User Manual

UM ePEC en 20230516 User manual

Entaksi Solutions SpA

Index

Document information

Project	User Manuals
Type	User Manual
Document ID	UM ePEC en 20230516 User manual
Version	1.0.0
Creation Date	16/05/2023
Last Revision	16/05/2023
Author	Erica Negri
Status	Released
Classification	Public

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

Document approval

Date	Employee	Mansion	Signature
16/05/2023	Paola Caioli	DelM	*Digital signed*

Revisions

Date	Version	Name	Mansion	Action	Distribution
16/05/2023	0.0.1	Erica Negri	IMSM	Draft creation.	Internal
16/05/2023	1.0.0	Erica Negri	IMSM	Release.	{Intestazione-distribuzione-01}

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 1 di 66

1. Introduction

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

The **ePEC** service is used to preserve documents relating to the mail sent o recived from a PEC box.

Entaksi appears in the list of **Accredited Digital Preservation Management for the storage of IT documents for the Italian Public Administration**. This accreditation was obtained at the Agency for Digital Italy on 17/03/2016.
The Storage 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 storage is based on supports with characteristics of high reliability and high permanence of data, and its duration is established in the service contract.

For a detailed description of all eCON system technical characteristics, please refer to the Entaksi digital preservation manual which is published on AgID and Entaksi website.

This manual describes:

- how to access the service and how to use it, in the chapter Entaksi Console registration procedure;
- all the functions provided by the ePEC service, in the chapter ePEC Console;
- information security procedures.

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

ePEC is available in SaaS (Software as a Service) mode, and it can be reached through the web interface hosted by the Entaksi infrastructure. From the interface it is possible to monitor the digital preservation system and to manage all the operations that can be performed by the service. 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 extrems in the initial block "Revisions".

Back to top.

1.1. ePEC service features

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

Figure 1. ePEC service.

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

Back to top.

2. Roles and responsibilities

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

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

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

The legislation defines "**Preservation manager**" as the natural person who defines and implements policies necessary for document storage, and he is responsible for managing documents. 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 D.P.C.M 3 December 2013, "The preservation can be entrusted to an external subject, according to the organizational models referred to in art. 5, through a contract or service agreement that provides for the obligation compliance with the preservation manual prepared by its manager.".

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**.

ePEC 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 ePEC Manager tasks.

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

The roles are represented in the following diagram.

Figure 2. Roles and responsibilities.
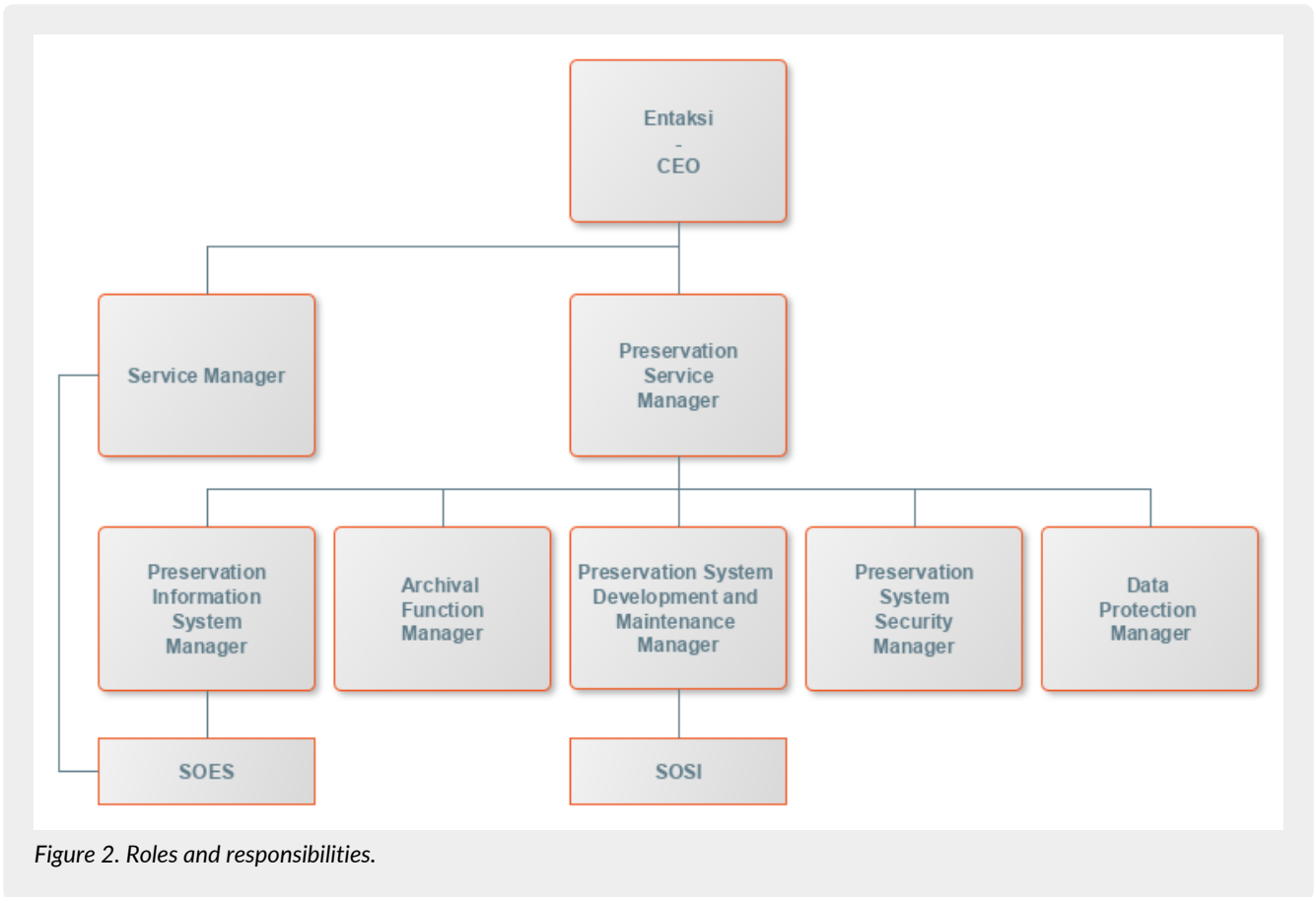
Entaksi Solution SpA is responsible for the provision of the service, and the Preservation Service Manager is the role appointed for the service delivery tasks. Preservation Service Manager can rely on the structures described in the following paragraphs to carry out his duties.

Back to 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 ePEC 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** assistenza@entaksi.eu.
> **SDOS is active from Monday to Friday from 09:00 to 18:00**.

Back to top.

2.2. Information System Operational Support (ISOS)

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

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 4 di 66

It works closely with SDOS to manage any malfunction report.

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

Back to top.

2.3. ePEC Manager tasks

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

Table 1. Tasks.

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

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

2.4. Service management responsibilities

Table 2. Responsibilities

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

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS   Pag. 5 di 66

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

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

Back to top.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS

Pag. 6 di 66

3. Entaksi Console registration procedure

ePEC service can be accessed after a **user registration to the Entaksi system Console**, which is reachable at the address:

- https://entaksi.eu/console

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

In order to access to the chosen service, each user must be **registered on the Entaksi Console platform**. He can log into the desired service using his registered credentials (username and password). Credentials are unique for every service provided by Entaksi.
The registration platform complies with the OAuth2 standard which guarantees high levels of access and credential protection.
The access to services' functionalities is subject to the completion of the contract.
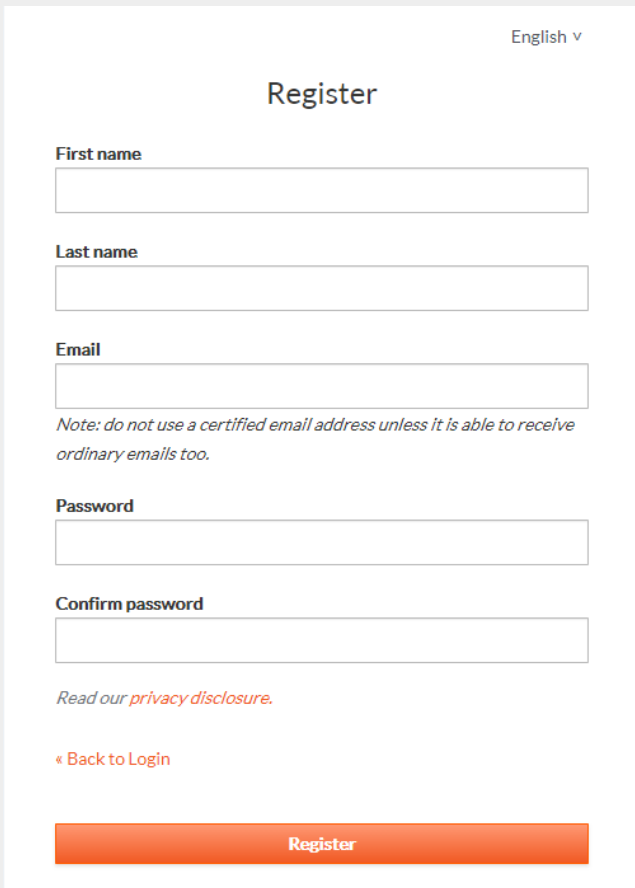
In order to register himself, the user must therefore access the Entaksi Console and click on the link "**Register**" placed next to the question "New User?".

