

POSEIDON

Protection and control of Secured Information by means
of a
privacy enhanced Dashboard

GRANT AGREEMENT NUMBER: 786713
H2020-DS-2016-2017/ DS-08-2017

Deliverable

D2.1 - Use cases analysis and user scenarios

List of Acronyms

AB	Advisory Board
CA	Consortium Agreement
EB	Executive Board
EC	European Commission
GA	General Assembly OR Grant Agreement
L3P	Linked Third Party
PC	Project Coordinator
TL	Technical Leader
USP	Business Service Portal (Unternehmensserviceportal)
WP Work	Package
WPL	Work Package Leader
PED	Privacy Enhanced Dashboard
PII	Personal Identifiable Information
GDPR	General Data Protection Regulation

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786713

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Use cases detailed information

Project Title:	POSEIDON
-----------------------	-----------------

Deliverable Number:	n.a
Grant Agreement number:	786713
Funding Scheme:	HORIZON 2020
Project co-ordinator name:	Francesco Paolo Schiavo – MEF (Italian Ministry of Economy and Finance)
Title of Deliverable:	Use cases detailed information
WP contributing to the Deliverable:	WP2 - Solution design and specifications
Deliverable type	Internal deliverables
Dissemination level	CO - Confidential, only for member of the consortium (including the Commission Services)
Partner(s)/Author(s):	Luca Nicoletti (SOGEI), Juan Echevarria Cuenca, Celia Gilsanz (SAN), Alessandra Bagnato (SOFT), Laurent Goncalves (SOFT), Pierre Vella (MITA), Marica Xuereb (MITA), Danielle Vella (MITA), Barbara Intonti (ACN)

History:			
Ver.	Comments	Date	Author
1.0	First release	31st August, 2018	
1.1	Reopen to insert MITA Use Case and eliminate BRZ Use Case	27 th December, 2017	Accenture, MITA

Project funded by the European Commission Horizon 2020 - The EU Framework Programme for Research and Innovation.

The POSEIDON Consortium consists of:











Logo	Name	Country
	MEF – Ministero dell'Economia e delle Finanze	Italy
	ACN - Accenture S.p.A.	Italy
	PNO – PNO Innovation	Belgium
	ELEX – e-Lex Studio Legale	Italy
	TECN – Fundacion Tecnia Research & Innovation	Spain
	SAN – Ayuntamiento de Santander	Spain
	SOFT - Softeam	France
	UC – Universidade de Coimbra	Portugal
	JIBE – SMARTFEEDZ B.V.	Holland
	MITA – Malta Information Technology Agency	Malta

Table 1: Consortium Partners

TABLE OF CONTENTS

1	Executive Summary	7
2	User Requirements	8
2.1	PED - Privacy Enhanced Dashboard	9
2.1.1	Access to the Web Dashboard	9
2.1.2	Tutorial.....	9
2.1.3	Structure of the Dashboard	10
2.2	Third Parties' interface.....	14
2.2.1	API Gateway Authentication	14
2.2.2	API Gateway	14
2.3	System Administrator's interface	15
2.3.1	Access to the Administrator Dashboard	15
2.3.2	Structure of the Administrator Dashboard.....	15
2.4	PII Dataset Requirements.....	19
2.4.1	Data Types	19
2.4.2	Encrypted PII	20
3	MEF Use case.....	21
3.1	Introduction.....	21
3.2	High-level description	22
3.2.1	NoiPA Consent scenario without PoSeID-on	22
3.3	Enhanced e-Services for Public Officials: Scenario.....	23
3.3.1	User Journey	23
3.4	Number and kind of services to be integrated	26
3.5	Third Parties to be involved.....	27
3.6	Types of Personal Data.....	27
3.7	Data privacy measures	28
3.8	Expected data volume and users	28
4	SAN Use case.....	29
4.1	Introduction.....	29

4.2	High-level description	30
4.2.1	Scenario without PoSeID-on	30
4.3	Municipal Digital Services: Scenario	31
4.3.1	User Journey	32
4.4	Number and kind of services to be integrated	34
4.5	Third Parties to be involved.....	35
4.6	Types of Personal Data.....	35
4.7	Data privacy measures	36
4.8	Expected data volume and users	36
5	MITA Use case	36
5.1	Introduction.....	36
5.2	High-level description	37
5.3	Dashboard for Businesses: Scenario	38
5.3.1	Scenario without Poseidon	38
5.3.2	Scenario with Poseidon	39
5.4	Number and kind of services to be integrated	40
5.5	Third Parties to be involved.....	40
5.6	Types of Personal Data.....	40
5.7	Data privacy measures	40
5.8	Expected data volume and users	40
6	SOFT Use case	41
6.1	Introduction.....	41
6.2	High-level description	41
6.2.1	SVE Privaciz Consent scenario without PoSeID-on	42
6.3	Simplified e-services for French citizens: Scenario.....	43
6.3.1	User Journey	43
6.4	Number and kind of services to be integrated	46
6.5	Third Parties to be involved.....	46
6.6	Types of Personal Data.....	46
6.7	Data privacy measures	46
6.8	Expected data volume and users	46
7	PDA and RMM Applicability on the Use Cases.....	47
7.1	Personal Data Analyzer (PDA)	47
7.2	Risk Management Module (RMM)	49
7.3	User Journey	50
8	Conclusions.....	53

1 Executive Summary

This document has been created to briefly provide more detailed information about the Use Cases/pilots of PoSeID-on project, accordingly with what emerged from the Task 2.1 "Use cases analysis and user scenarios". All the Use Cases will match PoSeID-on technology, that could be developed according to the need of the single pilot. The platform used by each Use Case is the same (PoSeID-on platform), but the different pilots could take advantage of different functionalities, made available by PoSeID-on itself.

The description of the platform starts by exposing the users' needs it must satisfy and the functionalities that have therefore to be granted. A general introduction to these subjects is provided in the second paragraph.

A more detailed view of how the platform performs is then made available through the following four paragraphs, each of them treating a different Use Case. Thanks to these dedicated insights a realistic projection of the PoSeID-on platform working is provided.

For a broader and more specific explanation of the technical and functional requirements, as well as of the architecture of the platform, the Deliverable 2.2 "System Requirements and Architecture" must be considered as the only official source of information on the matter.

The document is an official deliverable.

2 User Requirements

The requirements described in the present chapter will explain the core functionality of the technologies used by users, Third parties and the System Administrator of PoSeID-on. From the users' point of view, the PED needs to have specific requirements, as well as from the point of view of Third parties; the interface through which they are able to access users' data needs to have specific requirements, too. Finally, the interface used by the System Administrator requires specific coverage features. These Requirements will ensure Confidentiality, Integrity and Availability. Along with compliance with the GDPR, traceability of and transparency about the data processed and related permissions will be guaranteed.

As reported in the introduction of this document, only a platform (PoSeID-on platform) will be developed, that each Use Case could use. All the requirements derive from the analysis of the Use Cases described in the following chapters; for the definition of these last, all possible features arose during the definition of each use case are considered, in order to make the requirements useful considering also the future application of PoSeID-on platform, that could be extended to other services not considered in the Use Case pilots of the present document.

2.1 PED - Privacy Enhanced Dashboard

The Web Dashboard is a web application giving Data Subjects access to the PoSeID-on functionality.

2.1.1 Access to the Web Dashboard

Access to the Web Dashboard is managed by national systems compliant with eIDAS (e.g. SPID, @firma, FRANCEconnect). Such systems guarantee users secured access to the digital services of Public Administrations.

These "*electronic Identities*" are released by Identity Providers, accredited bodies that release the credentials (User ID and Password) after verifying the user's identity.

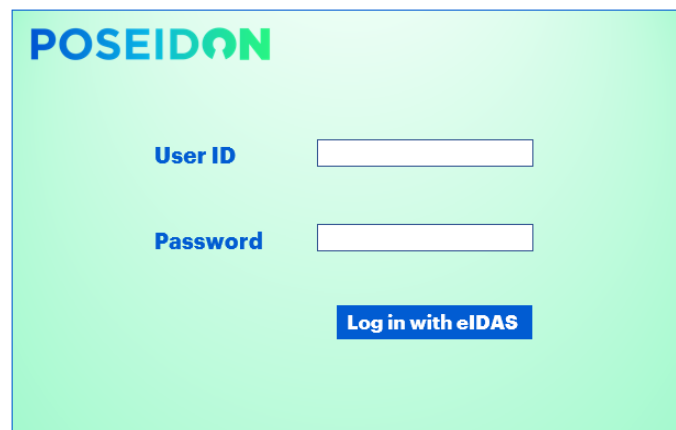


Figure 1: Dashboard access Concept Design

2.1.2 Tutorial

Once logged in, a tutorial will appear on the user's first access to the platform. This tutorial provides an overview of the Dashboard features and shows a number of tasks that the user can perform. The user can watch the tutorial again by going to the Dashboard Homepage and launching it.

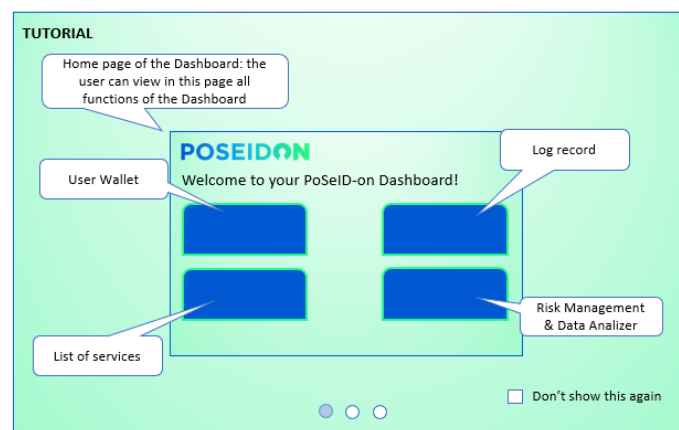


Figure 2: Tutorial Concept Design

2.1.3 Structure of the Dashboard

After watching the tutorial, the User is redirected to the **Dashboard Homepage**, partitioned in 4 functional areas:

- Portfolio Wallet;**
- List of Services;**
- Log Record;**
- Risk Management and Data Analyser.**

Moreover, in each functional area's page, there will be 4 icons: one to go back to the Dashboard Homepage and the remaining 3 to reach the other functional areas' pages.

Be aware that the Structure of the Dashboard and Structure of the Administrator Dashboard may change after more thorough analysis of the use cases or after detailed Functional requirement analysis. According to this point of view, the one presented in this paragraph is a preliminary possible design addressing User requirements.

2.1.3.1 Dashboard Homepage

On the Homepage, the user is able to:

- **Select language** - select the primary language for his/her interface;
- **Have GDPR information** - read a summarized version of the GDPR on a dedicated page;
- **Watch tutorial** - watch the tutorial again;
- **Select a Functional area** - have an overview of all the functional areas available and select one.

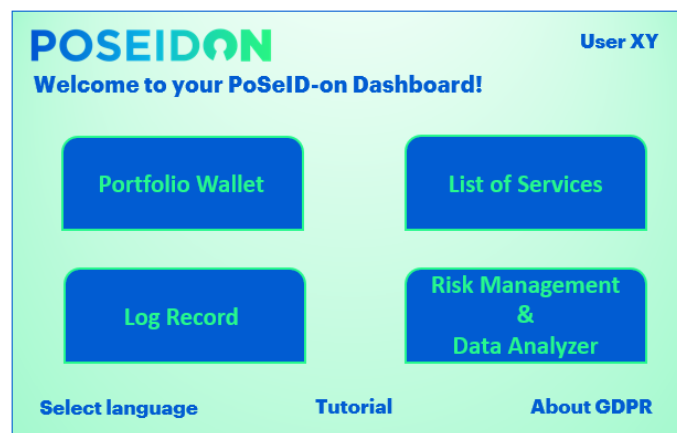


Figure 3: Dashboard Homepage Concept Design

2.1.3.2 Portfolio wallet

The Portfolio Wallet contains the list of the PII related to the user. Thanks to this functional area the user can fulfill the following activities:

- **Visualize PII** - Users may visualize as a list within the summary page on the Dashboard all their PII that could be requested for a service processing. Such a list is continuously updated, since it is pointed to the container where the real data are stored.

- **Visualize ongoing services** - the Users can visualize through a specific section which services are activated and, for each of them:
 - be informed about permissions status: Users are informed about national legal provisions allowing Third Parties to store users' data for a certain amount of time even after permissions have been revoked. Moreover, they can check which Third Party is actually being permitted at that moment;
 - be informed about data status: Users may visualize who is requesting their data, when and for how long, for which purpose and which specific data are sent;
- **Update/modify PII** - Users may update or modify their PII via Dashboard, selecting the specific information to be updated/modified and changing it;
- **Upload PII** - Users may upload – only within a predefined set of accepted filetypes processed by the PoSeID-on system – user-owned data (data that arise from a public authority or that are in their exclusive possession) on the PED, making them available to Third parties;
- **Research services** – Users may research a single service in order to visualize the specific set of PII that the service uses;
- **Select a service** – Users may select the service they need to take advantage of and then make the access permission from the PII point of view;
- **Manage access permissions** - Users see permissions as a list of checkboxes.
 - Give access permissions: whenever they want to add a permission to one or several Third Parties, the Users can simply change the checkbox's status and submit the action. This has two consequences: first, the Third Party is allowed to treat the Users' data; second, the PII will be shared with the Third Party itself in order to have the service provided. Furthermore, a time limit will be set so that Third parties are only able to keep these data for a certain amount of time. In fact, for legal reasons, after a certain period, permission may be automatically revoked, and the users are alerted about this action.
 - Revoke access permissions: the action is specular to the one described above; whenever the Users want to remove a permission, they simply change the checkbox's status and submit the action. After revoking access, the Data Processor will be notified with an API call that access has been revoked. In this case the Third Party is no longer able to process User's PII and it is up to the Data Processor to destroy all copies of this PII. In some cases, national legal obligations require a Third party to store copies of personal data for a certain amount of time; according to this a data Timer for deletion is set and it will start at the moment the user will authorize the Third Party involved to access the PIIs; at the end of the period (Time to deletion) a trigger will automatically revoke the user permission's to the Third Party (see SOFTEAM Use case). If the User decides to revoke the access permission on a specific PII for a service that requests another PII to work, a warning window alerts the User that this further permission shall be revoked, too. Finally, if the PII is uploaded by the Third Party, the User can't revoke the access permission to a Data generated from the Third Party itself.

