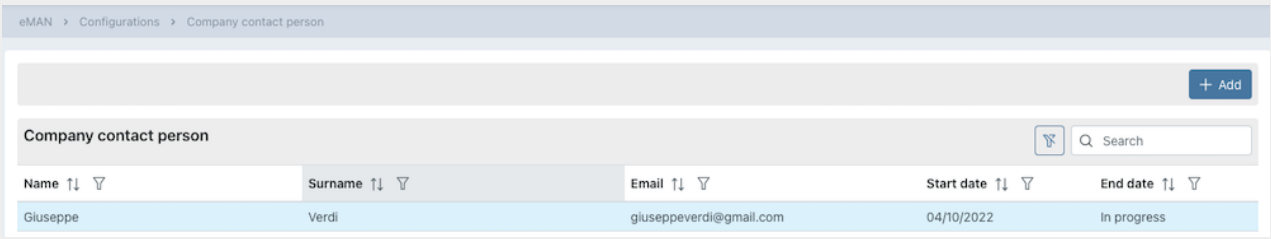

Figure 75. Company contact person.

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

- **Name**: the company contact person's name;
- **Surname**: the company contact person's surname;
- **Start date**: the company contact person's role start date;
- **End date**: the company contact person's role end date.

Thanks to the start and the end date of the role, it is possible to have the historian of the company contact people.

From here it is possible:

- to sort the columns and to filter the elements in the list;
- to access to the detail page by clicking on the single row in order to make any changes.
- to insert new managers by clicking on the "**Add**" button.

9.2.4. Adding company contact person

In this section it is possible to add a new company contact person. It is not possible to delete an inserted company contact person.

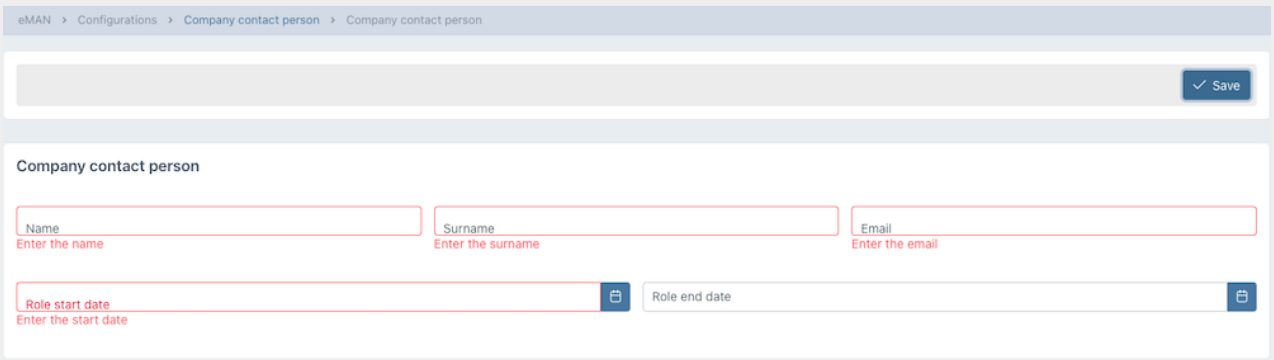

Figure 76. Adding a company contact person.

It is necessary to insert the following data:

- **Name**: it is the company contact person's name. It is a mandatory item.
- **Surname**: ist is the company contact person's surname. It is a mandatory item.
- **Email**: ist is the company contact person's e-mail. It is a mandatory item.
- **Role start date**: it is the the company contact person's role start date. It is a mandatory item.
- **Role end date**: it is the the company contact person's role end date. if it is not inserted it indicates that the role is active until a date to be determined.

The mandatory items are shown in red and it is not possible to save until they are correctly entered.

All the entered data is saved by clicking the "**Save**" button.

It would be possible to come back to the company contact people's list by clicking on the breadcrumb on the top "Company contact person".

9.2.5. Adding a company logo

In this section it is possible to save the company logo which will be automatically shown in the digital preservation manual.