Figure 3. Sign in.
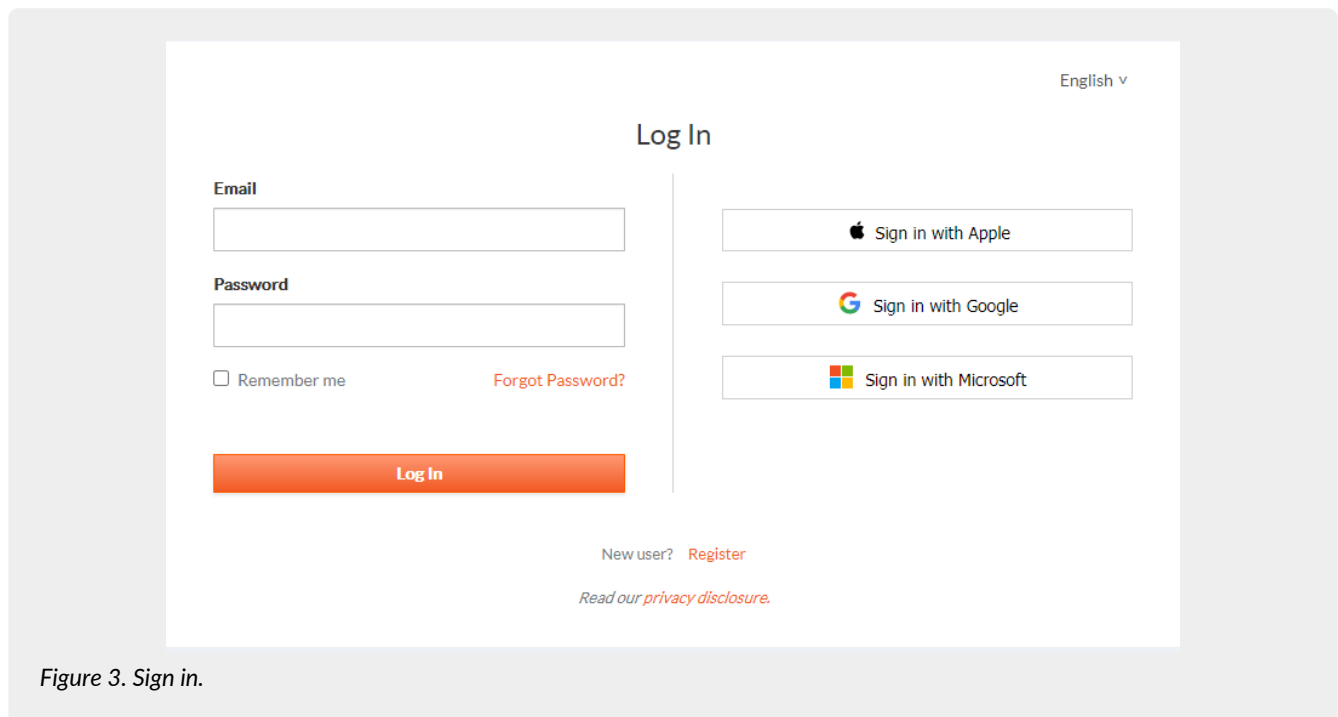
Into the following form the user must enter his personal data: name, surname, **NOT PEC email if not enabled to receive non-certified email**, username and password.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 7 di 66
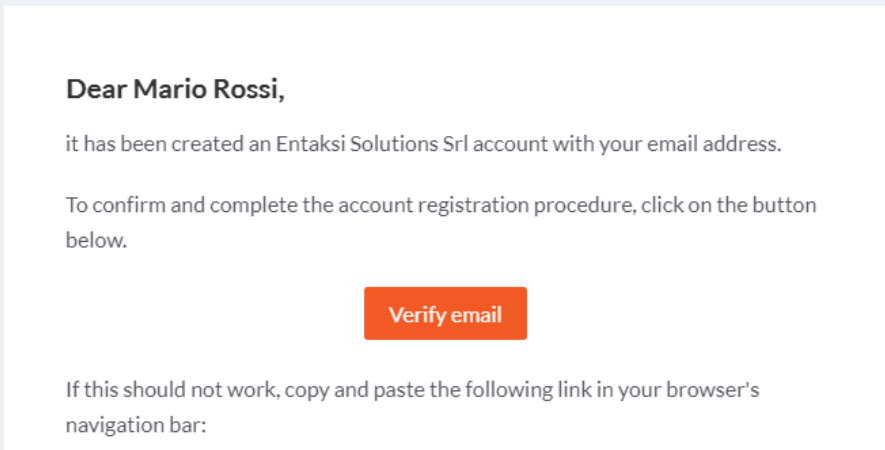
Figure 4. Inserimento dati.

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

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

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

Figure 5. Email confirmation.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 8 di 66

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

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

3.1. Single Sign-on access

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

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

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

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

Back to top.

3.2. Resend registration link and password recovery

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

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

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

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

3.3. How to access the Service

The Service is available using the following browsers:

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

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

Back to top.

3.4. User settings management

From the ePEC 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

ENTAKSI SOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 9 di 66

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 10 di 66

4. ePEC Console

ePEC service is available on **Entaksi Console**, the web application that allows you to **upload digital documents, search them within the storage system and download Dissemination Information Packages (DIP), which contains legally-compliant documents and proofs to be exhibited in the event of inspection or control**.

4.1. Dashboard

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

All contracted services are displayed in "**My services**" section.
By clicking on each service button, the main page opens.
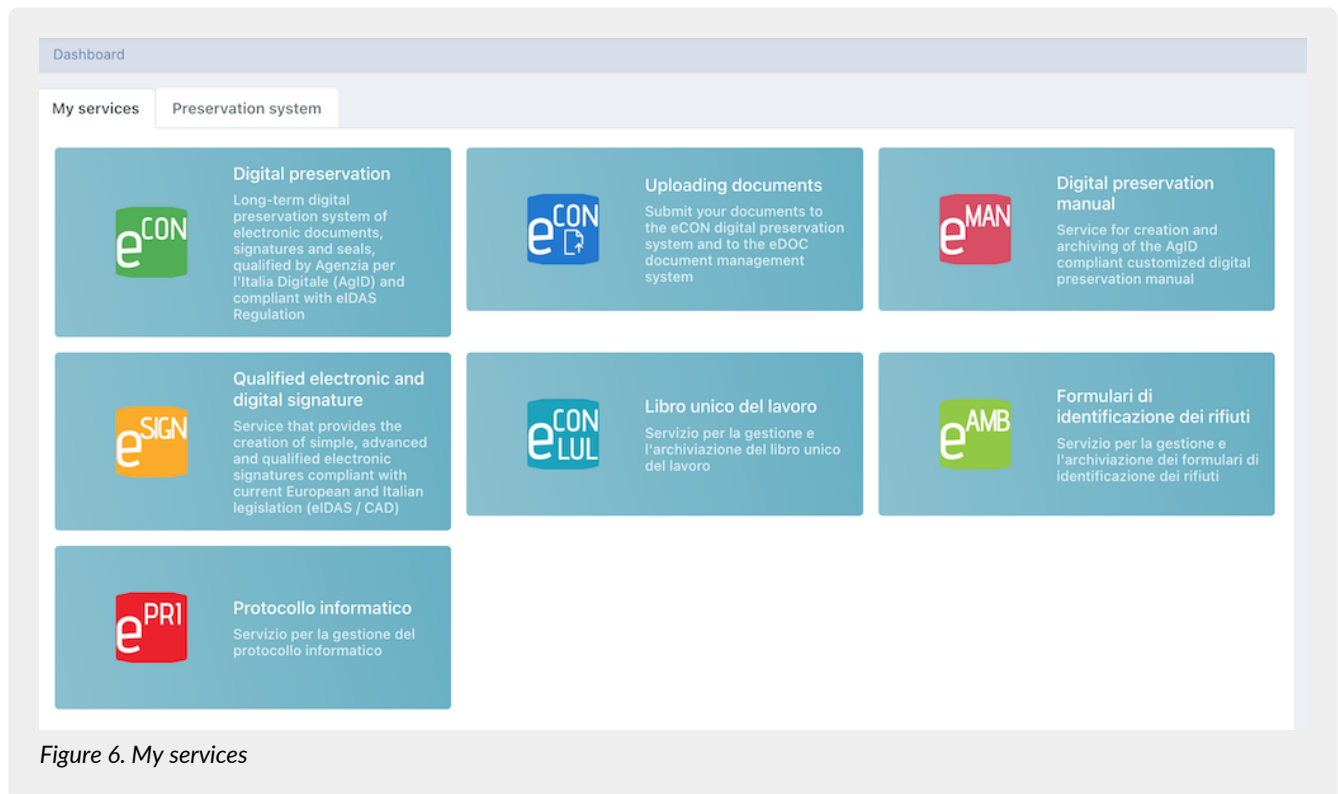
Figure 6. My services

The "**Preservation system**" section presents a summary of the archive status, with the quantity of space disk occupied, number of documents and files uploaded.
Below there is a summary of the latest uploaded documents divided into three sections Submission Information Packages, Archival Information Packages and Dissemination Information Packages.
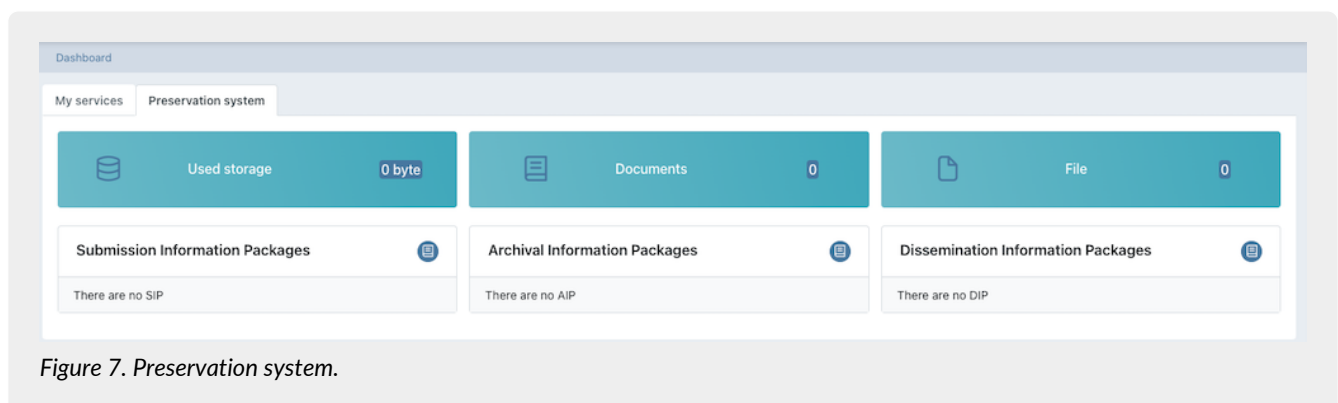
Figure 7. Preservation system.

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

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 11 di 66

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

4.2. Console tables

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

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

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

For all system tables, two functions are particularly useful to have an immediate search within the list: the **Filters** and the **Sorts**.
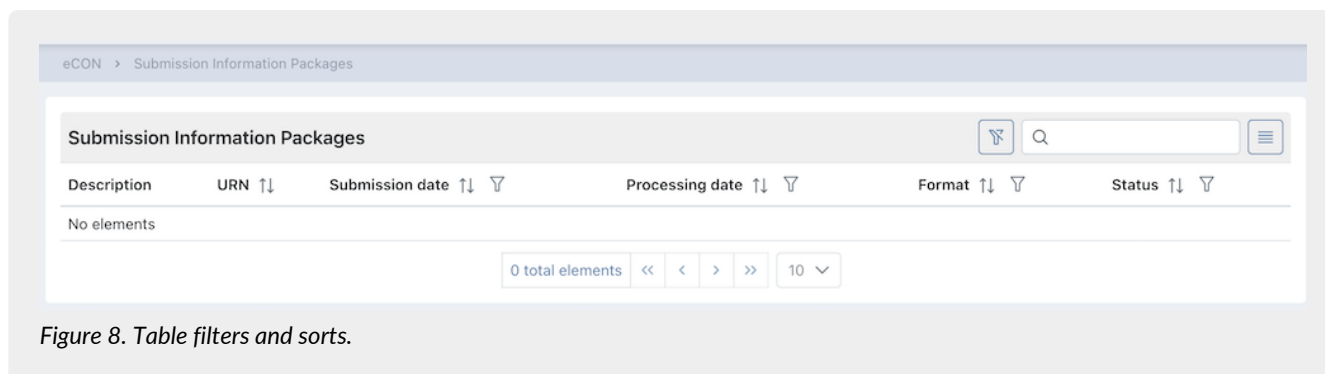
Figure 8. Table filters and sorts.