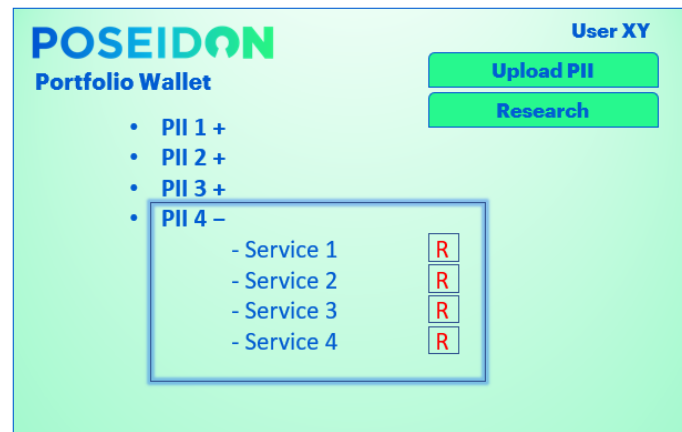


Figure 4: Portfolio Wallet Concept Design

Finally, in order to meet short-term goals and in the case of automate technical interface are middle- and long-term vision from the Partner Application side, it is important to consider other ways to communicate access permission actions from PoSeID-on to Third Parties: an alternative possibility of notification must therefore be considered to notify 'out of the box' all the actions available in this section (i.e. via automatic email).

2.1.3.3 List of Services

In this area of the Dashboard the user can, thanks to a dedicated section:

- **Visualize Services** - visualize the list of available services offered by Third Parties, with a short description and information about data processing; the user will visualize activated services first, then all other services;
- **Visualize/change Services' status** - have an overview about which services are or not activated, besides activate the latter;
- **Activate Services** - decide to activate a specific service, checking the related box, thus allowing the Provider (Third Party) to have access and to process the minimal enabling PII.

Once a service has been activated in this area of the Dashboard, the Users will find that their Portfolio wallet has been updated to show the new Third Party within the list of data processors.



Figure 5: View of the List of Services Concept Design

2.1.3.4 Log Record

The Log Record contain the transactions' history to allow the possibility of reconstructing a series of events. In this section of the Dashboard the user can:

- **Visualize Transactions** - visualize all the transactions related to his/her PII. Information that could be recorded are on the list below:
 - User log in to the Dashboard;
 - User log out;
 - Service activation;
 - Access permission revoke;
 - Third Parties' access to specific PII;
 - Third Parties' data upload;
 - User data upload;
 - ...
- **Visualize date and time of records** - For each transaction recorded, date and time are specified and visualized by the User.

POSEIDON		User XY	
Log Record		Time	Date
Third Party X had access to PII y		13:43	07/06/2017
User #123 had modified PII x		15:02	07/06/2017
.....			
.....			
.....			
.....			
.....			
.....			
.....			
.....			
User #789 had uploaded PII z		16:31	09/12/2017

Figure 6: Log Record overview Concept Design

2.1.3.5 Risk Management and Data Analyser

This component will be used to evaluate and manage a risk score as well as to monitor all personal data flow and usage in addition to related warnings generated, in order to detect and prevent anomalies and misbehaved transactions (data flow and usage). With the Risk Management and Data Analyser section, the user could be aware about data privacy exposure and have a control on his/her personal data. Users are advised on which service to eventually disable in case of anomalies or high exposure of their data to privacy risks. So according to the use of this Module the User can:

- **Visualize PII Risk Score** – have an overview of Risk Level of a specific PII as associated to each service, referring to Confidentiality, Integrity and Availability parameters. Consequently, he/she could decide which services to disable in case of anomalies and high exposure to privacy risks, by simply directing him-/herself to the **List of Services** page;
- **Monitor Update Transactions** – be informed, thanks to a label, each time a transaction is not received and approved by all the interested parties, i.e. whenever a datum update/modification made by the user or the data owner still has to be marked as received by all the other actors whose services relied upon it. This component allows to control personal

data in a transaction, with the aim of discovering all previously non-identified personal data, such as personal data for which there is not data subject authorisation.



Figure 7: Risk Management and Data Analyzer Concept Design

2.2 Third Parties' interface

The API Gateway is the access point for Data Processors to communicate with PoSeID-on. This interface allows Data Processor to have a direct connection with the repository that hold Users' PII, only for information the Users gave access permission.

2.2.1 API Gateway Authentication

Third Party are authorized to access PoSeID-on only thanks to a certificate-based authentication process. In fact, this is a clear authentication method since neither a user ID nor a password are required once the certificate validity has been confirmed.

2.2.2 API Gateway

Through the API Gateway, the Data Processor can request the PII values from one Data Subject. The actions that this interface allows the Third Parties to carry out are the following:

- **Access Users' PII** - Third Parties can access all the PII users have shared with them;
- **Request Data Subset** - to request a minimal dataset for each specific service. Third Parties could ask for a minimal enabling dataset, needed to provide a specific service, by only selecting the interested PII checkbox;
- **Be notified about permission status** - Third parties are informed whenever access permissions are given to them or revoked. If revoked, they are informed about the legal consequences of keep on utilizing the data. This solution meets both the RTBF (Right to be forgotten) of users and non-invasiveness for Third Parties;
- **Be informed about Data Changes** – to be informed about every change of the PII values made by the User;
- **Validate Data changes** – it could be possible simply selecting the 'Accept change' checkbox related to a modified PII to give approval if the User decides to make a change on a specific PII stored in PoSeID-on, in order to make it effective. This is to emphasize that a transaction needs to be approved by all the interested parties;

- **Update PII** - to update data whenever they are modified/updated by users;
- **Upload PII** – Authorized Third parties may upload data/documents they emitted/that reside with them. Certain PII will be stored temporarily on the PoSeID-on platform, while in transit between Data Processors.

All these actions need to be automated; as automate technical interface are middle- and long-term vision, in order to meet short-term goals, it is important to consider other ways to communicate access permission actions from PoSeID-on to Third Parties: an alternative possibility of notification must therefore be considered to notify 'out of the box' all the actions available in this section (i.e. via automatic email).

2.3 System Administrator's interface

The System Administrator must ensure the PoSeID-on correct functionality, which is possible thanks to a dedicated dashboard.

2.3.1 Access to the Administrator Dashboard

The Administrator Dashboard is the front page of the Administrator interface. It provides convenient shortcuts for common management tasks, some server information, etc. The access to the Dashboard is provided by a multifactor authentication system, that expects an OTP in addition to a User ID and a Password.

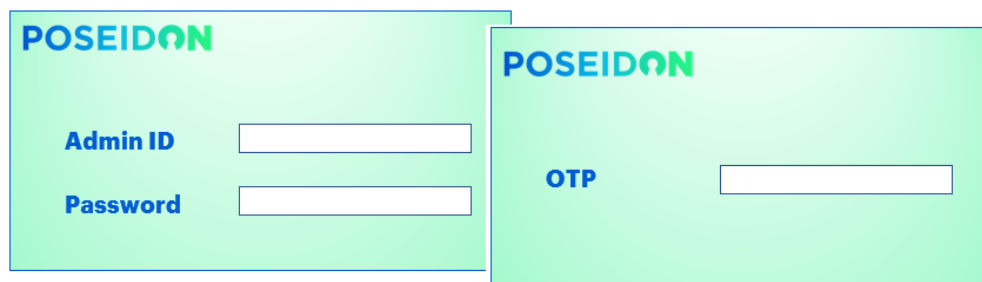


Figure 8: Administrator Access to PoSeID-on Dashboard Concept Design

2.3.2 Structure of the Administrator Dashboard

Once logged in, the Administrator is redirected to the **Dashboard Homepage**, partitioned in 4 functional areas:

- Global PoSeID-on Geography;**
- System event log;**
- Ticket Management;**
- Gateway Certificate Management.**

Be aware that the Structure of the Dashboard and Structure of the Administrator Dashboard may change after more thorough analysis of the use cases or after detailed Functional requirement analysis. According to this point of view, the one presented in these paragraphs is a preliminary possible design addressing User requirements.

2.3.2.1 Dashboard Homepage

Once logged in, after watching a tutorial, the user is redirected to the **Dashboard Homepage**. On the home page, the Administrator is able to:

- **Select language** - select the primary language for his/her interface;
- **Select a Functional area** - have an overview of all the functional areas available and select the appropriate ones.



Figure 9: Administrator Dashboard Homepage Concept Design

2.3.2.2 Global PoSeID-on Geography

This section hosts a global overview of the PoSeID-on System as a whole. The Administrator through this area can **visualize**:

- PoSeID-on growth: a section that shows with a chart the growth of PoSeID-on in terms of users, services and data flow;
- The platform status: in this section there could be indicated platform real time information as the number of users that join PoSeID-on technology, the number of services integrated, the amount of data flow shared, etc....;
- The platform capability: memory available and in use. Besides, more information and statistics are given in a synthetic view (e.g., best working capacity related to a specific memory usage; history of previous time spans and of any potentially occurred criticalities; which Use Case needs more dedicated resources; ...).

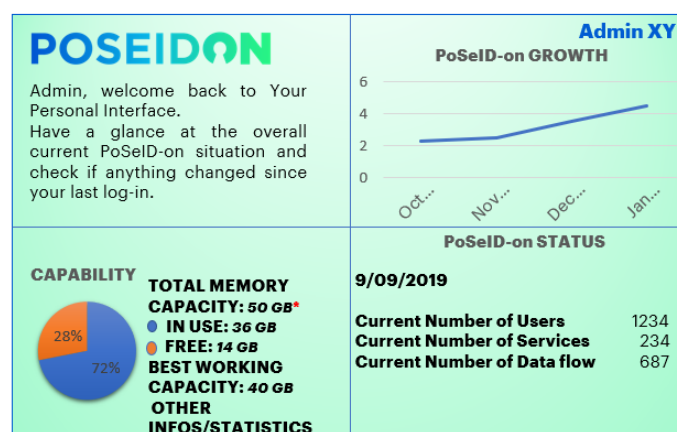


Figure 10: Global PoSeID-on geography overview Concept Design

These functions will be provided to the System Administrator by specific administrative tools - closely related to the technology that will be used to build the platform - in order to monitor network status: the Dashboard should be the collector of all these graphic interfaces.

2.3.2.3 System event log

In order to efficiently control the status of any occurring transactions, a specific section is provided. Hence the System Administrator can:

- **Visualize Transactions** - visualize a list of all the transactions recorded in PoSeID-on:
 - The effort of exposed API;
 - Communication between PED and PII repository;
 - Communication between API and PII repository;
 - User log in to the Dashboard;
 - User log out;
 - Service activation;
 - Access permission revoke;
 - Third Parties' access to specific PII;
 - Third Parties' data upload;
 - User data upload;
 - Etc.....
- **Visualize Transactions' status** - visualize the working functionality status for each log. Specifically, they could be indicated as:
 - Success - when their functioning is as expected;
 - Failure - when some adverse situations impede the correct functionality; in this scenario, the possibility to open a related ticket is given, having the latter available in the specific section.

Please note that the Administrator could decide to open an incident ticket even if no failure is reported whenever he/she might suspect that any unclear transaction is happening.

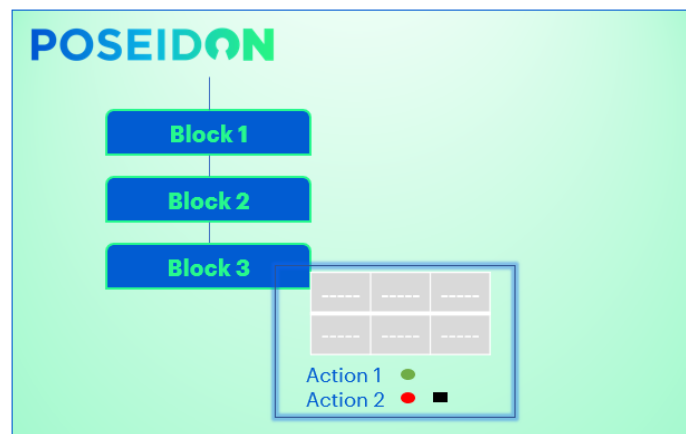


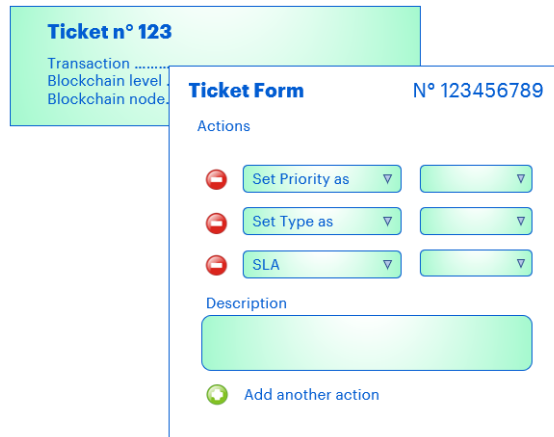
Figure 11: System event log Concept Design

2.3.2.4 Ticket Management

This specific section is critical to manage/investigate every anomaly occurring during the PoSeID-on working. Thanks to this area of the Dashboard, the Administrator can:

- **Open a ticket** - write up a ticket according to the request previously sent in the System event log section, completing the following actions:
 - assign an identification number;
 - assign it to a person in charge;

- set the priority;
- write a short description;
- set a type (e.g., incident, failure);
- define the SLA;
- choose to add other options.
- **Visualize Ticket status** - be aware about the status of a ticket (e.g. pending; resolved; in process) or mark it if he/she is the owner of this process;
- **Delegate a Ticket** - designate any member of the Consortium (mandatory with the Administrator role) to specifically be in charge of the Ticket management and keep a communication channel with the Resolution Responsible about any update, issue or progress;
- **Track changes** - monitor any changes made to the ticket and inform interested parties of this changes;
- **Resolve a Ticket** - mark a processed ticket as resolved and then close it. Please note that will kept the ten latest tickets, then they will be gradually moved to a history section, always available to be consulted;
- **Visualize resolution Time** - visualize the Time spent processing the ticket from its opening to its resolution.



The image shows a user interface for ticket management. On the left, a light blue box titled "Ticket n° 123" contains the text "Transaction", "Blockchain level", and "Blockchain node ..". To the right, a white box titled "Ticket Form" with the ID "N° 123456789" contains an "Actions" section with three items: "Set Priority as" with a dropdown arrow, "Set Type as" with a dropdown arrow, and "SLA" with a dropdown arrow. Below these is a "Description" section with a large text input field. At the bottom of the form is a green circular icon with a plus sign and the text "Add another action".