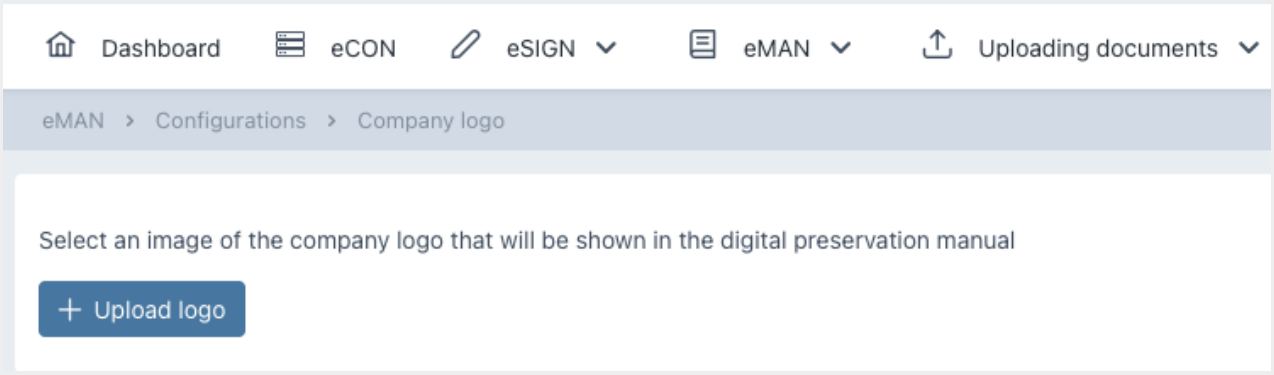

Figure 77. Uploading company logo.

It is possible to upload the company logo by clicking on "**Upload logo**". When uploaded, the logo will appear in the body of the page. In order to delete the uploaded logo, just click on the icon and upload another logo.

9.3. Sign and preservation

Once obtained the digital preservation manual, in order to make it legally valid, and archive it in the preservation system, it is necessary to proceed with the digital signature.

The digital signature can (currently) be applied in two distinct ways: through the automatic remote certificate issued by Entaksi, or through any signature device registered to the digital preservation manager.

Signature through signature device or remote certificate
In order to digitally sign the Digital preservation Manual using your own signature device, you need to download the Manual by clicking the button in the row.
The Digital preservation manager may review the Digital preservation Manual.

If there are any errors or anomalies, the Manual can be deleted by clicking the button to proceed with a subsequent generation.
If the Digital preservation Manual is correct, the digital preservation manager can proceed to digitally sign it with their own device and upload it back to the system by clicking the button .

The document has protection of the content.
Some digital signature software cannot sign documents in PAdES format with this protection. In this case, the document can be digitally signed in CAdES format (p7m).

For the application of a qualified electronic signature, Entaksi offers its eSIGN Desktop signing application.
Information regarding the installation and management of the software and the service is available in the eSIGN service user manual, which can be downloaded from the following link https://www.entaksi.eu/pdf/docs/doc_services/UM_eSIGN_Manuale_utente.pdf, under the "*eSIGN Desktop*" section.

Signature through automatic remote certificate

If an automatic remote certificate issued by Entaksi has been purchased and configured on the service, no manual action is required after the Digital preservation manual is generated: the Digital preservation Manual is automatically signed by the service.

Send to preservation system
The signed Manual will assume the status "*Processing*".
Thanks to an automatic process, when the digital preservation manual will be signed and reload into the system, the system proceeds to create a SIP and to send it in the preservation system. When the SIP containing the manual will be present in the preservation system, the manual's status will be changed from "Archiving" to "Archived" as described in Digital preservation manuals paragraph.

The archived manual can be searched in Entaksi Console, as described in the paragraphs SIP List and Search and request documents.
In particular in the SIP list, the manual's SIP will appear with the description "Manuale di conservazione" and it will be possible to see the detail, as described in SIP List.

When the SIP is in "Accepted" state and its relating AIP is "Closed", it will be possible to do a "Search and request documents" by inserting the *Documento type - is equal to - D8503 Manuali* as criteria. If it is necessary, it would be possible to request the relative DIP.

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.

Document Management Divisions

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 (Titolario)

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) Nº 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 ofr 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) в „- 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 ePRI, **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, comma3, 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).

Istruzioni per la produzione e conservazione del registro giornaliero di protocollo

Istruzioni ufficiali pubblicate da AgID nel marzo 2016 (Official instructions published by AgID in March 2016.)

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 accesibility.

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 https://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 at the following link: https://www.entaksi.eu/politica-sicurezza-informazioni/.

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 the 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.