By clicking on the column header on the ↑↓ icon you can sort the list in ascending order (and in this case the icon becomes ↑≡) or in descending order (and in this case the icon becomes ↓≡).
There are several types of available sorting:

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

In order to filter data, you have to click on the icon ▽ on the desired column.
A form opens and you can enter the desired filter.
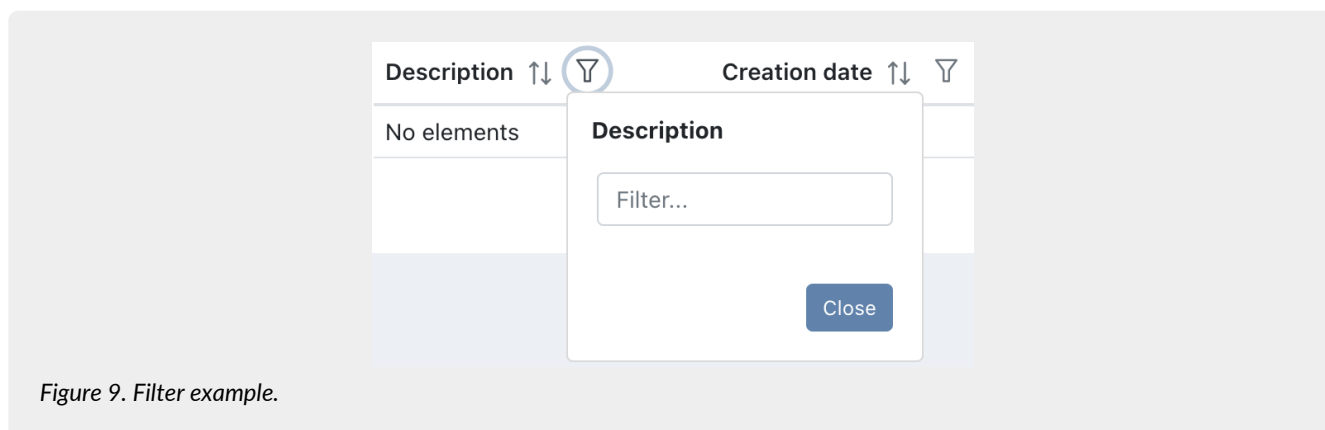
Figure 9. Filter example.

By entering the criterion and clicking the "**Close**" button, the list filters and the icon turns colored (▽). It indicates the presence of a criterion.
Hovering with the mouse over the icon a tooltip displays the criterion without entering in the form again.
By clicking on the delete filter button (▽) placed at the top right next to the box search, you can massively eliminate all the filters and orders of the list.
On the other hand, if you have several filters set but you need to delete a single one, you have just to click on the "filter" icon again, enter the form, delete the criterion and click the "Close" button.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 12 di 66

ENTAKSISOLUTIONS

Various filter types are available:

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

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

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

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

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

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

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

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

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

4.3. Console Menu

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

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

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

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

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

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

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

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

⛔	**WARNING**: in order to have a quick access to Entaksi services, **we recommend to memorize the login page link and not the single page one**. This is for two fundamental reasons. 1. The direct link to the pages, the one obtained after performing an authentication through the access form, it keeps in memory, in addition to the address of the page, also the entered user and login. For security reasons, a password change is required every 90 days. Once the password has been changed as requested, the previously saved link will not allow access to the pages of the service, as the password saved in the link is different from the new one. On the other hand, by logging via the link to the access page, the problem does not exist because you have to enter the login and password again. 2. The direct link to the pages, in addition to keeping the user and password in memory, also keeps a specific page address. In case of a refactoring or maintenance of the service, the pages can be moved or renamed. For this reason, the stored link could be incorrect returning a "404" error of "Page not found". On the other hand, by logging via the link to the access page, the problem does not exist because pages are reloaded.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 13 di 66

5. Configuration

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

The menu contains:

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

5.1. Company master data

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

The data cannot be changed directly, because it refers to the service contract. For any changes it is necessary to contact assistenza@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 ePEC service.
ACTIVATED	The user is inserted and the role is active: the user can access to the ePEC service.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 14 di 66

Value	Description
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 ePEC service.

To insert a new user, click on the "**Add**" button. A new form opens where you have to enter the user's name, surname and email. You have also to select a profile among those available.
Each service has roles and dedicated configuration possibilities.
Mandatory fields are shown in red and you'll save only if they are correctly filled in.

5.2.1. eCON service access management
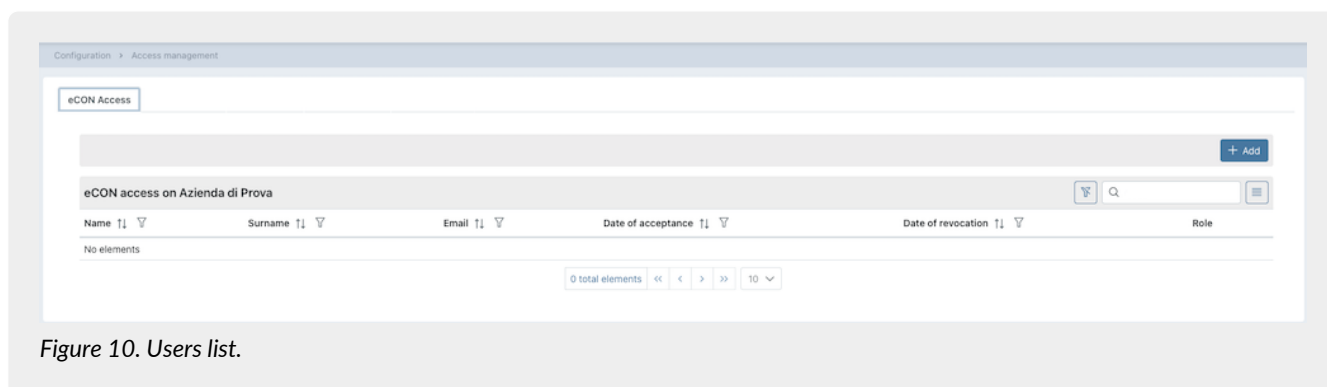
Figure 10. Users list.

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

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

If the enabling of document visibility segregation on eCON has been requested, it can be entered when entering the user.
In fact, when you are entering the user, you can choose one of the listed segregation possibilities. So, the user can manage **only** the eCON documents for which he has been enabled.
In case an user must have no restrictions (he can manage all documents), just do not select any item.

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

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

5.3. 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.
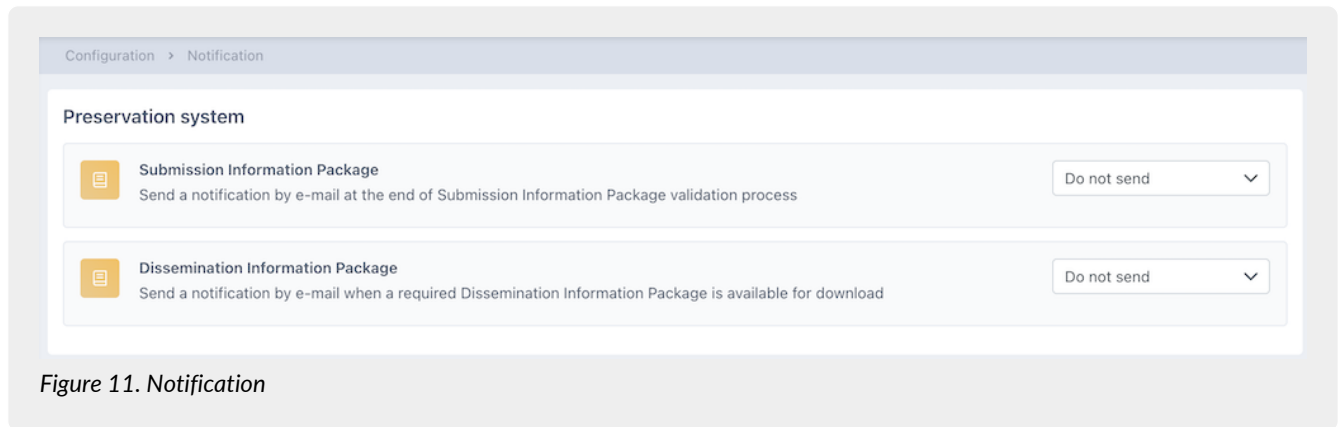
Figure 11. Notification

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.
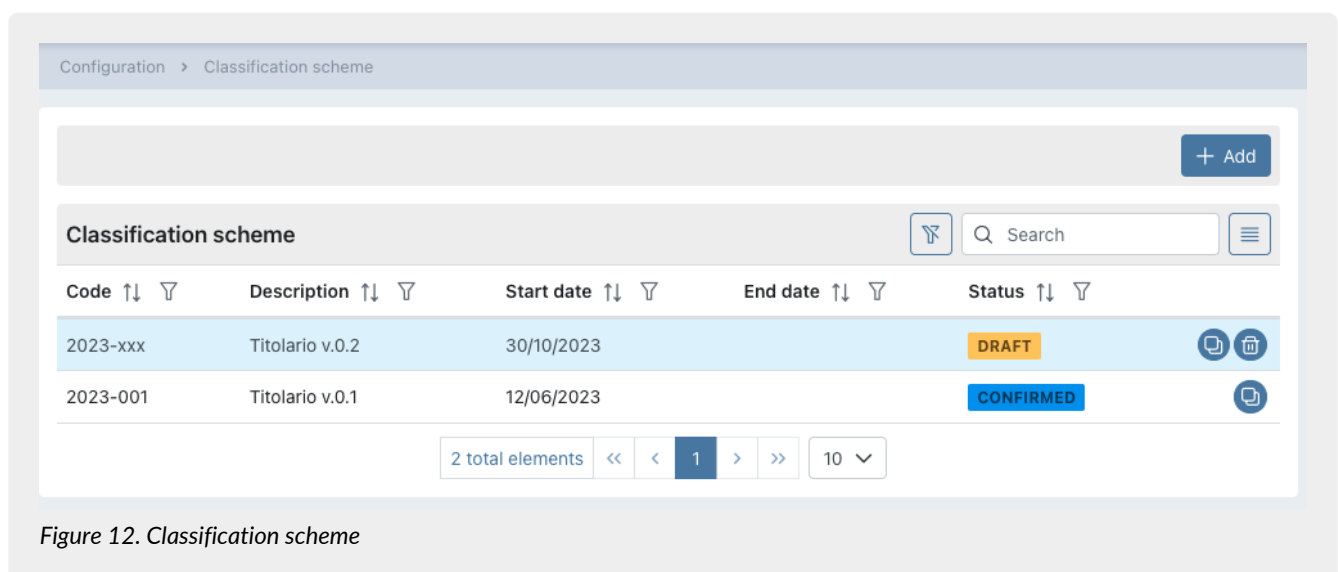
Figure 12. Classification scheme

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**: descprition enterd 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 Entering a classification scheme) and the start date which will be equal to the day after the duplication date;
- to enter in the classification scheme detail page by clicking on the row. If it is in "Draft" status, you can modify it. If it is in "Confirmed" status, you can put it back in draft status only if its start date is after the current one. In any other case, you can only see its structure or apply it only on eDOC, only on eCON or both on eDOC and eCON (see.Entering 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. Entering 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 13. Entering a classification scheme.