Figure 12: Ticket Management Concept Design

2.3.2.5 Gateway Certificate Management

In order to effectively tackle any misbehavior by Third Parties or by Users and to ensure the compliance to GDPR, the Administrator can:

- **Check valid certificates** - be aware about which certificates are expired, marked as not acceptable anymore or about to expire, thanks to a control light with three statuses: red – expired; yellow – about to expire (e.g. within two weeks); green - OK;
- **Send a reminder** - remind the Third Parties with expired/about to expire certificates to renew them, in order to keep on acceding the PoSeID-on System, by selecting the voice "Notice";
- **Black list** - enlist those Third Parties' or malicious users' certificates that must no longer be accepted as access authorization systems to PoSeID-on. This could be the case of a Third Party convicted for violating any GDPR requirement or of the user, faking his/her identity trying to overcome the Segregation of Duties and to access unauthorized functions.

There will be two dedicated lists, each for "Users" and "Third Parties". The Administrator will be able to view them separately by selecting them from a top-fixed bar.

The image shows a web interface for the POSEIDON Gateway Certificate Management. It features a header with the POSEIDON logo and two tabs: 'Third Party' and 'User'. Below the tabs is a table with four columns: 'Certificate', 'Type', 'Status', and an unlabeled column. The table contains four rows of data. The first row has a blue circle in the Status column and the word 'Notice' in the unlabeled column. The second row has a red circle in the Status column. The third row has a blue circle in the Status column and the word 'Notice' in the unlabeled column. The fourth row has a green circle in the Status column.

Certificate	Type	Status	
			Notice
			Notice

Figure 13: Gateway Certificate Management Concept Design

2.4 PII Dataset Requirements

The initial data set of PII types serviced by PoSeID-on shown below covers the pilot use cases. The platform should be designed in a way it can address other PII types in the short-, middle-, long- term. Therefore, the Dataset is meant to reach the right trade-off between the minimal enabling dataset for each Use case and a reasonable extended dataset that may enable Third parties to offer additional services. Therefore, certain PII will be stored temporarily on the PoSeID-on platform, while in transit between Data Processors.

2.4.1 Data Types

The dataset will include the following classes of data types:

- **Personal user's data** - data that identify uniquely a person, relating to his/her digital account (e.g.: First name, Last name, email address, etc...);
- **Minimal enabling dataset for the Use case** - a minimal set of data that could be request from the Third Party, relating to the Use Cases described in the chapters above (e.g.: car plate, Bank details, etc...);
- **Data requested for new services** - data that could be required by a Third party to offer a new service the user may advantage of in the future (e.g.: Medical/Handicap certificates, Monthly pay slip, etc...).

The table below shows a classification of the data defined for each use case and those that will be integrated in order for PoSeID-on to be open to other services in the future:

Personal data	Minimal enabling dataset for the Use case	Data requested for new services
Title	Postal address	University curriculum and official diploma
First name	Social security number	Equivalent Financial Situation Index Form
Last name	National ID number	Medical/Handicap certificates
	Unique identification feature of a person	School/University enrolment certificate
Email address	Bank details	Monthly pay slip
Phone number	Employment contract	Marital status

Date of birth	Salary Information	Law enforcement/Armed forces membership
Municipal census	License plate number	
Sex	Residence Address (Postal address): - Street name - Street number - Post code - City - Country	
Birth Place	Living Address: - Street name - Street number - Post code - City - Country	
	Available data from attributes from certificates	

Table 2: Classification of PII datasets

2.4.2 Encrypted PII

PII must be encrypted to guarantee Confidentiality, Integrity and Availability of data. Encryption ensures that only the right people can read the information.

A key point to underline is that both the data entered by the Data Subject and by the Data Processor must be encrypted as long as they are stored within PoSeID-on.

The method and procedure of encryption will be clarified in a specific technical document.

3 MEF Use case

3.1 Introduction

The General Administration, Personnel and Services Department (DAG) of the Italian Ministry of Economy and Finance (MEF) is in charge of the management of payroll functions for approximately 2.1 million Italian public sector employees. Such service is provided through a unique payroll function, NoiPA – which annually manages more than €51 billion in payments.

NoiPA is a portal created to manage administrative and economic data of central and peripheral Public Administration employees. Therefore, NoiPA has a big experience in personal data management and it could be very close to PoSeID-on project because this platform aims to collect user's given authorizations of sharing personal information, that are stored in the platform itself.

NoiPA's main services are:

- Processing of legal-economic data, including fiscal and social security ones;
- Processing and matching of presence/absence data;
- Management of collected data, production and distribution of the monthly pay slip and communication of information linked to its content.

Current NoiPA users can be divided into the following three categories:

- Administrative employees of the entities managed by the system;
- Public Administrations that have adhered to NoiPA (public administrations that are or not are in the State's financial statement, public entities, local entities, schools, national healthcare, etc.);
- Partners that collaborate and interact for different reasons and in different ways with the NoiPA system.

NoiPA is very interested in PoSeID-on project and on investing in the growing market of Personal Information Management. At the moment it doesn't support the eID and blockchain integration, that PoSeID-on technology could offer. NoiPA's client, as selected for the pilot, could access to the PoSeID-

on platform with their eIDAS account and give permission to NoiPA of managing their personal information through PoSeID-on itself.

NoiPA will select end-users from his customers portfolio to participate to this pilot. This will allow a variety of users from different fields to test our PoSeID-on solution.

3.2 High-level description

The NoiPA pilot will be based on its services. It will imply the customization of this services to integrate PoSeID-on solution to provide the users with a single platform for personal data management, as well as to support NoiPA to be compliant with the GDPR.

Through PoSeID-on solution NoiPA's users will access to the available services; the access to the PoSeID-on platform (PED – Privacy Enhanced Dashboard) will be allowed upon access authentication using "SPID" – the Italian current service acting as the trusted eIDAS Access Management Authority. The PED (Privacy Enhanced Dashboard) will empower the user in having a concise, transparent, intelligible and easy access to, as well as tracking, control and management of their PII (Personal Identifiable Information). The pilot's objective is to allow the user to modify his personal data and to take advantage of different services enabling the processing of his/her personal data.

Through the PED and the data that flow in it, the user can access the NoiPA services allowing the processing of a subset of his/her personal data (i.e. only name, surname and address).

The user will be able to make conscious decisions about who can process his/her own data, by enabling, restricting or revoking permissions in accordance to the GDPR data minimization principle, as well as to be alerted in case of privacy exposure through the Risk management module.

3.2.1 NoiPA Consent scenario without PoSeID-on

NoiPA, as explained in the introduction of this chapter, is the portal created to manage administrative and economic data of central and peripheral Public Administration employees.

Currently, NoiPA offers three kinds of services that will constitute the use case pilot.

Before integration with PoSeID-on, these services were:

- a) Residence address and
- b) IBAN upload/update via NoiPA based application:
 1. the user logs into NoiPA;
 2. he/she opens the web-page (application form) dedicated to the functionality of editing data related to residence address / bank account;
 3. once modified, data are rectified and stored on the NoiPA database.
- c) Insurance policy subscription provided by Reale Mutua Assicurazioni:
 1. the user logs into NoiPA;
 2. the insurance policy service is showed in his/her personal web-interface;
 3. once the user selects such an option, he/she is redirected to the Reale Mutua website, where an insurance estimate is calculated. At this point, the user manually inserts the minimal enabling dataset for this specific service: first name, last name, SSN, IBAN, etc.
 4. a code is generated as the estimate is completed;
 5. back on NoiPA the user inserts the previous code in order to complete the procedure. Redirected to the Reale Mutua website, there is the user validation as being a NoiPA member;
 6. once the previous step is fulfilled, the user can accept/refuse the estimate on the Reale Mutua website and, if the latter is the case, subscribe the policy.

3.3 Enhanced e-Services for Public Officials: Scenario

The Use case foresees the integration of the NoiPA portal with PoSeID-on, a system based on blockchain technology and smart contracts that ensures confidentiality, integrity and availability of personal data as well as traceability of PII transactions.

After logging into PoSeID-on through eIDAS, users will be able to visualize a list of services available to them, both internal and external, and easily manage their PII related to the activated services, a great step towards the data minimization principle. Users will be able to interrupt a service at any time, denying further access to their personal data by the Third Parties involved.

Basically, users will be able to centrally manage their personal information and take advantage of services via the PoSeID-on Dashboard.

With a single change, they are able to rectify any information for all Third parties that had permission to access it and store it, given that these changes will synch immediately with Third Parties' repositories.

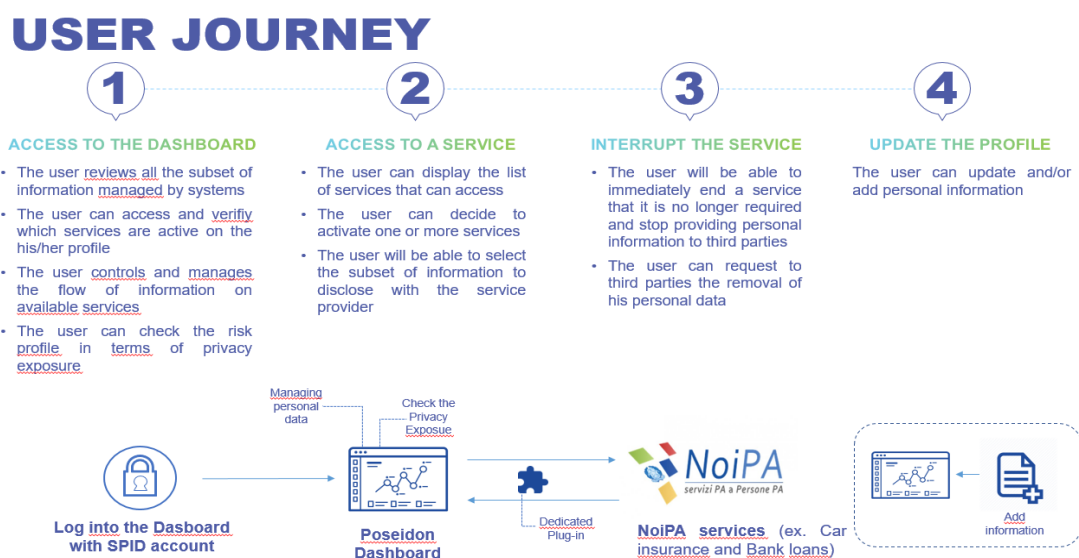


Figure 14: MEF Use case - User journey

3.3.1 User Journey

The pilot will validate different actions involving customer personal information:

1. Access to the PED:

The PED (Privacy Enhanced Dashboard) displays the whole subset of personal information globally managed by any system. The user can check which services he has activated as well as the extent of personal information shared/involved. The user can oversee and manage the flow of such information related to the available/activated services. Also, he/she can view the privacy exposure of the PII loaded on PoSeID-on (a remarkable added value from a personal information security point of view).

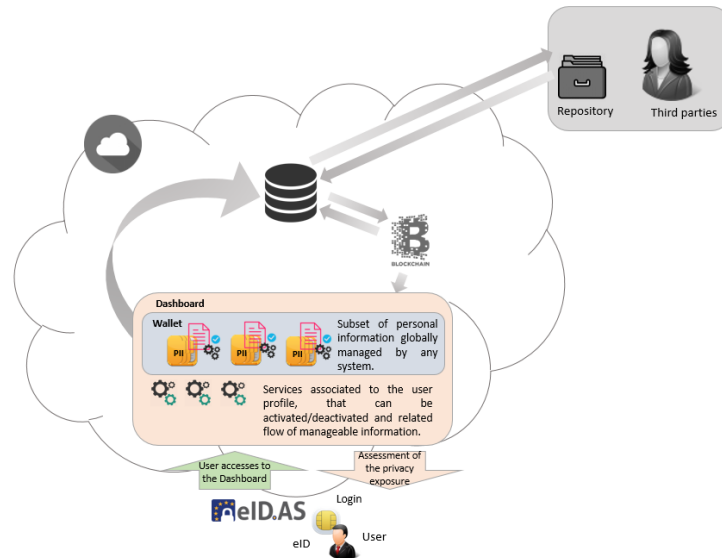


Figure 15: MEF Use case - Access to the PED

2. Use a service:

Once on the PED, the user sees a list of available services; he/she is able to take advantage of these services, simply by selecting them from that list. For each selected service, the user chooses the information to be shared with the Third Party in charge of providing the service.

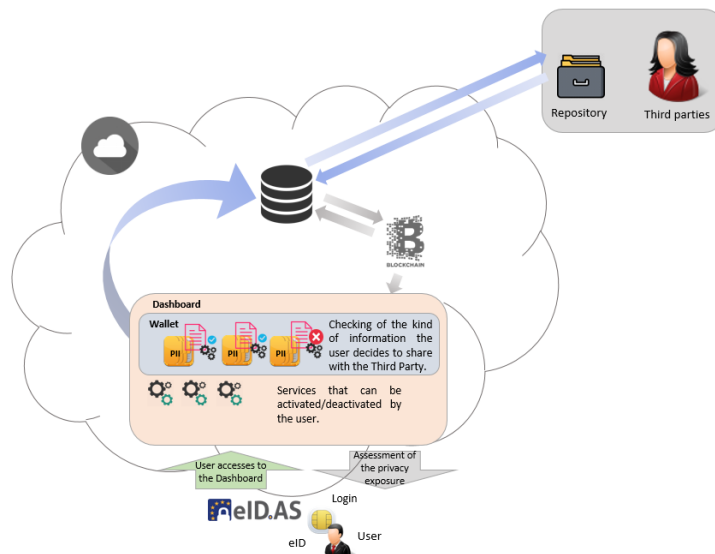


Figure 16: MEF Use case – Use a service

3. Interrupt a service:

At any time, the user can interrupt a service, simply unchecking the related checkbox, automatically denying further access to the service provider. The Third Party receives a data deletion request from the user as well as a reminder of its legal accountability for the unauthorized use of PII.