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

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

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

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

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

It should be noted that the start date must **not** overlap with any start date of classifications previously entered in the system.

The service proposes the day following the date of creation as the default start date in order to prevent any error.

The expiry date may also not be entered: the system will automatically enter this date upon confirmation of a new

classification by reporting in this field the day before its start date.

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

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

This field is mandatory to confirm the classification scheme.

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

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

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

To cancel a previously entered value, click on ☒ .

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

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

This classification scheme has a tree structure.
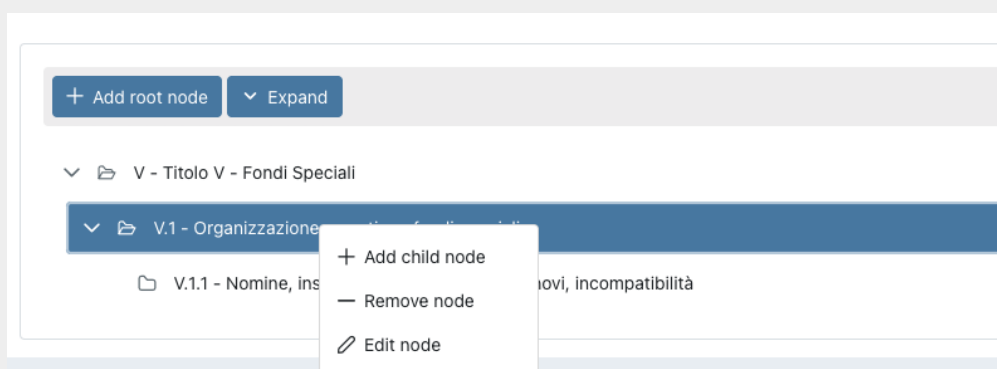
Figure 14. Example of classification scheme structure

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

To insert / edit / delete 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 "**Delete 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 18 di 66
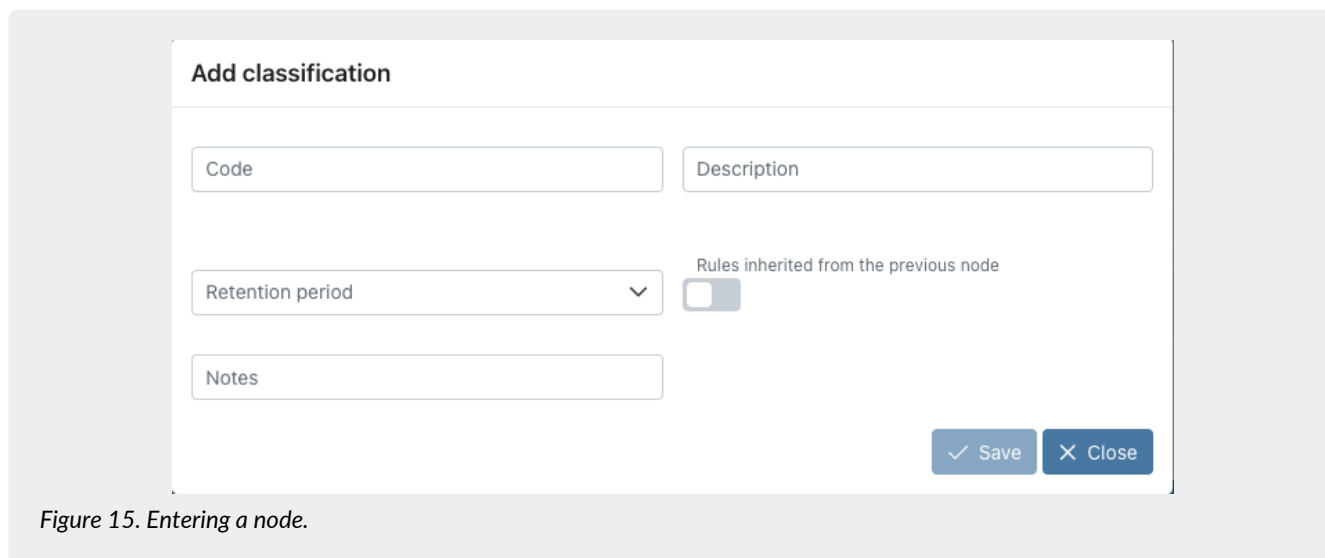
Figure 15. Entering a node.

To complete the entry, it is necessary to enter the code and description of the node, any additional notes, define a conservation rule, choosing an element from those proposed in the list or inherit the rule of the "parent" node by ticking the relevant item, and click the "**Save**" button.
You can choose to inherit the retention rule from the parent node only for child nodes. On the root nodes, this option is not visible.

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

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

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

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

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

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

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

5.5. Organizational areas

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

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

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 19 di 66
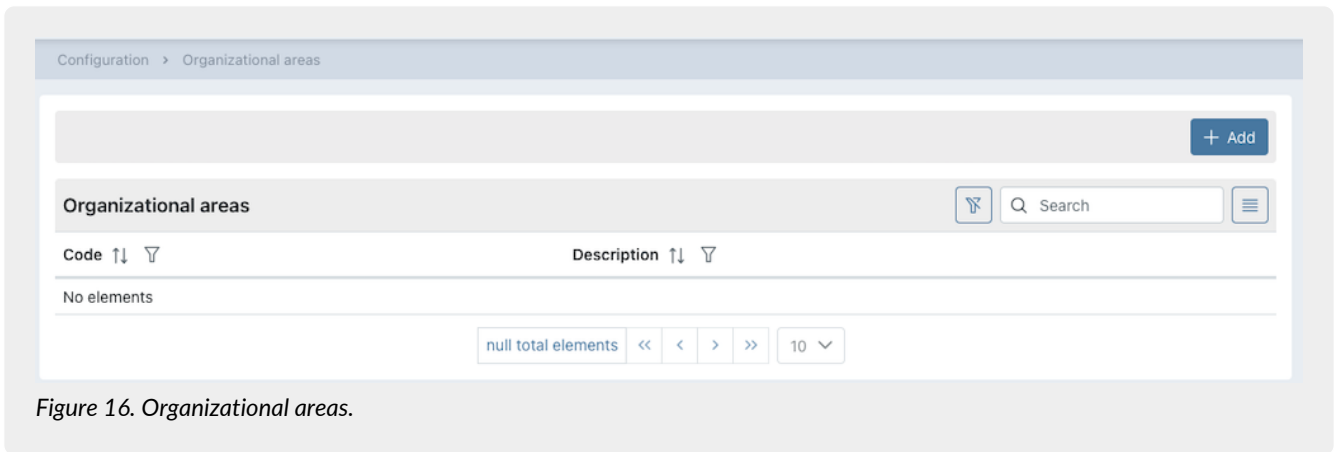
Figure 16. Organizational areas.

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

From this section it is possible:

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

5.5.1. Entering organizational areas

By clicking on the "**Add**" button a new page opens where you can insert a new organizational areas.
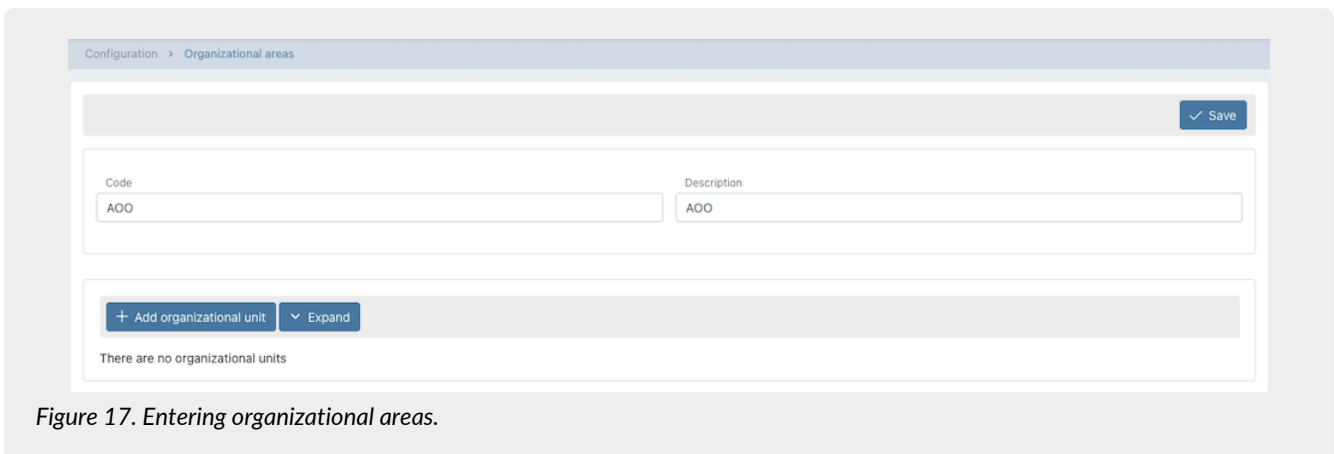
Figure 17. Entering organizational areas.

In order to uniquely identify an organizational area, you have to enter a code and a description.
To save the entered data, click on the top right "**Save**" button.
To enter a new organizational area click on the "**Add organizational unit**" button. The inserted organizational units have a tree structure.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS   Pag. 20 di 66
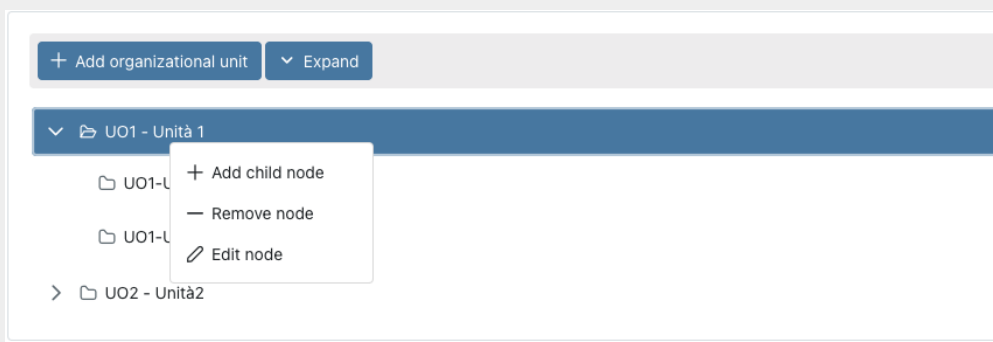
Figure 18. Example of organizational area structure.

To insert / edit / delete 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 "**Delete 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 19. Entering organizational area units.

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

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

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

6. eCON - Preservation

Once logged into the Entaksi Console, to access the interface of ePEC 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 Anformation 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.

6.1. Pacchetto PEC

To archive Certified Electronic Mail (PEC) messages with ePEC service, it is necessary to produce a dedicated SIP, said **PEC package**.
The PEC package is a .zip file. It must **exclusively** contain one or more folders named as the address of the PEC box of the documents being preserved. Inside each folder, there must be the messages received or sent from that PEC box in a `.eml` or `.mbox` format.

In general, the following types of messages can be present in each PEC mailbox:

- message sent without S/MIME signature;
- message received from another PEC mailbox with S/MIME signature;
- message received from another non PEC mailbox without S/MIME signature;
- message received from the PEC mailbox manager in acceptance of a sent message with an S/MIME signature;
- message received from the recipient's PEC mailbox manager in acceptance of a sent message with an S/MIME signature.

You have to download messages you want to preserve in `.eml` or `.mbox` format from the PEC boxes. The `.mbox` files are split into `.eml` files while processing.
Then, you have to make a "PEC package" with the characteristics previously described.

You have to group the PEC box messages (sent or received) in distinct folders. Each folder must be renamed with the name of the address of the PEC box itself.

For example, suppose you want to archive messages ("message1.eml","message2.eml", "message3.eml") contained in Mario Rossi's pec mailbox ("mario.rossi@pec.it") and the messages ("message4.mbox","message5.mbox" and "message6.mbox") contained in Aldo's pec mailbox Bianchi ("aldo.bianchi@pec.it"). After downloading the messages, they have to be divided into two folders, "mario.rossi@pec.it" and "aldo.bianchi@pec.it". The first folder contains "message1.eml, message2.eml, message3.eml" and the second one contains "message4.mbox, message5.mbox, message6.mbox", that is:

- mario.rossi@pec.it
  - message1.eml
  - message2.eml
  - message3.eml
- aldo.bianchi@pec.it
  - message4.mbox
  - message5.mbox
  - message6.mbox

Within the root folders files can be organized in subfolders, for example using a breakdown by month. Such organization does not influence the processing and it is not necessary to remove subfolders before uploading. The submission process considers only the `.eml` or `.mbox` files and automatically removes subfolders.

Once the package has been created according to the requirements defined above, you can proceed to compress it in a `.zip` file creating the PEC package. You can upload it and submit documents (see chapter Uploading SIP).

In the event that a file contained in a mailbox folder is neither sent nor received from that mailbox, the E024 validation error accurs during the SIP uploading phase and the package is discarded.

Furthermore, the messages contained in a PEC package must all relate to a single year. In the event that the messages relate to different years, the SIP isn't correct and the E025 validation error accurs during the SIP uploading phase.

6.2. Uploading SIP

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

With ePEC 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".
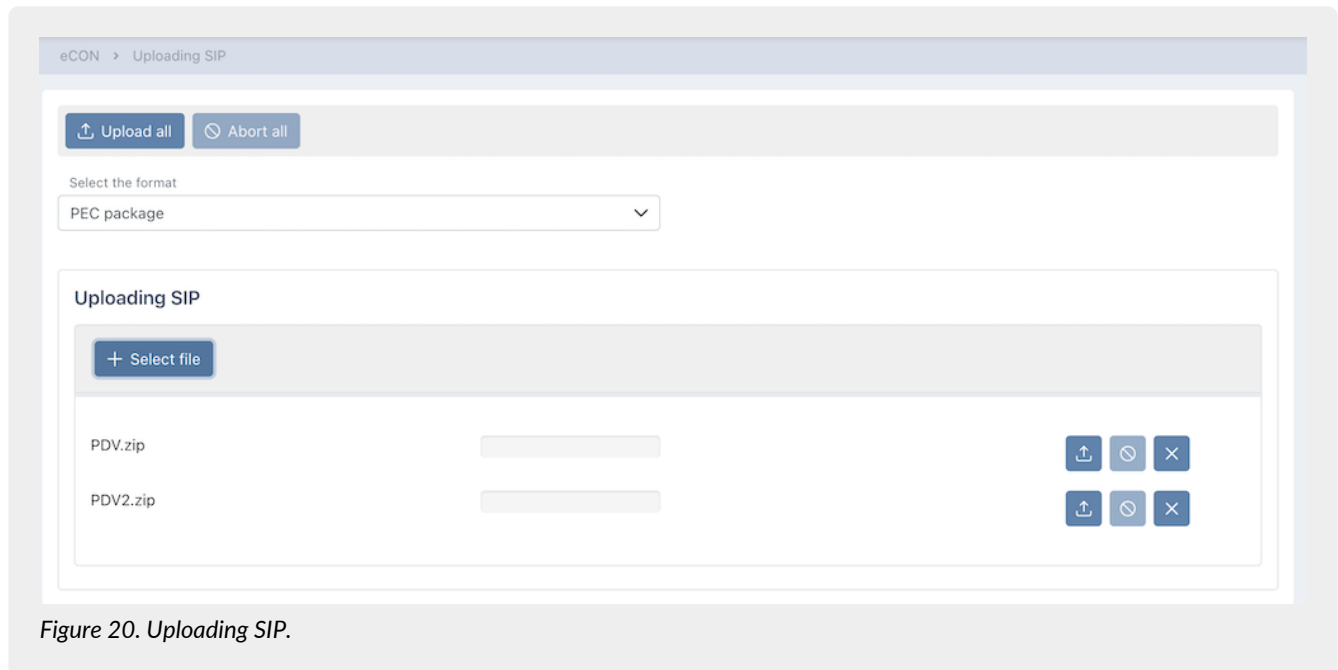
Figure 20. Uploading SIP.

The following table describes the SIP validation formats managed by the system:

Table 3. SIP validation formats

Content	Description
PEC package	.zip file created by compressing a folder with the same name as the PEC address, which contains .eml or .mbox file formats.

Technical specifications of the .zip file format and of index types are described in the chapter [PEC package] or in the manual "UM 20150928 eDoc API User Manual" available on the site www.entaksi.eu.

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 23 di 66
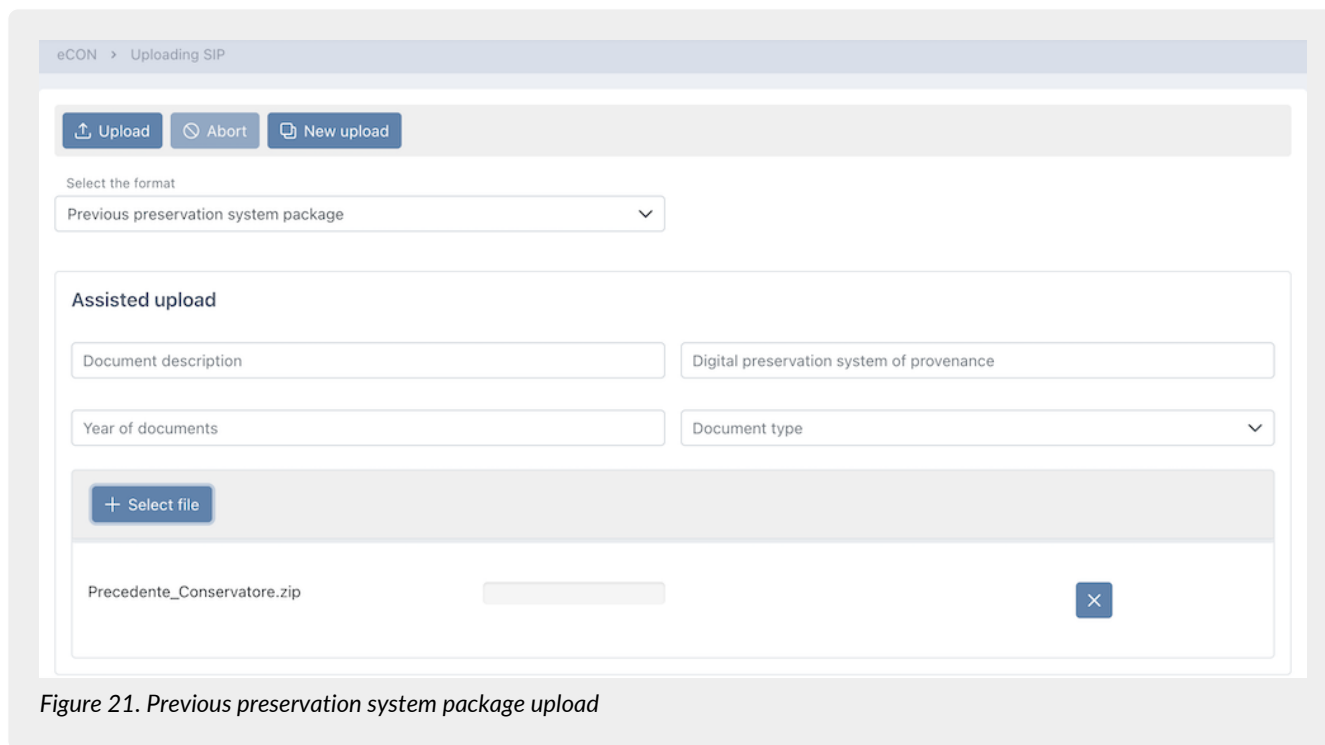
Figure 21. Previous preservation system package upload

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.

6.2.1. 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 4. 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.

Search key	Metadata	Obligatory	Description
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. Nei
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.
Dscription	`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.
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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 25 di 66

ENTAKSISOLUTIONS

Search key	Metadata	Obligatory	Description
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.
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.

Search key	Metadata	Obligatory	Description
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".
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.
Document format	`documento:formato`	Yes	It indicates the document format as defined by Annex 2 of the "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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 27 di 66

Search key	Metadata	Obligatory	Description
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 '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
Document registration	documento:registrazione	No	In the received documents indicate the protocol assigned in the VAT register.
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 protocol/Emergency protocol) - 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 28 di 66

Search key	Metadata	Obligatory	Description
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).
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.
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).

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 29 di 66

Search key	Metadata	Obligatory	Description
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.
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.
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.
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).

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 30 di 66

Search key	Metadata	Obligatory	Description
Recipient name	`destinatario:nome`	Yes	Recipient name (mandatory in case of natural person).
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.
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).
PEC			
PEC direction	`pec:direzione`	Yes	Direction of the email message.
PEC operator	`pec:gestore`	Yes	PEC mailbox manager.
PEC id	`pec:msgid`	Yes	Email message identifier (handler).
PEC message id	`pec:id`	Yes	Email message identifier.

For other SIPs examples please refer to our website www.entaksi.eu.

6.3. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 31 di 66

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.
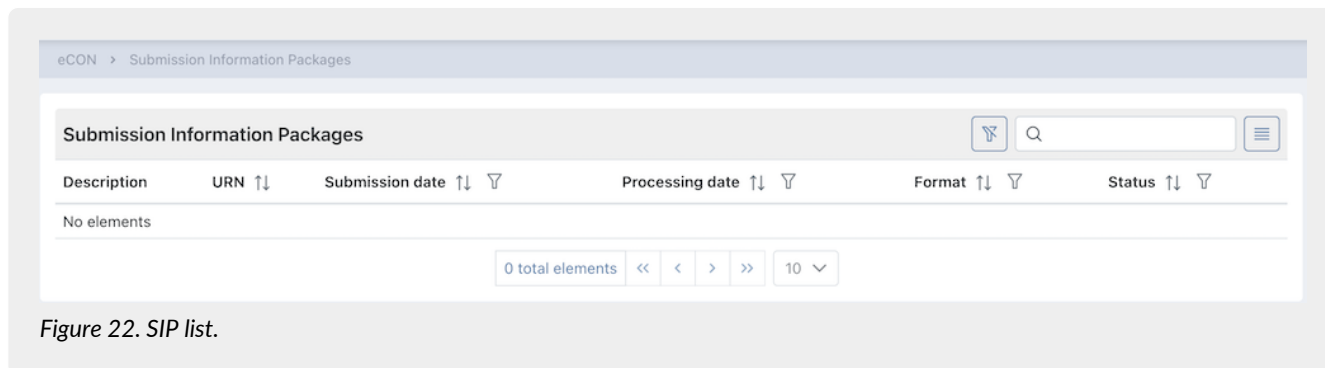

Figure 22. SIP list.