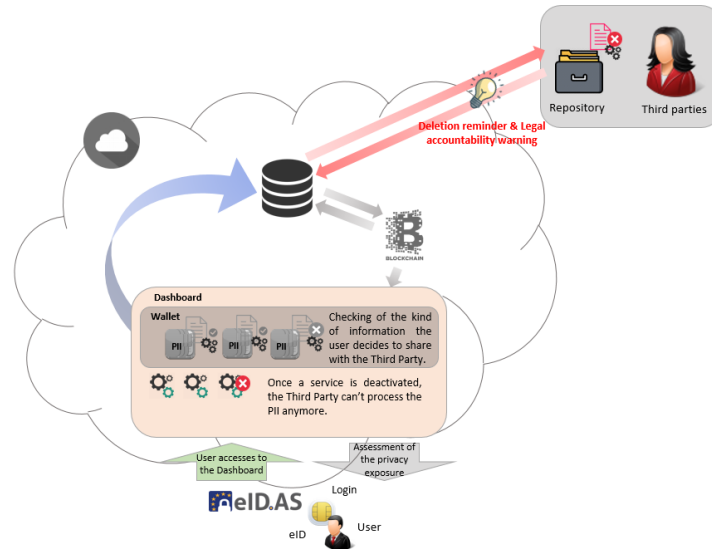


Figure 17: MEF Use case - Interrupt a service

4. Update profile:

Another advanced feature that PoSeID-on makes available to the user is centralized information about data updating/adding. Whenever the user needs to rectify or add any information, changes will be immediately synced, via the PED, with all the repositories of Third parties involved. This option is a big step towards compliance with GDPR requirements about the "Rights of the data subject".

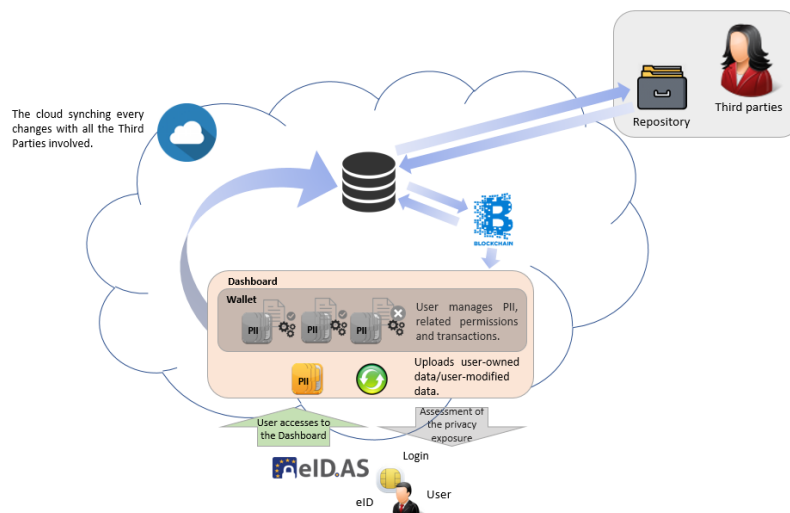


Figure 18: MEF Use case - Update profile

3.4 Number and kind of services to be integrated

Three services – all dashboard-structured - will be integrated: two internal and one external. Following preliminary possible design may change after more thorough analysis of the use cases during project development phase.

Internal ones will allow users to:

- Change their permanent residence address;
- Change their International Bank Account Number (IBAN).

Logging into NoiPA, users will be able to modify information a) and b) giving consent to their processing, and activating the service, directly to the PoSeID-on PED. With a single change, this information will be rectified to all the Third Parties that had permission to process it and store it. Thanks to this mechanism, any change will be greatly simplified, better structured and secured.

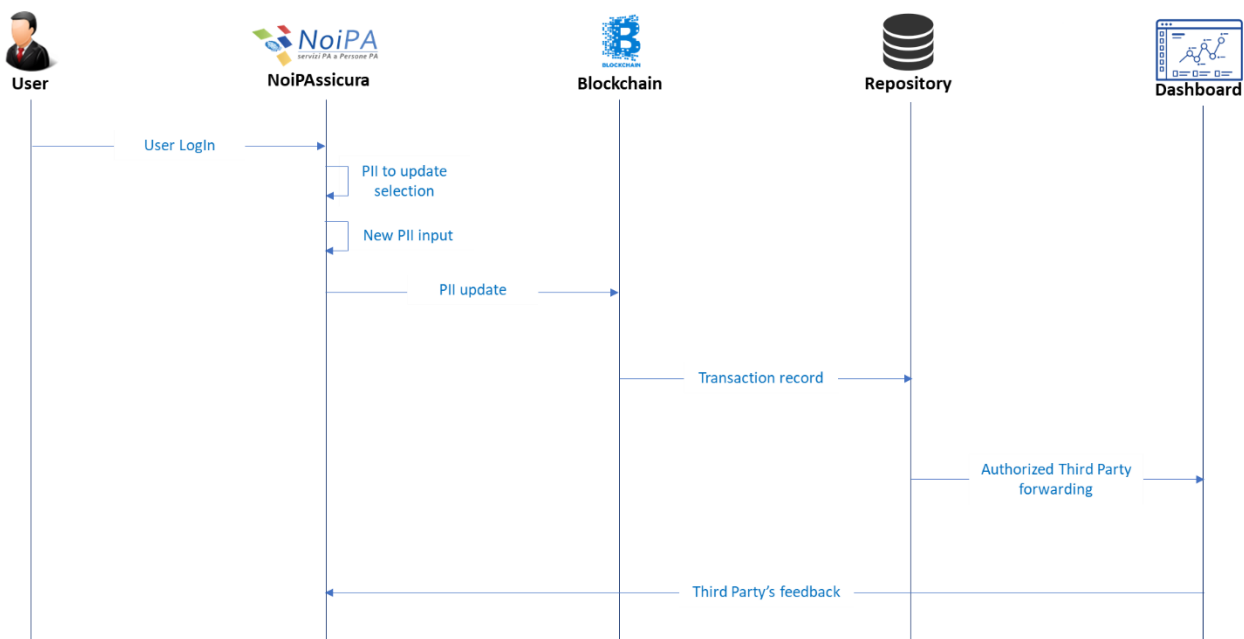


Figure 19: MEF Use case - Internal services

The external one, is a self-service activated for the benefit of the NoiPA affiliated. It enables to purchase a motor insurance (cars/motorbikes/boats) directly from the Reale Mutua Assicurazioni Insurance Company, via the NoiPA dashboard.

The user logs into his/her personal page and checks available services. In this scenario, the user will be asked to give permission to Reale Mutua Insurance Company to access the data required to estimate the user's insurance policy. Once calculated, the user may decline the offer or accept it and subscribe the conclusive policy - thus paying in instalments from his/her own income with no interest ratio.

Two scenarios arise:

- In the first scenario, a trigger is activated to have the data access permission expire within a defined time span, to allow the user to make a cost estimate;
- If the policy is subscribed, the Third Party is allowed - through a further permission - to process user's data compatibly with GDPR requirements. The user may revoke access permissions at any time.

Please note that users' data will be all managed through the PoSeID-on system.
More in detail:

- If the user owns such data, he/she will upload (and then, if needed, modify) them and this will be traced via PED (Privacy Enhanced Dashboard);
- If the data are generated by a Public Entity/Authority (e.g. a working contract), they will be automatically synched with the PoSeID-on repository in cloud.

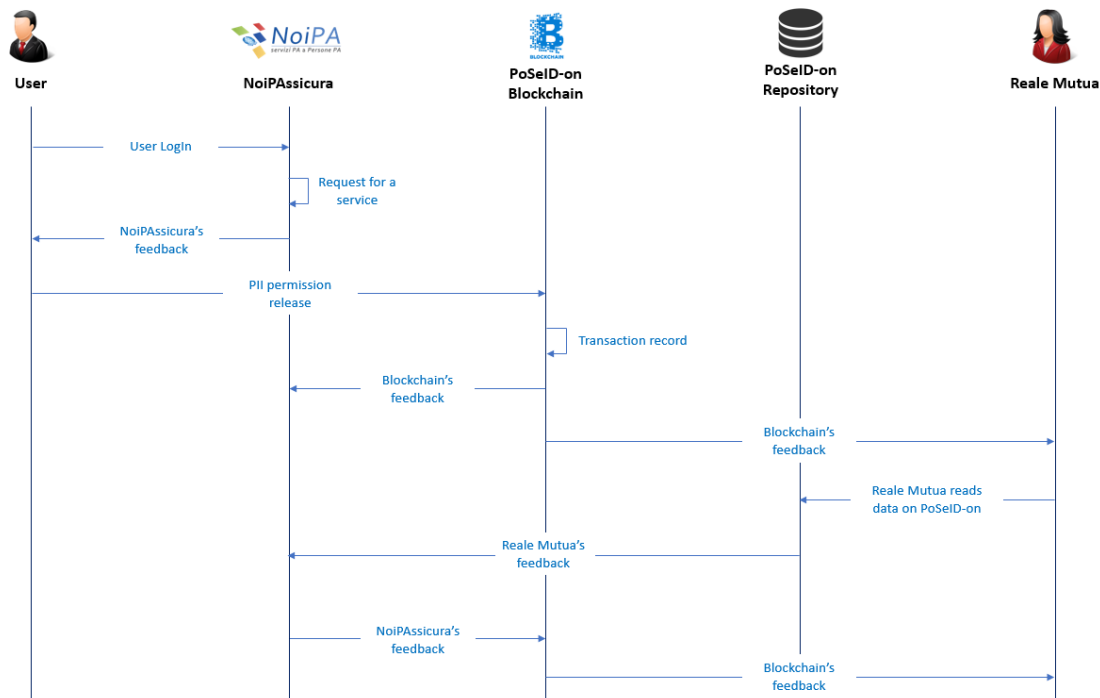


Figure 20: MEF Use case - External service

3.5 Third Parties to be involved

The only Third Party involved will be Reale Mutua Assicurazioni, Italy's biggest mutual insurer. It provides insurance cover to around three and a half million Policyholders and in 2014 reported premium income of over 3,7 billion.

3.6 Types of Personal Data

Below is a list of Personal Data that could be used for this pilot:

- Title
- First name
- Last name
- Email address
- Residence address (postal address)
 - Street name
 - Street number
 - Post code
 - City

- Country
- Social security number
- Bank details
- Employment contract and salary information
- License plate number

3.7 Data privacy measures

This pilot will use fake data, as a way to be compliant with the GDPR requirements. Indeed, this technique will allow to process data during the whole pilot – that can be easily considered as an experimental project – avoiding all the relevant risks for and potential damage to any prospective user, as a result of mistakes, data breaches, malignant attacks, etc.

Furthermore, to improve the overall security, data minimization and encryption techniques, as well as digital signature, will be employed.

3.8 Expected data volume and users

A sample of about 10 users is expected to be involved in the pilot deployment.

4 SAN Use case

4.1 Introduction

The city of Santander is the capital of the Cantabria region in the north of Spain and has a current population of approximately 173,000 inhabitants it extends over 33 square kilometers. Santander City Council / Ayuntamiento de Santander is a Public Administration at local level in charge of the government of the following municipal services: mobility, transport, street and public lighting, cultural and touristic services, e-administration, waste management, irrigation, water management, social care among others.

Santander City has been characterized by its eagerness to provide a more efficient city management closer to the citizens using Information and Communication Technologies. Innovation has a fundamental role in increasing the dynamism of the economic activity potentiating the model of Santander as integral Smart City and favoring an open innovation ecosystem in which both entrepreneurs and local businesses participate. The modernization of public administration, oriented towards the citizens is also part of this plan.

Driven by administrative laws, currently Santander is involved in a digitalized process of all administrative procedures. Santander is working on the creation of confidence in the use of online procedures, showing the benefits to eliminate long queues of people and the waste of time and paper in order to transform citizen interaction with public administration, from the long queues of people to the e-Administration. Currently, citizens can access to more than 60 online procedures through the website of Santander City Council with the support of Munitecnia.

Munitecnia is a company that has eXperta platform as its main product. It is a company specialized in knowledge management solutions, electronic administration and attention to multi-channel citizen in the field of public administration; a solution based on online knowledge management services that implements advanced modules, such as: Virtual Window, Citizens' Directory, Citizen Services Offices or Tele-Assisted Activity Management.

Munitecnia's goal is to lead initiatives of Modernization and Electronic Government, within the so-called "Intelligent Administration", through its eXperta platform. eXperta platform are a group of online services for the collection and distribution of Knowledge cells, it enables the use of techniques for the accumulation of experience and its application based on management and resolution patterns based on the detected case studies. The aim of this platform is achieve an increase in productivity and efficiency in the processes of Electronic Government, Citizen Service and administrative modernization in general.

Use case by Santander City Council, will be run to validate PoSeID-on solution in a scenario involving e-administration services, evaluating PoSeID-on from both the data subject's (citizens using e-administration platform) and the data controller's (the public entity) perspectives.

From the personal data protection perspective, Santander City Council, as responsible of the citizens' personal data, should ensure compliance with the GDPR. In this way, citizens will take the control of their personal data which will make them have more confidence on the e-administration. As a consequence, a significant increase in the use of the online procedures by citizens is expected.

Santander City Council, as a public administration, handles a set of personal data of special sensitivity. Although the basic data that is collected is established by law, there are a series of additional data that speed up the operation of the procedures offered by the municipal services. Citizens must be protected and informed about the use of these data. In addition to this, there are municipal companies that provide various services such as sports activities that are not legally regulated as the basic services of a public administration. In this case, since they deal with PII to carry out their activity, the municipality considers it important to provide the same level of protection in all their services. On the other hand, the City Council is promoting greater citizen participation through participatory budgets. This participation entails the collection of IIPs also beyond normal activities. For all these reasons, these use cases are considered interesting and necessary not only for those currently being carried out but also to serve as a model for those to be developed in the immediate future.

4.2 High-level description

As described in the paragraph above, use case by Santander City Council, will validate PoSeID-on solution in a scenario involving e-administration services, evaluating PoSeID-on from both the data subject's (citizens using e-administration platform) and the data controller's (the public entity) perspectives.

Santander's pilot will be based on its services. It will imply the customization of this services to integrate PoSeID-on solution to provide the users with a single platform for personal data management, as well as to support Santander to be compliant with the GDPR.

Through PoSeID-on solution users will access to the available services; the access to the PoSeID-on platform (PED – Privacy Enhanced Dashboard) will be allowed by a strong authentication process upon the @firma platform, compliant with eIDAS regulation.

The PED (Privacy Enhanced Dashboard) will allow the users to control and manage their PII (Personal Identifiable Information) by only one platform.

The pilot's objective is to allow the user to modify his/her personal data and to take advantage of different services enabling the processing of his/her personal data.

Through the PED and the data that flow in it, the user can access the eXperta services allowing the processing of a subset of his/her personal data (i.e. first name, last name, living address).