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 status of interest to the user are:

- **Open package**: the package remains in this status from the payment until the end of the month, when the associated management cycle is closed and the package is submitted into the preservation system. Once it is closed and paid, the payment report is issued.
- **Processed**: 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.
- **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.

Other status are mostly automatically generated by the service, and the SIP assumes these values only for few seconds.

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.

Figure 23. 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 you can download the SIP ZIP file and by clicking on the "**Deposit receipt**" button you can download the SIP deposit receipt.

In the section below "**Receipt of submission**", the data relating to the receipt is present.

6.4. 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.
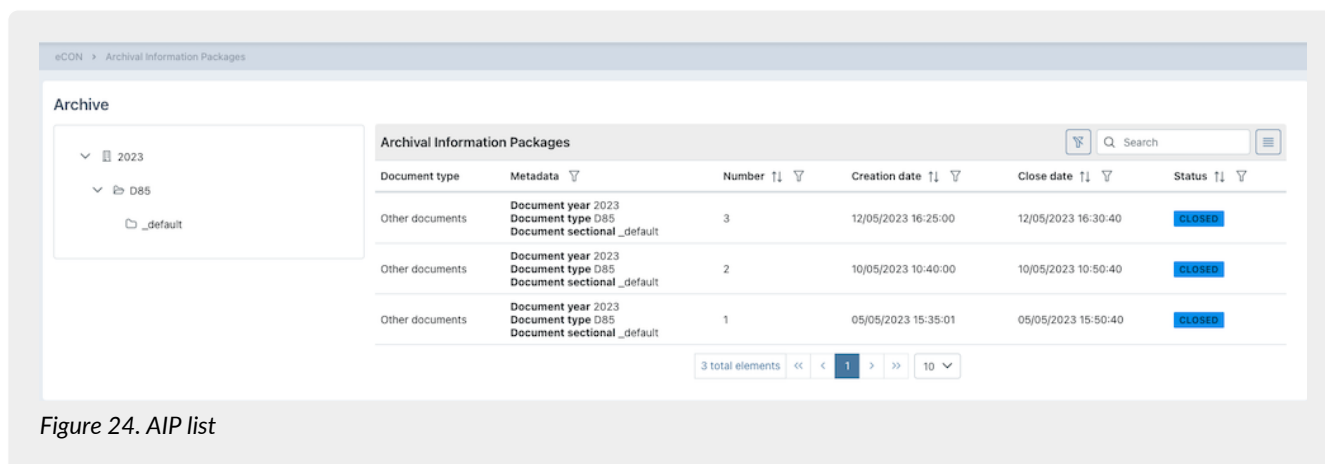

Figure 24. AIP list

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";

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS

Pag. 33 di 66

  ◦ "Closed".

The most important states for the user are:

- **Processed**: 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.

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-T standard. 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 list of documentary units contained therein, divided by number, title and description.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 34 di 66

Figure 25. 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.

6.5. Search and request documents

Figure 26. Search and request documents.

Through "**Search and request documents**", using the predefined searching metadata and setting the value to be assigned to the key ("equal" in the case of text searches, "greater" and "lesser" if looking for a range, such as for dates), it is possible to set up the general search within all the preserved documents for the company and to request DIPs.

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, click on the "**Add criteria**" button: a second section appears where further criteria can be entered.

To enter multiple values for the same search key (where it is possible) just click on the "+" button next to the value box. By clicking on this key a further line is displayed where the new value can be entered.

If you want to delete an entered value because it is not correct, just click on the blue trash icon. Instead, by clicking on the red trash icon all entered predicates of the line are deleted.

To carry out a search, you have to insert a title into the "Search title" box (the one proposes by default is "Search for" plus the current date) and to enter the predicates in the selection criteria.

The "**Save**" button allows you to save the terms without start the search, the "**Find**" button starts the search which is saved in the "Search and document collections" section, the "**Search and Request DIP**" button starts the search and automatically requests a Dissemination Information Packages.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 35 di 66