The user will be able to make conscious decisions about who can process his/her own data, by enabling, restricting or revoking permissions in accordance to the GDPR data minimization principle, as well as to be alerted in case of privacy exposure through the Risk management module.

4.2.1 Scenario without PoSeID-on

Of the approximately 60 services currently integrated into the eXperta platform, the ones that will be included to meet PoSeID-on project are the following:

- a) Resident card application for parking time limitation: an internal service that let resident citizens located on the so-called blue lanes may apply for a badge, which will entitle them to park properly on any blue lane in their area of residence, except those classified as "high rotation areas". Through this procedure, the Citizen may apply for or renew this badge;
- b) Application for possession of dangerous animals: an internal service that let citizens requesting the permit to keep any animal classified as potentially dangerous (usually dogs) which,

according to law, requires the prior obtaining of an administrative license, which will be granted by the City Council of the applicant's municipality of residence. Through this process, the citizen can apply for the relevant license;

- c) General application form: an internal service that allow citizens fill a generic application for registration. Citizens can make use of it if they cannot find the specific procedure they wish to carry out or if this procedure is not available in the catalogue of procedures of the Town Hall;

That will constitute the internal services of this Use Case pilot.

At the moment, in order to take advantage of these services the user:

1. Logs into the eXperta platform;
2. Opens the web-page related to the request for the specific application;
3. Fills in the form dedicated entering all the needed personal information (i.e. name, surname, living address, license plate, ...);
4. Submit the request, after completed the form in all respects;
5. The request is processed and then accepted or declined.

Also, another Service will be introduced in the present Use Case as external, in order to meet this project. The ones concern the sports department of the Santander City Council, the Municipal Institute of Sports – Instituto Municipal de Deportes (IMD).

Carrying out the enrolment to the Municipal Institute of Sports, without PoSeID-on support, citizens need to do the following actions:

1. Open the Municipal Institute of Sports web-page and enter in the section dedicated to information about the enrolment;
2. Select the link related to the enrolment;
3. Fill in the related form with the personal information requested (i.e. first name, last name, ...);
4. Submits the request for the enrolment;
5. The request is processed and accepted or declined, depending on the validity of the data expected (i.e. name, telephone, living address, ...).

4.3 Municipal Digital Services: Scenario

The Use Case will meet the PoSeID-on project by the integration of Santander services with this new platform that ensure confidentiality, integrity and availability of personal data, as well as traceability of PII transactions.

After logging into PoSeID-on platform the user will be able to visualize all the service available, select the ones He/She wants to gain, select the subset of personal information requested by the service, as well as decide to interrupt the service He/She does no longer to take advantage or updates/adds personal information.

Basically, users will be able to centrally manage their personal information and take advantage of services via the PoSeID-on Dashboard. With a single change, they are able to rectify any information for all municipality services and any potential Third parties that had permission to access it and store it, given that these changes will synch immediately with all municipality services and any potential Third Parties' repositories.

USER JOURNEY

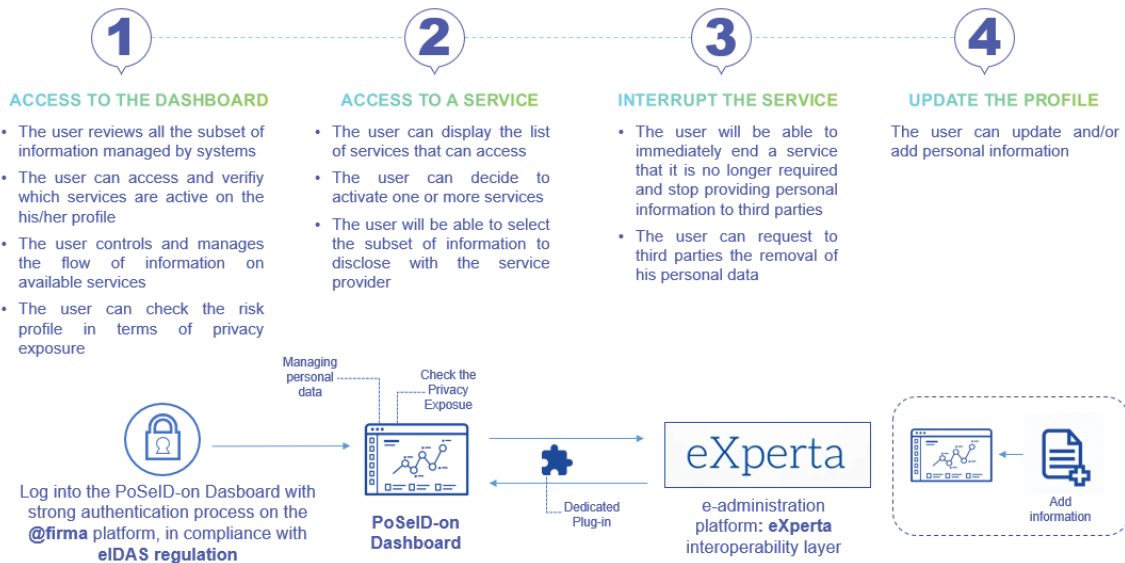


Figure 21: SANTANDER Use case - User journey

4.3.1 User Journey

The pilot will validate different actions involving customer personal information:

a) Access to the Dashboard:

The user could access to the PoSeID-on Dashboard with a strong authentication process by @firma, an eIDAS compliant platform. By the Dashboard the user is able to have a view of the list of all His/Her PII shared and globally managed by any system. The user could also verify which services are active on His/Her profile as well as control and manage the flow of information on available services. The user could finally check the risk profile in terms of privacy exposure.

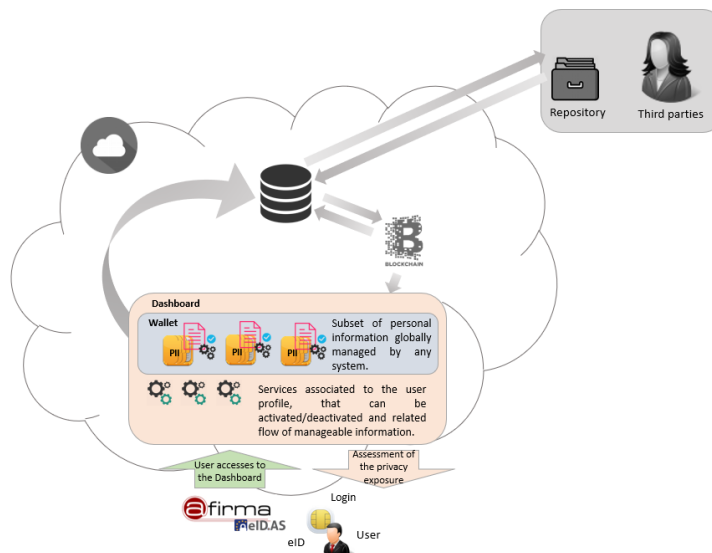


Figure 22: SAN Use Case – Access to the Dashboard

b) Access to a service:

Ones on the PoSeID-on Dashboard the User could display the list of all the services available and decide the one (or more than one) He/She wants to activate, simply by selecting it. The user will be able to select the subset of PII to share with the service provider.

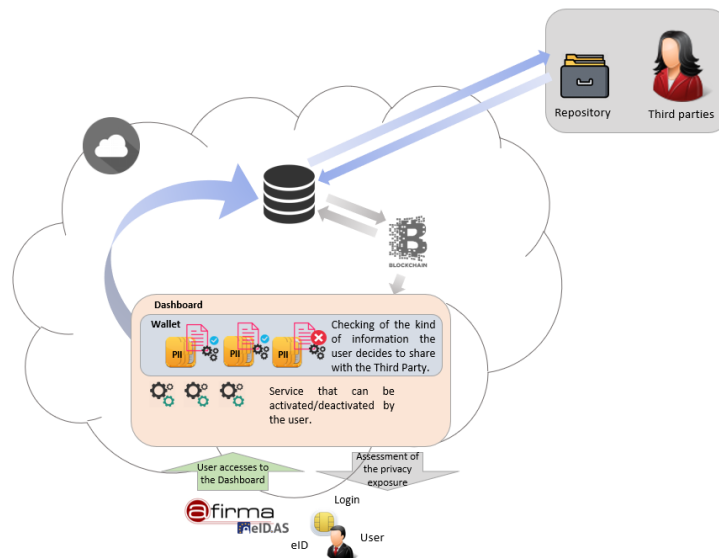


Figure 23: SAN Use Case - Access to a Service

c) Interrupt the Service:

At any time, the User could be able to interrupt a service that is no longer required by simply turning down the related checkbox and decide to do not providing personal information. According to this decision, the user could request the removal of his personal data. Any potential service involved receives a data deletion request from the user as well as a reminder of its legal accountability for the unauthorized use of PII.

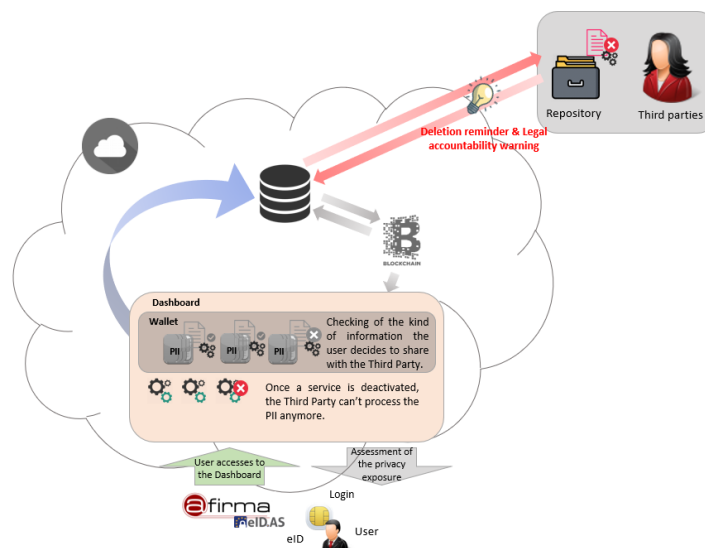


Figure 24: SAN Use Case - Interrupt the Service

d) Update the Profile:

The user will be able to update/upload His/Her PII. The centralized information updating/adding permit via the PoSeID-o Dashboard, to immediately synchronizing the changes with all the repositories involved, whenever the user needs to rectify or add any information.

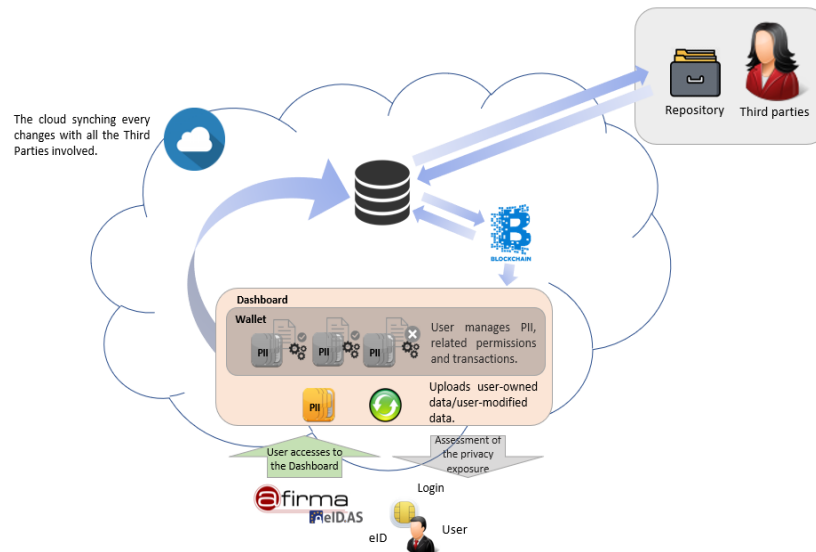


Figure 25: SAN Use Case - Update the Profile

4.4 Number and kind of services to be integrated

Two kinds of services – all dashboard-structured - will be integrated: municipality services and a municipality linked entity one. The Santander services provided for the pilot will be customized to integrate PoSeID-on in order to help user to share their PII through a single platform for personal data management, as well as to make Santander GDPR compliant.

Through the PoSeID-on platform, for each service, the User will be able to:

- Select the interested service from a list displayed on the Dashboard for activation;
- Have a view of all the PIIs requested for the Service activation;
- Upload the specific PIIs needed for the service, that aren't stored in PoSeID-on yet;
- Select all the PII requested for taking advantage of the service, in order to share these PIIs with the service provider.

Basically, the user logs into his/her personal PoSeID-on page and checks available services, depending on His/Her interest. In this scenario, the user will be asked to give permission to the to access the data required, according to permit the User to gain the Service. Once the User had shared the requested PIIs, the latter will have to process the request for the service usage and give a feedback to the User that could be the granting of the request or its decline.

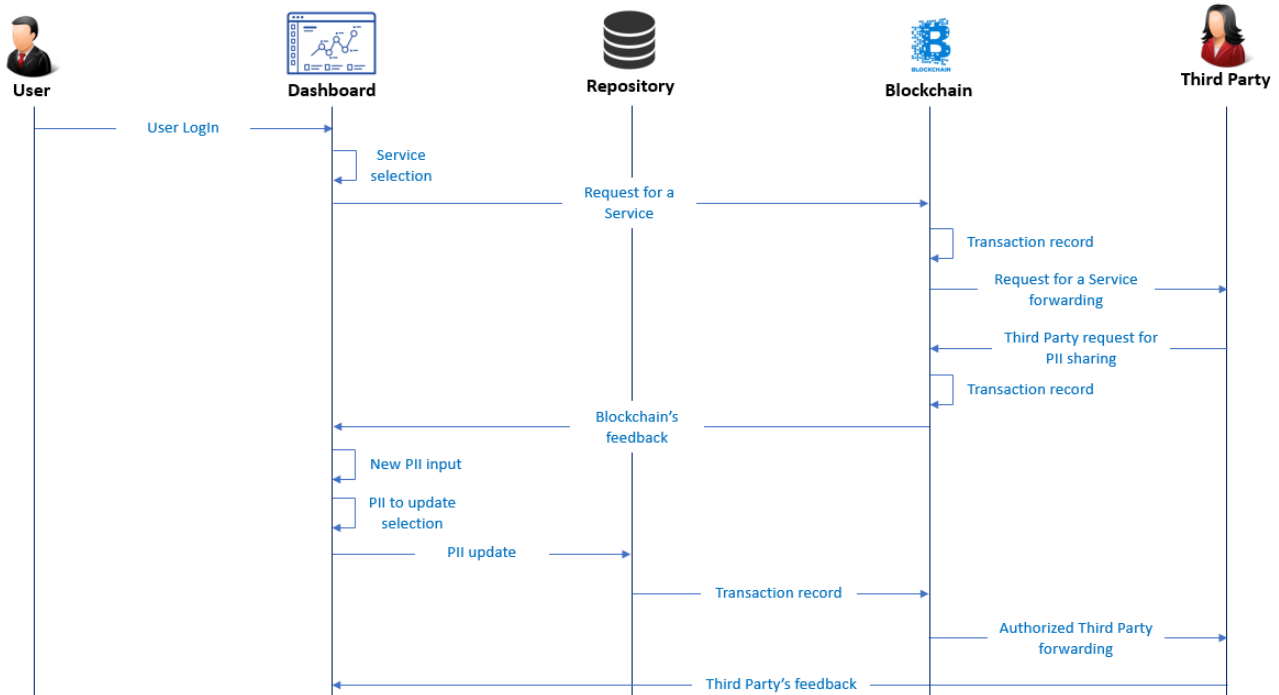


Figure 26: SAN Use Case - Flow of actions

4.5 Third Parties to be involved

Santander's use case foresees no Third Parties. There are external providers involved but they are only product and maintenance providers. The contract signed with the providers includes their obligations as data processors in their daily activities supporting municipality. They can only access PIIs stored in their e-administration platform eXperta for that purpose.