6.5.1. 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
```
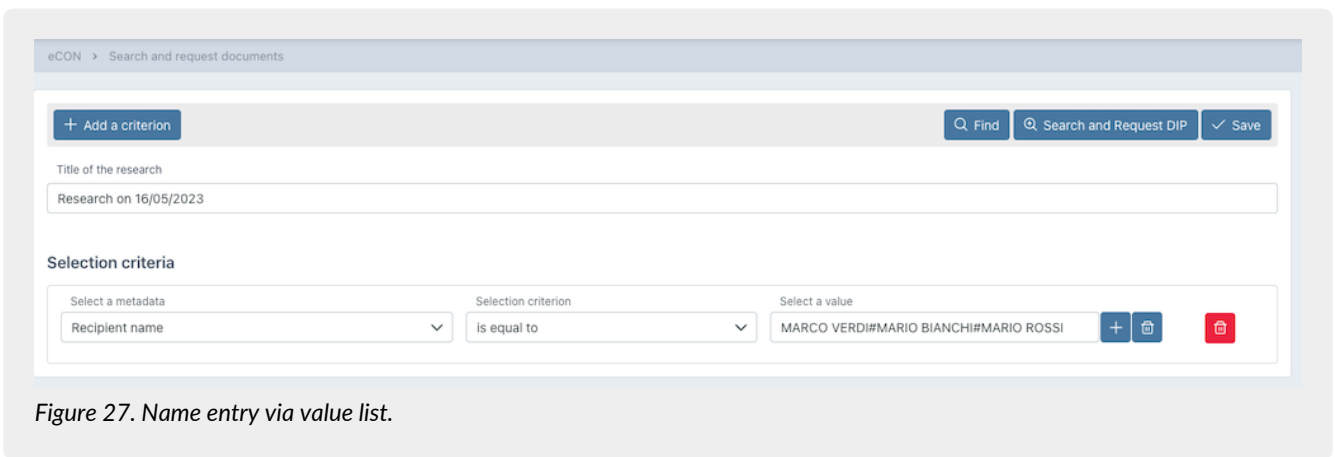

Figure 27. Name entry via value list.

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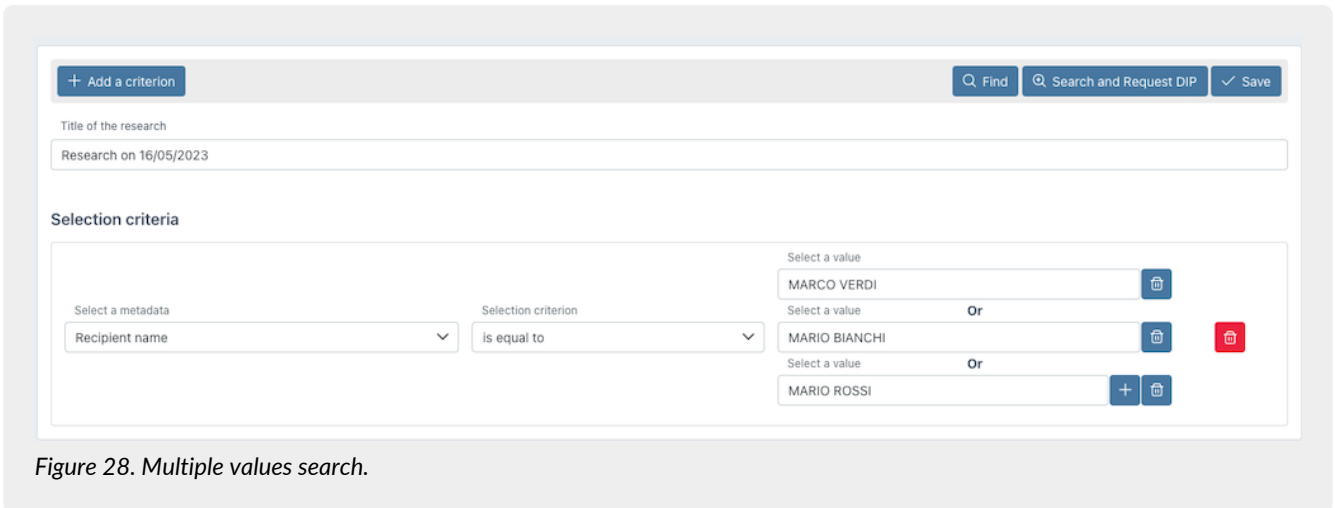

Figure 28. Multiple values search.

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`

Type of criterion	Example list of values
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.

6.5.2. 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.

In the "Search and request documents" function (Search and request documents) **leave all the data selection fields blank** and click on the "Search and Request DIP" button. In this way, the research has all the archived AIPs for the 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.

It is possible to check the search progress looking at the status that appears in the last column of the "Document collection" section: when it is finished it is set on 'DIP ready' by the system. Once the search process is finished, you can select the obtained search in "Document collection", and the following section appears:

Figure 29. Interoperability DIPs creation.

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

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 37 di 66

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.

6.6. Search and document collections

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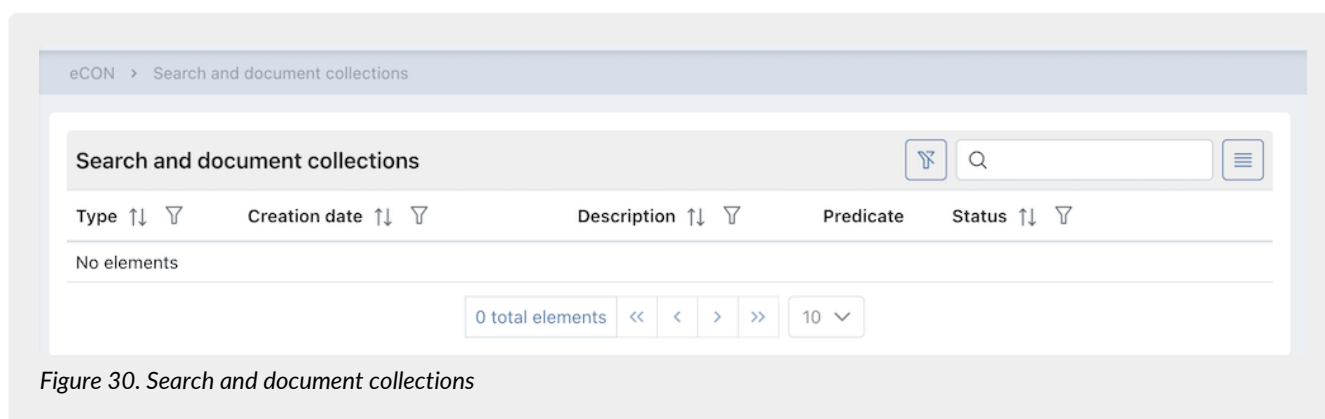

Figure 30. Search and document collections

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)
- **Satus**: it is he 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 delate";
  - "DIP delated";

Among these, the statuses the more interesting are:
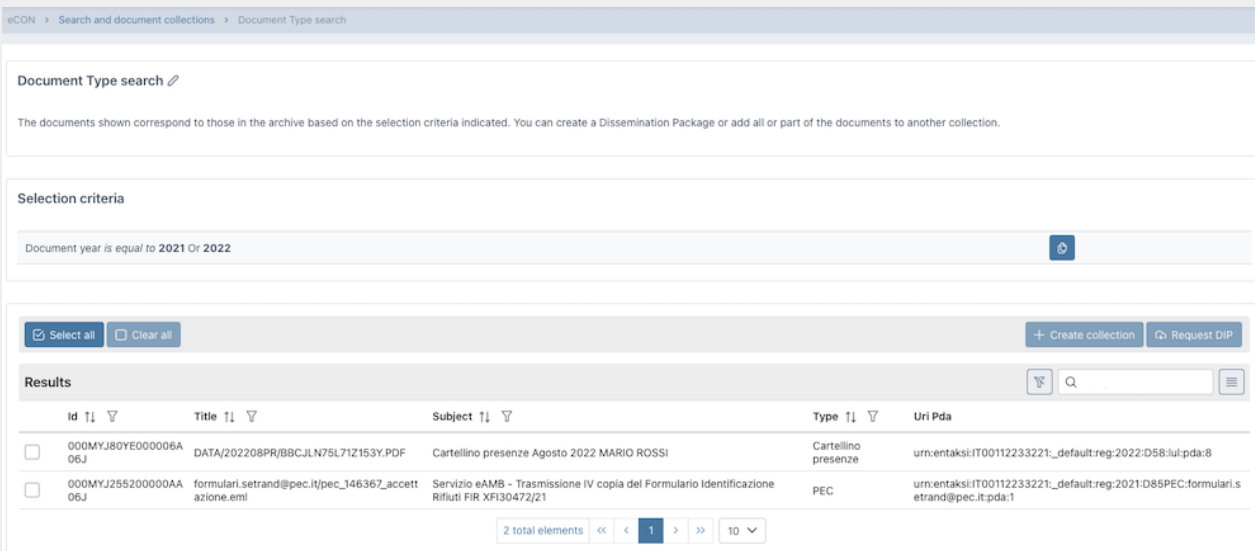
- **Draft**: it means that the search made in Search and request documents has simply been saved.
- **Search in progress**: your requested search is being processed.
- **Results available**: your search is finished. To view the results, just click on the row to enter the detail page.
- **DIP ready**: the required DIP is available.

From this section it is possible:

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 38 di 66

- 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 31. 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.

6.7. DIP list

You can see all the **Dissemination Information Packages (DIP)** request through the functions previously described in the "DIP List" section.

You can search and extract documents stored in the system, for the purpose of consulting them or distributing them to third-parties.

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

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 39 di 66

- a DIP index, digitally signed by the Preservation Service Manager, which also constitutes the confirmation of DIP's distribution;
- the documentary units within the archive, corresponding to the selection criteria;
- 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.
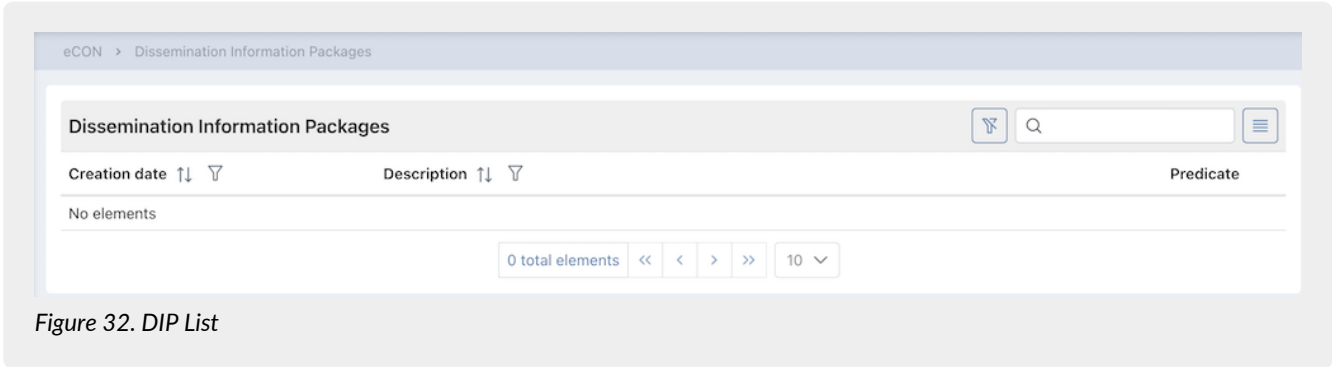
Figure 32. DIP List

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.
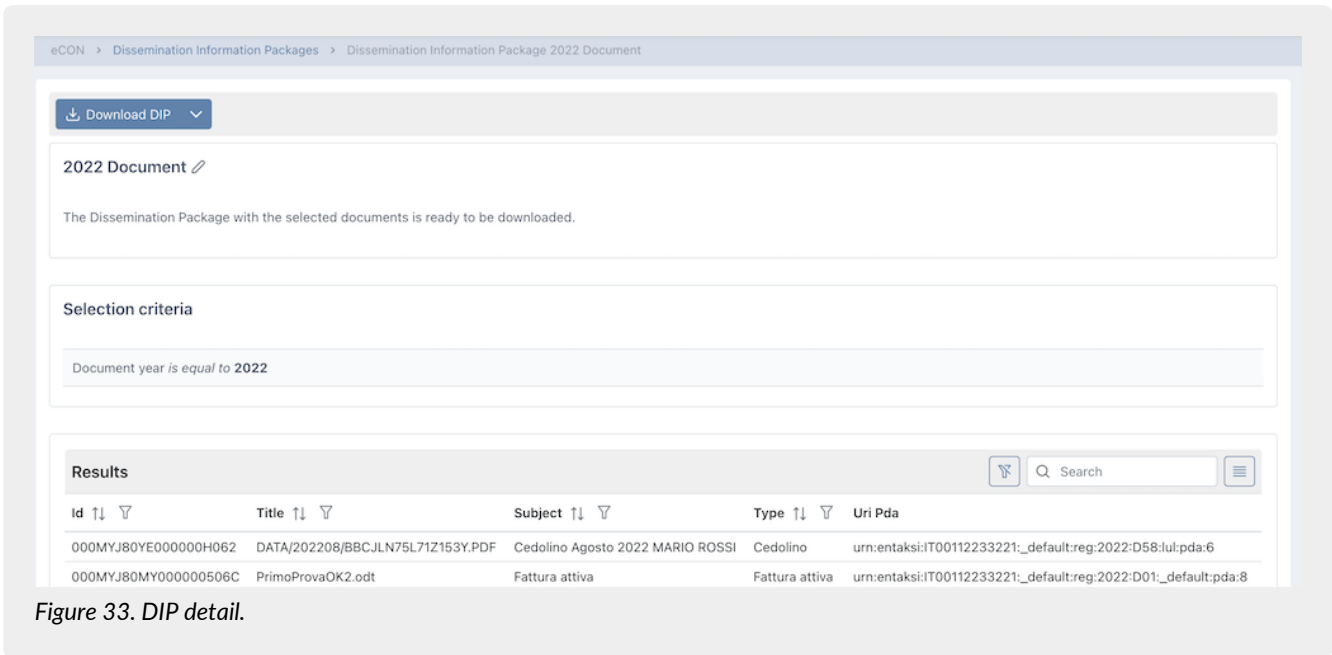
Figure 33. DIP detail.

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.

7. eMAN - Digital preservation manual

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

"In Public Amministration, 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 possesion of suitable legal, archival and IT skills;
c. he can be the responsible of the document management or the coordinator of the documet 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 Preservator, 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 signaures 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.

7.1. 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.
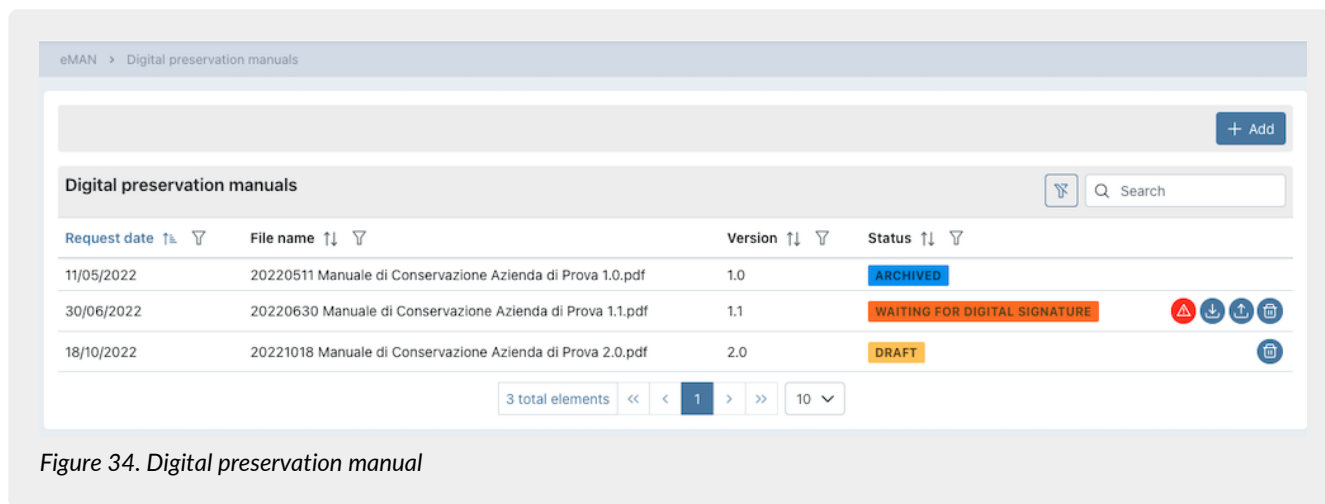
Figure 34. Digital preservation manual

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.
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.
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.

Valore	Descrizione
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.
2. Wait for the manual to be created and the changing of the status from "In Process" to "Waiting for digital signature".
3. When the status changes into "Waiting for digital signature", 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".

7.1.1. 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 state is in "Draft".
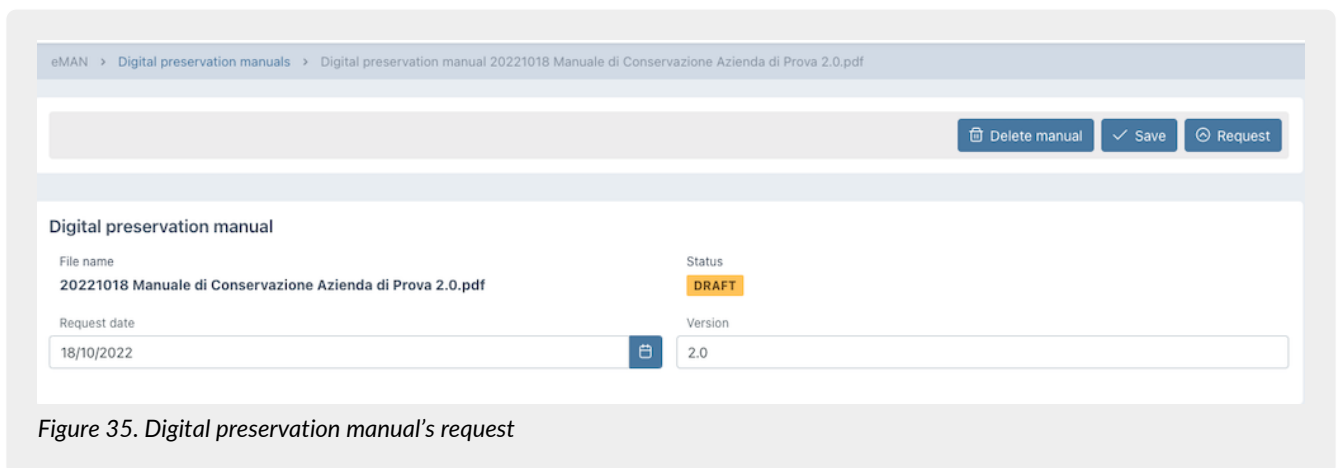
Figure 35. Digital preservation manual's request

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;

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 43 di 66

- "**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".

7.2. 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.

7.2.1. Digital preservation managers

In the **Digital preservation managers** section all the inserted preservation managers are shown in a list.
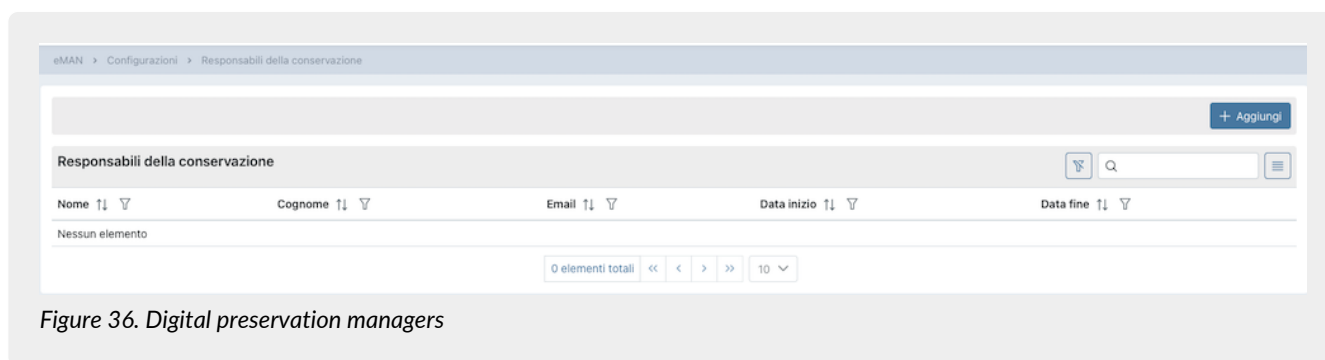
Figure 36. Digital preservation managers

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**".

7.2.2. 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 37. 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 enetred 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".

7.2.3. Company contact person

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

Figure 38. 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.
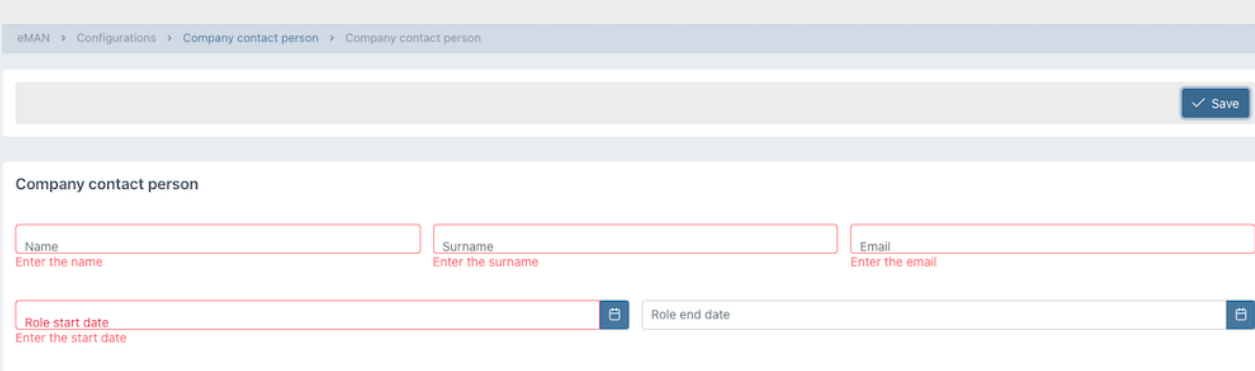
Thanks to the start and the end date of the role, it is possible to have the historian of the company contact people.

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 45 di 66

7.2.4. 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 39. 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.
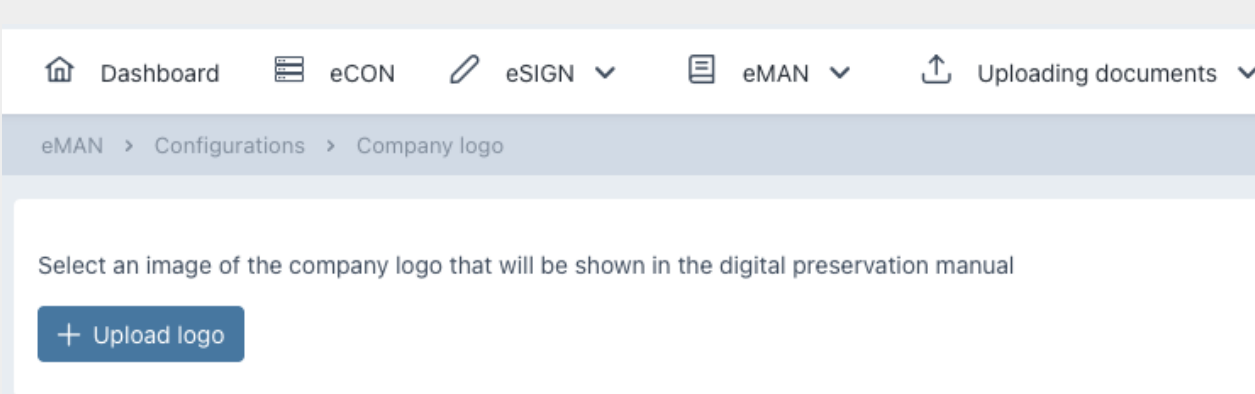
The mandatory items are shown in red and it is not possible to save until they are correctly entered.

All the enetred 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".

7.2.5. 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 40. Inserimento 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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 46 di 66

7.3. Sign and preservation

Once obtained the digital preservation manual, in order to make it legally valid, the digital preservation manager will have to digitally sign it and reload it on the system through the same interface.

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).

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.

8. Terminology

The terminology used in the manual is shown below, divided between the glossary of technical terms and acronyms.

8.1. Glossary

Access