4.6 Types of Personal Data

According to this pilot the list of Personal Data that could be used for the Services are:

- Title
- First name
- Last name
- Date of Birth
- National ID number
- Municipal census
- Sex
- Home telephone
- Mobile telephone
- Email address
- Residence address
 - Street name
 - Street number
 - Post code
 - City
 - Country

- Living address
 - Street name
 - Street number
 - Post code
 - City
 - Country
 - Social Security Number
- License plate
- Employment contract and salary information
- Bank details

4.7 Data privacy measures

In order to meet the need of the project, this pilot will use data belonging to a group of friendly users. According to make Santander GDPR compliant, the overall security, data minimization and encryption techniques, as well as digital signature, will be employed.

4.8 Expected data volume and users

A sample from 5 to 10 users is expected to be involved in the pilot deployment.

5 MITA Use case

5.1 Introduction

The Malta Information Technology Agency (MITA) is the central driver of Government's Information and Communications Technology (ICT) policy, programmes and initiatives in Malta. As part of its functions, MITA manages the implementation of IT programmes in Government to enhance public service delivery and provides the infrastructure needed to execute ICT services to Government.

For the purpose of this project, MITA has selected an eGovernment Services provided by Business First (<https://businessfirst.com.mt/en/Pages/home.aspx>), a Government entity acting as a front line for persons wishing to set up a business. It acts as a one stop shop and gathers all information required by various local authorities in one submission. Once information is gathered Business First transfers the relevant data to third party data controllers such as the VAT Department to issue a VAT number, the Office of the Commissioner for Revenue (CFR) to issue a PE number, Jobsplus to issue

an employer number, the National Statistics Office as required depending on the type of business activity (NACE Codes), the Environmental Health Unit as required by law.

Business First currently gathers all information, including personal information through an electronic form (eForm) and notifies applicants (data subjects) of the transfer of their personal data as part of form. The procedure can be availed of by persons registering a company or a sole trader business. Two forms are available at the following links:

(i) To register a Company:

<http://eforms.service.gov.mt/EForms/Account/Authorize?Controlled=True&CustomLoginName=Companies>

(ii) To register as a Sole Trader:

<https://forms.gov.mt/en/Services-And-Information/eforms/Pages/MainPages/FormsHandlerPage.aspx?version=Simplification&processid=498&applicantType=1&locale=en-GB&retURL=/en/Services-And-Information/eforms/Pages/Landing%20Pages/BusinessStartup-SoleTraders.aspx>

As part of this eForm applicants are required to provide personal information which makes the process a very valid use case to test the PoSeID-on platform. Moreover, this particular eForm is significant as a use-case for the PoSeID-on platform because it involves a number of actors as recipients of the personal information provided via one form/electronic service. The purpose of the processing and processing requirements differ between the various recipients. This information is currently provided to the data subject at the moment of collection of the personal information subject to consent. Once the eForm is submitted, any further action in relation to that personal data by the data subject would need to be addressed to the relevant recipient or recipients separately. It is envisaged that the PoSeID-on platform will provide the data subject with better visibility (access to one dashboard noting the various transfers of personal information) and better control for any follow-ups in relation to the personal information submitted to the recipient entities.

5.2 High-level description

MITA is limiting the scope of this exercise to the eForm for Registration of Companies.^[1] The eForm provides a single channel for prospective companies to commence operating as company registered with the Maltese Registrar of Companies. The eForm amalgamates all forms required by the various local Government authorities and/or agencies into one form. The eForm may also be used by a registered company that does not have a valid VAT number but requires a VAT Identification number for VAT grouping purposes.

By submitting the Business First eForm, the applicant triggers the following processes:

1. Creation of a VAT number/s – to register with Office of the CFR - (VAT Department) in the event that the business activity is taxable;
2. Creation of a PE number – to register as an employer with the Office of the CFR (IRD Department) in the event that the activity will entail the engagement of employees during the initial stages;
3. The National Statistics Office are also notified with the registration of the new business registration;
4. Creation of an Employer number – applicable only when the applicant registers for a PE number applicants are automatically registered with Jobsplus and an employer number is provided.

[1] MITA will not be implementing Poseidon in connection with the Registration as a Sole Trader Form due to technical reasons.

5.3 Dashboard for Businesses: Scenario

5.3.1 Scenario without Poseidon

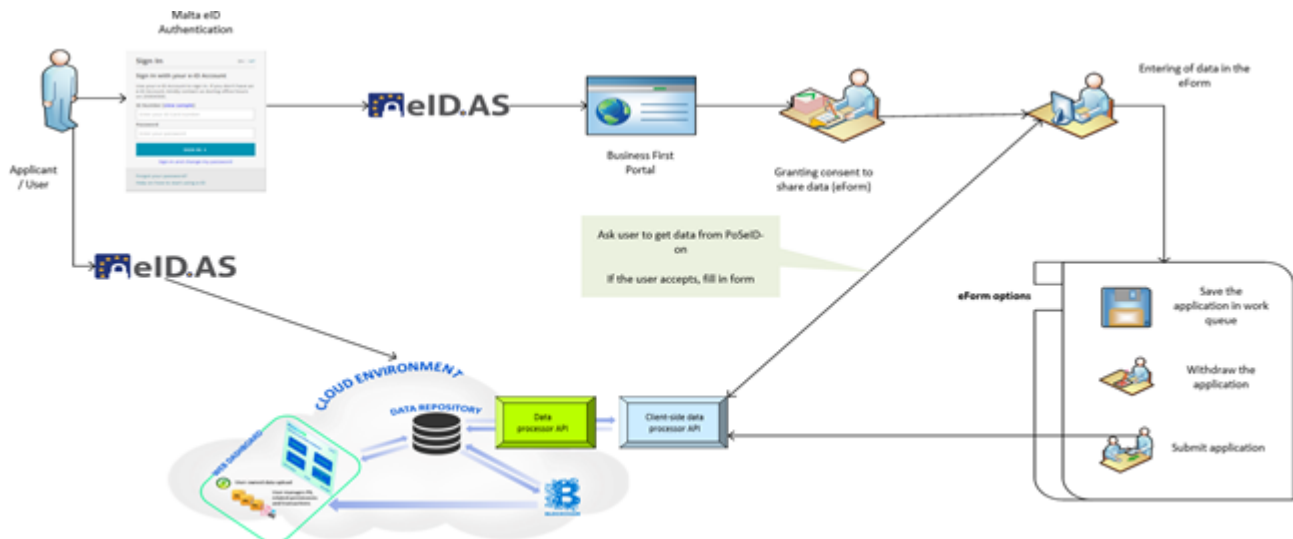
The current scenario for submitting an eForm with Business First for the Registration of a Company is as follows:

1. Open URL

<http://eforms.service.gov.mt/EForms/Account/Authorize?Controlled=True&CustomLoginName=Companies>
2. Login the eForm (through the above link) using eID or using his/her ID Card Number and ID Document Number, the latter is found at the back of the Identity Card. Both options will prompt the user to access the eForm as "Individual" or "Authorised Representative on behalf of the Applicant". Where the applicant is an "Authorised Representative on behalf of the Applicant" the competent authorities and/or agencies vetting the application will confirm the validity of the applicant acting as representative (which is registered with the Office of the CFR).
3. Applicant is directed to the Data Protection Notice and Consent Form and requested to provide consent for the transfer of data to the respective Government entities as applicable. Once consent is provided, the applicant may proceed to next screen detailing the type of information that will be forwarded to the respective Government entities.
4. Applicant is directed to populate the form. Where the company Registry of Companies (ROC) number and Contact ID Card/Passport number are validated against the Commissioner for Revenue (CFR) systems, the contact, applicant, business and address sections would be pre-populated with the information retrieved from the Government Corporate Data Repository and CFR systems. Other information pertaining to the applicant, bank, business, employment (in case of employee engagement), business activity, and branches (where applicable) would need to be completed by the applicant manually.
5. In case the applicant has not used his/her eID to access the eForm, a copy of the ID card or Passport would need to be attached to the application.
6. Depending on the information submitted, the applicant would be required to select the type of VAT registration according to CFR business rules.
7. Once the applicant clicks on "Submit Form", the eForm will send email notifications to the intended recipients as notified in the "data protection notice and consent form" and "transferring of data section" of the eForm. The competent authorities and/or agencies will

process the part of the application concerning their service and will create the VAT number(s), the PE number and the Employer reference as applicable. The eForm will also send email notifications to the intended recipients and will be transferred to the VAT Anti-Fraud Unit for vetting.

5.3.2 Scenario with Poseidon



5.3.2.1 User Journey

With integration to the PoSeID-on platform it is envisaged that the process flow will work as follows:

- i. Applicant logs into the eForm;
- ii. In the process of filling in the eForm, Applicant may opt to get personal data through PoSeID-on or input the data manually and register the consent in PoSeID-on;
- iii. Applicant clicks link to PoSeID-on and is prompted to identify themselves;
- iv. PoSeID-on identifies information required by the eForm and requests Applicant (as data subject) to accept or decline the provision of information to the competent authorities and/or agencies as required;
- v. On accepting to provide information, Applicant is redirected to the eForm which is populated with data retrieved from the consents/transfers registered on PoSeID-on.

Once the eForm is submitted the resulting consents/transfers should be registered **automatically** the PoSeID-on Platform, unless already registered.

5.4 Number and kind of services to be integrated

MITA will limit the scope of the exercise to the Registration of Companies eForm (<http://eforms.service.gov.mt/EForms/Account/Authorize?Controlled=True&CustomLoginName=Companies>). It is envisaged that integration to the PoSeID-on platform will entail customisation of the eForm solution.

5.5 Third Parties to be involved

Although the business process is owned by Business First (a Government entity), MITA will be the sole representative for the purpose of completing the deliverables of the PoSeID-on project in relation to the MITA use case. For this purpose MITA will be provisioning a virtual environment that will be used specifically to test the PoSeID-on platform.

The ultimate objective is to test this Platform as a proof of concept on one eGovernment Service and, if successful, propose implementation for other eGovernment Services. As the Government IT Agency, MITA is in a position to advise Government on the changes necessary to eGovernment Services to integrate with the PoSeID-on Platform for other services.

5.6 Types of Personal Data

The type of personal data gathered by the eForm for Registration of Companies includes the following:

- Name
- Surname
- Identity Card Number
- Identity Card Document Number
- Residential Address
- Email address
- Telephone Number
- Nationality

5.7 Data privacy measures

The MITA use case will involve the provisioning of a separate environment to test the PoSeID-on platform (separate from the live environment which processes live data) and will use dummy data to test the process flow of the eForm as integrated with the PoSeID-on platform.

5.8 Expected data volume and users

At least two (2) users to represent Applicant applying to register their own Company (as owner) and an Authorised Representative on behalf of the Company (the latter being a tax practitioner which is registered with the Office of the Commissioner for Revenue).

6 SOFT Use case

6.1 Introduction

The pilot in the private sector, hereafter Pilot 4, will be implemented and deployed by SOFT selecting some of their users, during the phase of pilot planning (WP6).

Softeam is a private French software vendor with about 1000 employees. Softeam develops a software called e-Citiz – a platform for Business Process Management for both e-government and companies, and which has been on the market since 2004. Softeam has a big experience in personal data management due to several business projects and some research projects. One of the last research project, PICS201611 (Personal Information Controller Service) is very close to PoSeID-on because it aims to collect user's given authorizations of sharing personal information. PICS2016 connects user's safe to help him to fill-in forms, but PICS2016 doesn't support the eID integration and blockchain storage of personal information. PoSeID-on and PICS2016 are complementary projects and Softeam is very interested in PoSeID-on project and on investing in the growing market of Personal Information Management.

With the e-Citiz platform, Softeam proposes the SVE ("Saisine par Voie Electronique" which means Seizure by Electronic Way), an eService product allowing users to apply for a claim or any sort of demand to the company.

This eService can be customized for various applications and is for now close to the market of eGovernment due to a regulatory constraint on municipalities in France. SVE can be used as well by eGovernment structure as private companies. The point of interest on the SVE service is about personal information because for every application, the user (citizen or customer) has to fill some personal data (first name, last name, postal address ...) on every claim. That's why the SVE eService is a good candidate for a PoSeID-on pilot.

Softeam has several clients of the e-Citiz platform and SVE product. There is BCA Expertise, a company leader in automotive expertise for insurance companies proposing a SVE service to customers for mediation with insurance companies, Certinomis, a company producing digital certificates to ensure security in communications using the eCitiz platform, etc.

Softeam will select end-users from his customers portfolio to participate to this pilot. This will allow a variety of users from different fields to test our PoSeID-on solution.

6.2 High-level analysis

The SVE pilot will be based on the SVE product. It will imply the customization of the SVE product to integrate PoSeID-on solution to provide the users of the current SVE services with a single platform for personal data management, as well as to support SVE to be compliant with the GDPR.

PoSeID-on solution will be integrated with the current SVE product and will be accessed upon access authentication using "France Connect" – the French current service acting as the trusted Access Management Authority. Softeam will be in charge of the SVE modifications and will provide an execution environment for the pilot.

Upon finishing the integration phase, the trial will be run for 1 or 2 months, to collect user's feedback, improve the solution and evaluate the provided service across the GDPR compliance and customer control of Privacy dimensions.

Analysis of the Poseidon platform shows that the main features for the End User(DataSubject) have to be tested. These main features are "subscribe", "share data", "list authorizations" and "revoke sharing". The scenario is built to test these features and, during these tests, technical results and benchmark will be evaluated too.

6.2.1 SVE Privaciz Consent scenario without PoSeID-on

Softteam provides a use case pilot in order to gain the PoSeID-on project.

Before Poseidon integration, the SVE Privaciz consent for Softteam can be described as this:

1. First the physical person has to create an account or identify herself with the "France Connect" Service which is the French service for "Access Management Authority".
2. Once identified, the user has to choose which Softteam's entity he wants to express his GDPR rights
3. Then he has to choose which right he wants to use
4. Depending on the selected right, a page is displayed to alert him about needed information to fulfil his claim
5. Information about his identity to prove who he is
6. A detailed description of what he expects from Softteam about his personal information
7. The tool displays a summary of the claim
8. The claim is then validated and sent to Softteam technical contact to handle the request

Figure 27: SVE scenario without PoSeID-on

6.3 Simplified e-services for French citizens: Scenario

USER JOURNEY

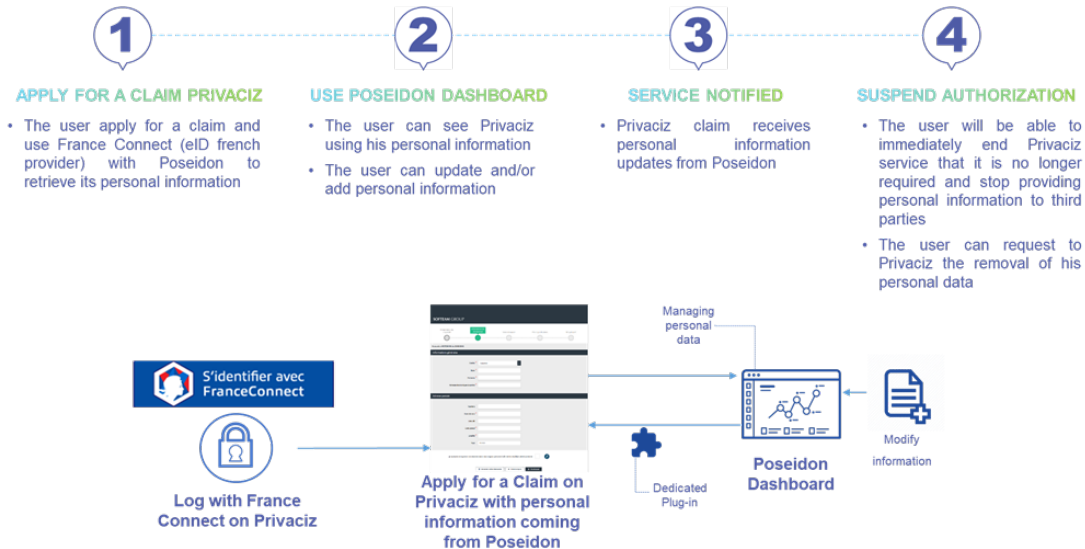


Figure 28: SOFTEAM Use case - User journey

6.3.1 User Journey

The pilot will validate different actions involving customer personal information:

1. Apply for a claim Privaciz:
The User will apply for a claim by connecting its certified identity from "France connect" to the SVE Product.

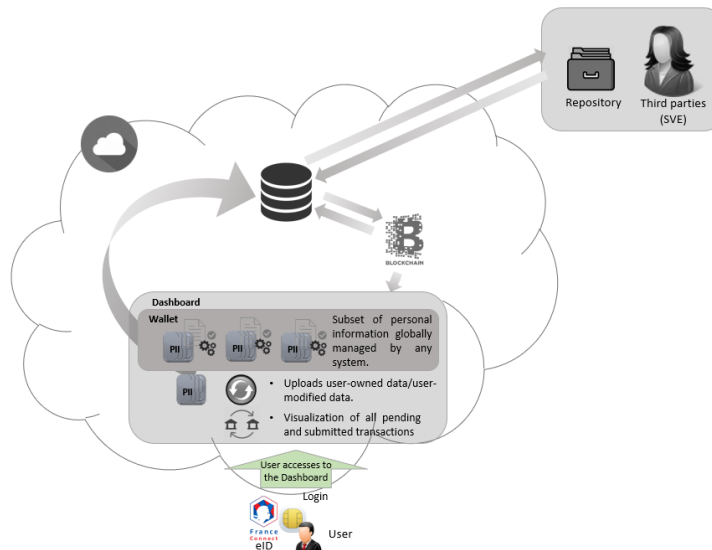


Figure 29: Apply for a claim Privaciz

2. Use PoSeID-on Dashboard:
The User will allow SVE to use a dataset of his personal information from PoSeID-on and access the PoSeID-on Privacy Control Dashboard:

- Identify all the entities processing personal data and sources where personal data is stored;
- Visualize all pending and submitted transactions (set/update/change permissions, modify/delete/update personal information).

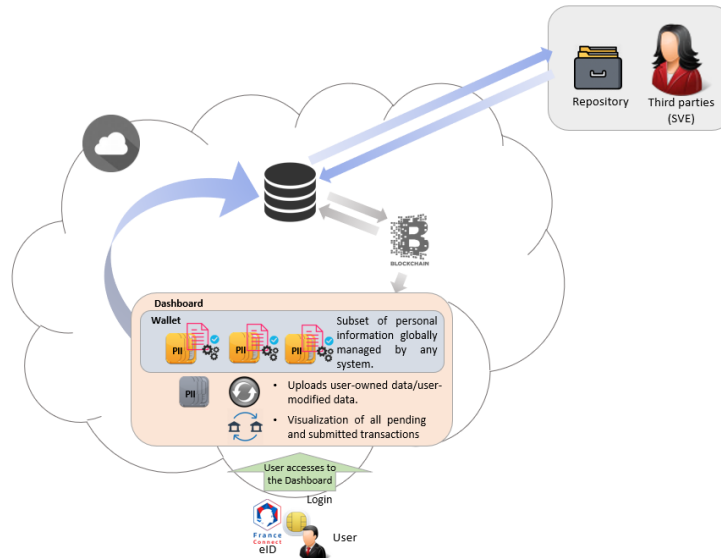


Figure 30: Use PoSeID-on Dashboard

- Service Notified:
Modify his personal information (postal address for instance) from the PoSeID-on dashboard and see if SVE received the modified information.

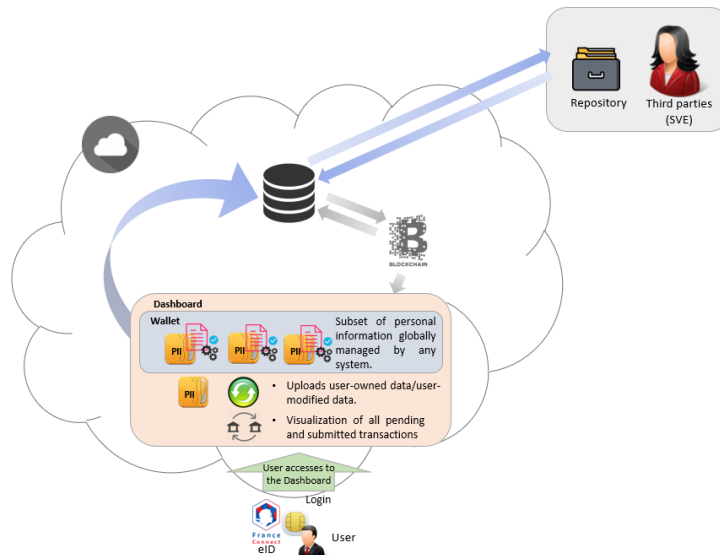


Figure 31: Service Notified

- Suspend Authorization:
Revoke (After a while) authorization for SVE to use the user's personal information.

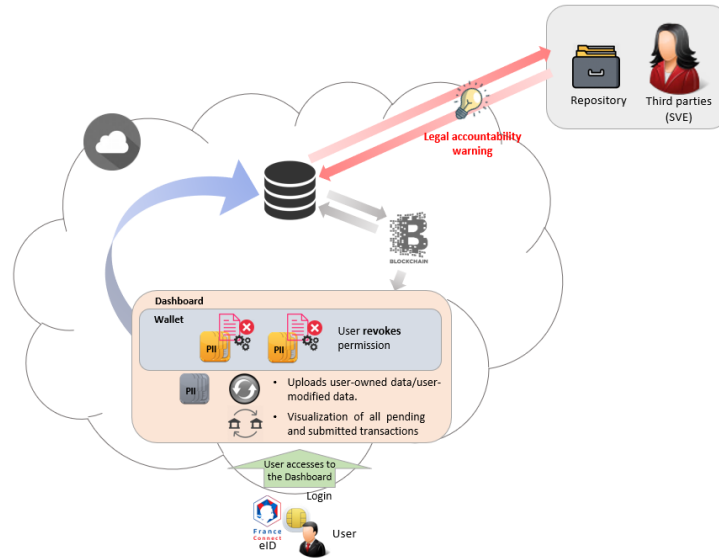


Figure 32: Suspend Authorization

Because of national legal provisions, SOFTEAM must keep some users' data for five years max. A data timer for deletion is then set. The timer starts from the moment the user authorizes SOFTEAM to access his PII. At the end of the five-year period, a trigger will automatically revoke the user's permissions to SOFTEAM.

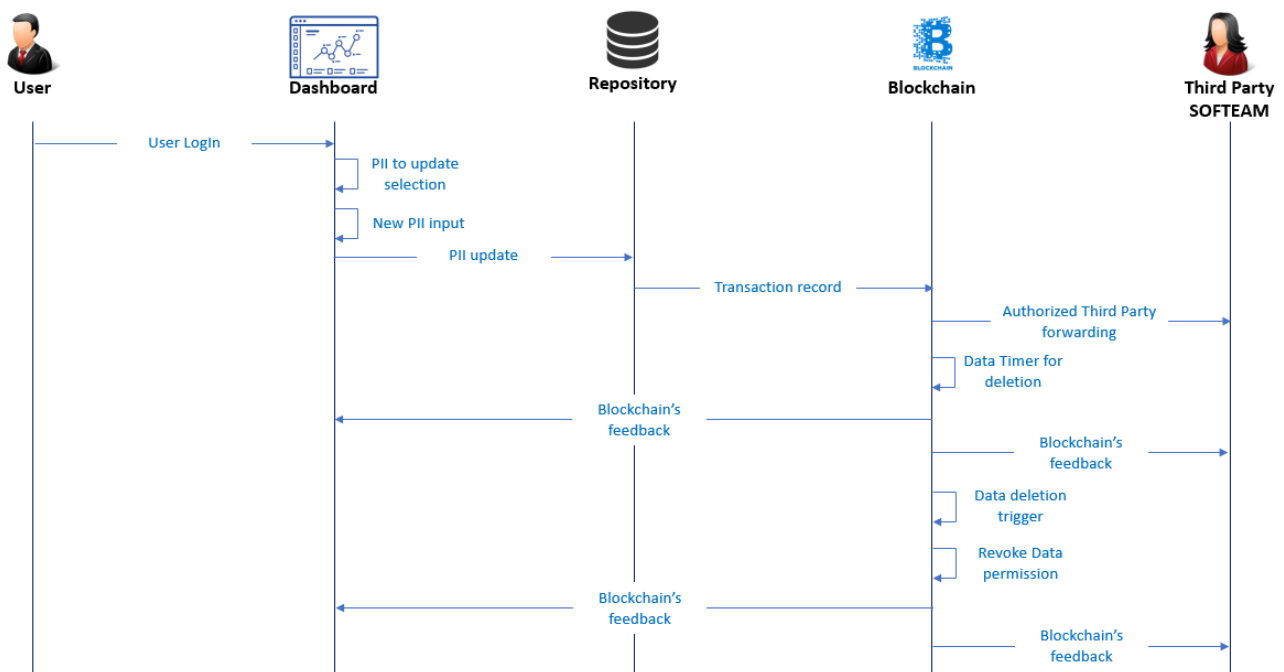


Figure 33: SOFTEAM Use case - Data deletion trigger

6.4 Number and kind of services to be integrated

The pilot will only integrate one service, SVE for Privaciz, as presented during the meeting in Rome. The SVE product will be customized to integrate PoSeID-on in order to provide users of the current SVE services with a single platform for personal data management, as well as to help SVE be compliant with the GDPR.

6.5 Third Parties to be involved

The whole pilot will see Softeam as the only actor involved, not needing any Third Parties for its accomplishment.

6.6 Types of Personal Data

Below is a list of Personal Data that could be used for this pilot:

- Title
- First name
- Last name
- Email address
- Postal address
 - Street name
 - Street number
 - Post code
 - City
 - Country

6.7 Data privacy measures

This pilot will use fake data, as a way to be compliant with the GDPR requirements. Indeed, this technique will allow to process data during the whole pilot – that can be easily considered as an experimental project – avoiding all the relevant risks for and potential damage to any prospective user, as a result of mistakes, data breaches, malignant attacks, etc.

6.8 Expected data volume and users

A sample that ranges between 7 and 10 users is expected to be involved in the pilot deployment.

7 PDA and RMM Applicability on the Use Cases

The PDA and RMM modules are suitable to be used across all the previously described use cases. In each case, their role is to monitor transactions and logs, respectively. Then, when privacy risks arise respective warnings are sent to the dashboard and/or data processors. Each warning message is either directed to data owners or administrators. By sending each warning message directly to each involved party, only the recipients can be notified and access the contents. Through the Web Dashboard, it is possible to access each notification and further explore its contents. The notifications contain information about the involved parties, the reason behind the warning and respective details.

7.1 Personal Data Analyzer (PDA)

The PDA is used to monitor personal data transactions and related warnings generated by the blockchain platform. The module detects and prevent anomalies and misbehaved transactions. A warning is generated each time a transaction does not comply with pre-defined rules (e.g., permissions or Data Processor internal reputation).

The PDA is used to control personal data in a transaction with the aim of discovering all previously non-identified personal data, such as personal data for which there is no data subject authorisation. Due to the sensitive nature of the analysed data, the PDA acts only when explicit consent is provided by the user. Furthermore, all input data is discarded after each analysis. In case the user does not provide explicit consent, the PDA will not operate for the data from that specific data subject. While this scenario is not the most desirable, it does not affect other data subjects.