It is an operation that allows you to view IT documents.

Reliability

In reference to a document management or preservation system, it expresses the level of trust that the user places in the system itself. In reference to the IT document it expresses the credibility and accuracy of the representation of acts and facts in it contained.

Computerized document aggregation

Set of IT documents or set of IT files grouped by homogeneous characteristics, concerning the nature and form of the documents or the object or the functions of the entity.

Archive

Set of documents produced or acquired by a public or private entity during the carrying out its business.

IT archive

Archive made up of IT documents, organized in IT documentary aggregations.

Homogeneous Organizational Area

In accordance with the provisions of art. 50 paragraph 4 of the Presidential Decree December 28 2000, n. 445, it is a set of functions and offices identified by the institution in order to manage documents in a manner unitary and coordinated. It represents the official channel for submitting applications and initiating proceedings administrative.

Certification of conformity concerning image copies of an analogue document on IT support

Declaration issued by a notary or another public official authorized thereto that is attached or sworn to the IT document.

Authenticity

Characteristic for which an object must be considered as corresponding to what it was in the original moment of its production. Therefore an object is authentic if, in the course of time or space, it has not undergone any unauthorized changes. Authenticity is assessed on the basis of precise evidence.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 47 di 66

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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 48 di 66

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.

ENTAKSISOLUTIONS

"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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 50 di 66

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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS   Pag. 51 di 66

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) № 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 52 di 66

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.

8.2. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 54 di 66

9. Regulations, reference standards and certifications

In order to guarantee the correct management of ePEC, **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.

9.1. 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.

9.2. 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).

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 55 di 66

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).

9.3. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 56 di 66

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.

UNI 11386:2020

Supporting interoperability in preservation and retrieval of digital objects.

ISO/IEC 14721:2012

"Space data and information transfer systems - Open archival information system (OAIS) - Reference model", open information system reference model for management and long-term preservation of information content.

ISO 15489-1:2016

Information and documentation - Records management - Part 1: Concepts and principles.

ISO 15836-1:2017

Information and documentation - The Dublin Core metadata element set - Part 1: Core elements.

ISO 16363:2012

Space data and information transfer systems - Audit and certification of trustworthy digital repositories.

ISAD(G)

General International Standard Archival Description, standard for the description of archives intended for the recording of documents produced by organizations, people and families.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 57 di 66

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 58 di 66

10. 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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 59 di 66

11. 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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 60 di 66

12. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 61 di 66

13. 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.

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

ENTAKSISOLUTIONS

Pag. 62 di 66

14. 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.

14.1. Service reports

The Customer can report any problems encountered by sending an email to assistenza@entaksi.eu.

Entaksi Solutions provides the customer with software environment, called Redmine, accessible via Internet and dedicated to the management and tracking of service reports (incidents, errors, change requestes, etc).

Through this ticket platform the Customer can insert any request related to technical or economic problems encountered in the use of the eCON service, and stay informed on their management and evolution.

Entaksi can also communicate through the site, through the page status.entaksi.eu, any malfunctions detected on the system.

Back to top.

14.2. 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.

14.3. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 63 di 66

15. Data protection management

Concerning access to data by Entaksi personnel, please refer to the data protection management procedures included into the official Entaksi's documentation.

Besides, regarding access to data by the Customer's personnel, and in particular by personnel who will have access to the web interface for searching, viewing and exhibiting documents, reference will be made to Customer data protection internal procedures.

As part of the processing of personal data related to the performance of the activities provided for in this Manual, Entaksi acts as a Processor, by virtue of by specific legal delegation conferred by the Customer.

The complete set of provisions relating to the processing of personal data is reported in the document "Condizioni Generali del Servizio", chapter "Trattamento dei dati personali".

The complete set of provisions relating to the processing of personal data is reported in the Entaksi website.

Back to top.

15.1. 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.

ENTAKSISOLUTIONS

ISO 9001 | ISO 20000-1 | ISO 22301 | ISO 37001
ISO 27001 | ISO 27017 | ISO 27018 | ISO 27035
ETSI 319 401 | ETSI 319 411-1,2 | ETSI 319 421 | ETSI 119 511

Pag. 64 di 66

16. Service Level Agreement

The service-levels or SLA (Service Level Agreement) are settled on the service agreement.

Back to top.

17. 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.