The PDA monitors PII transactions, where explicit consent is provided, in order to detect and assess privacy risks. The module interacts with the message bus, which, in turn, communicates with the dashboard and the data processor API. Through the data processor API, a data processor can send PII data to the PDA for analysis and detection of possible privacy issues. shows the path of a transaction that is sent for the PDA for analysis.

Send Data to PDA for Analysis

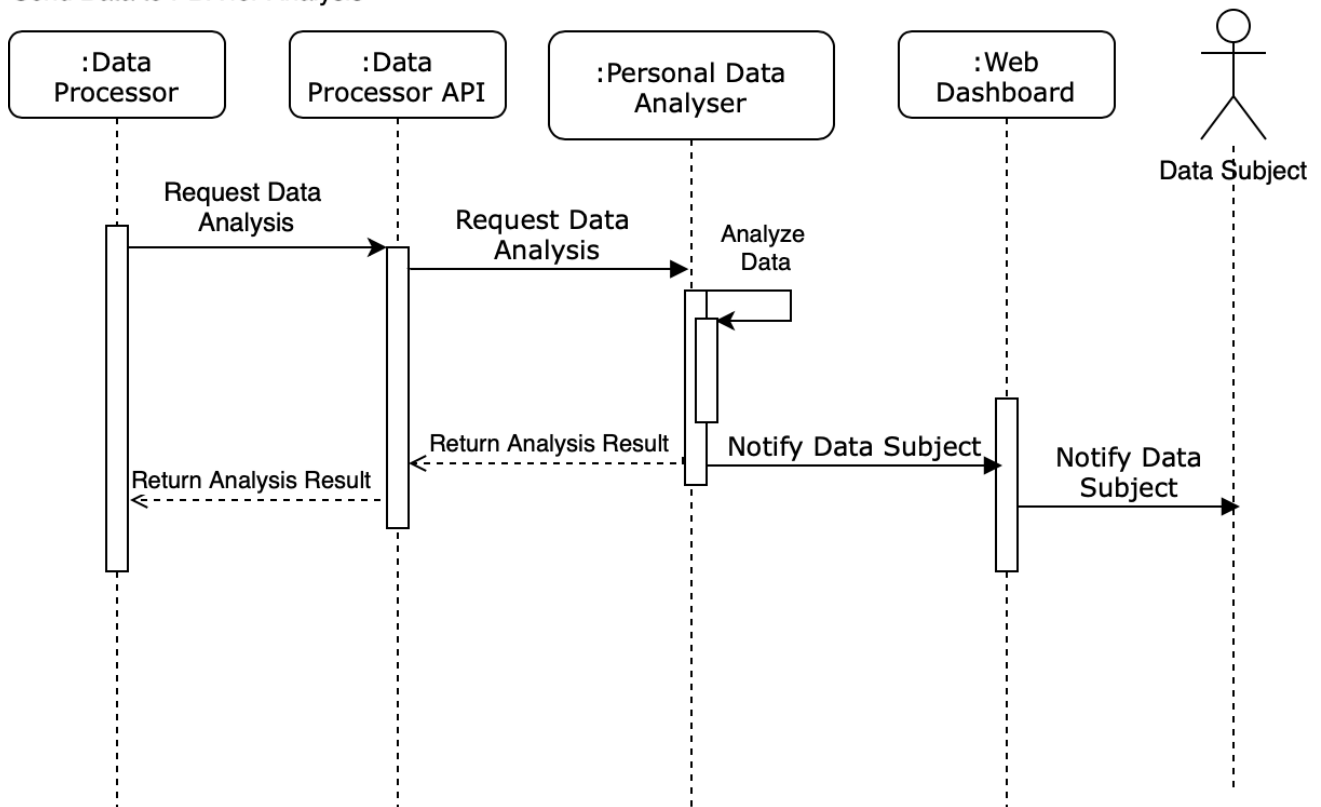


Figure 34: Data Sent to PDA for Analysis

The reason for warnings (i.e., types of alerts) to be generated by the PDA can be due to any of the following situations:

- Permissions do not match the data contained in the transaction.
 - For example, a data processor has permission to access the user's email and phone number, but the transaction also contains the address.
- PII type does not match with the respective content.
 - For example, a credit card number not containing the expected type of information: Credit Card Number: address of the person.
- The reputation of a Data Processor involved in a transaction is below a threshold.
 - For example, with a normalized reputation, if a data processor has a reputation below 0.3, then a warning message may be sent to the user.
- The combination of the PII types involved in a transaction.
 - For example, if a transaction containing highly sensitive PII types (e.g., bank details, passport number, and social security number) is occurring, a warning may be generated.
 - Moreover, if a transaction involving Data Processors with a low reputation and highly sensitive PII is occurring, a warning may also be generated.

Moreover, if a transaction involving Data Processors with a low reputation and highly sensitive PII is occurring, a warning may also be generated.

7.2 Risk Management Module (RMM)

The RMM is responsible for monitoring the PoSeID-on, both from a system-wide perspective and from individual data subjects' operations. The RMM is expected to detect and evaluate possible security and privacy risks, such as anomalous behaviour from data processors (e.g., a specific data processor suddenly starts collecting much more data than usual from a large number of data subjects, which may mean the data processor was hacked and is being used to syphon PII to external attackers) or risks associated with a specific data subject (such as successive attempts to log in with his or her credentials).

Risk detection is performed by combining Machine Learning (ML) algorithms, which analyse multiple sources of information about transactions, user-level behaviour, and system-level behaviour, in the form of component logs. When the data subject provides explicit consent, transaction-specific data and PII will also be sent to the RMM and used to complement this analysis. High-risk levels may trigger alerts to PoSeID-on administrators and data subjects, depending on the RMM settings.

The RMM module is used to evaluate and manage privacy and operational risks within the PoSeID-on system, through analysis of operational logs and PII exchanges, and manages a risk score associated with each data processor. This can be used to advise on which service should eventually be disabled in case of anomalies and high exposure to privacy risks. Figure 35 depicts an operational log being sent to the Risk Management Module for analysis.

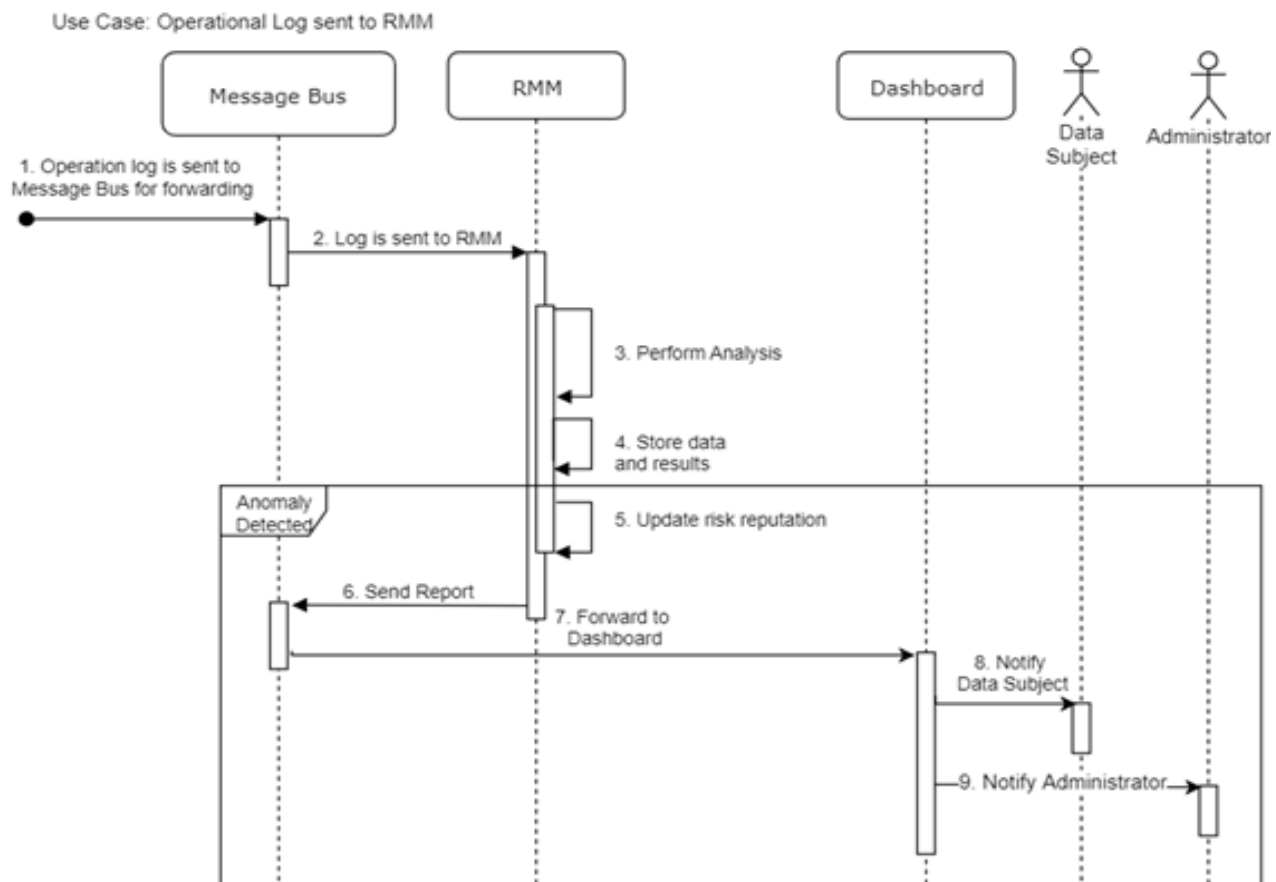


Figure 35: Operational Log Sent to RMM

The reason for warnings (i.e., types of alerts) to be generated can be due to any of the following situations:

- System-wide log patterns deviate from the normal patterns of PoSeID-on
 - For example, if a module of PoSeID-on crashes or starts exhibiting strange behaviour, operational logs will deviate from the regular log pattern and a system-wide warning will be issued.
- A collection of logs involving a data subject deviates from the expected pattern of logs for data subjects
 - For example, if a data subject receives requests from multiple data processors at the same time, it may be a target and if that pattern is not according to the expected pattern of requests, a warning will be generated.
- A collection of logs involving a data processor deviates from the expected pattern of logs for data processors
 - Similarly, if a data processor starts making a large number of requests to a single or multiple data processors and that behaviour does not comply with the normal behaviour of a data processor, a warning will be generated.

Similarly, if a data processor starts making a large number of requests to a single or multiple data processors and that behaviour does not comply with the normal behaviour of a data processor, a warning will be generated.

7.3 User Journey

The following points describe the steps that users need to perform in order to assess or visualize a warning message from the Personal Data Analyzer or the Risk Management Module. It is also shown how the user can take action to solve the issues raised by the warnings.

1. Access and login PoSeID-on Dashboard:

Figure 36 shows the concept access page. The user needs to introduce his/her credentials in order to access the information provided by PoSeID-on. After a successful login, the user is redirected to the main page of the PoSeID-on platform.

POSEIDON

User ID

Password

[Log in with eIDAS](#)

Figure 36: Dashboard access Concept Design

2. Visualize the main page of the PoSeID-on Dashboard

At this stage, the user is presented with a summary of his/her account. As shown in Figure 37, the information displayed is related to the number of the data requests, the number of data processors, number of permissions granted and the latest exchange reports.

The user can also access specific details of his/her account. On the left-hand side of the webpage, the user can check the latest *Messages*, information about the *Data Processors* and look for *Help*. Since all the warnings generated by the PDA and RMM are accessible through the *Messages* tab, the user should click on it for further information.

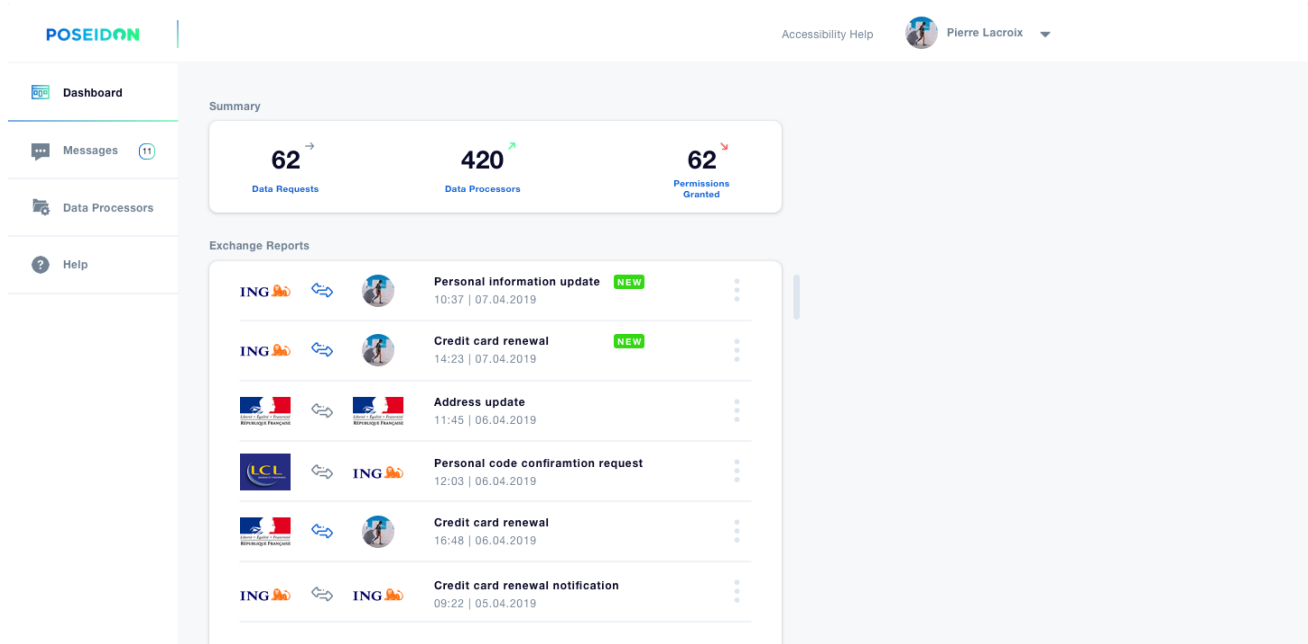


Figure 37: Main page of the Web Dashboard

3. Visualizing and resolving the PDA and RMM warnings

After clicking the *Messages* tab, the user is redirected for the messages page. If there are any warnings issued by the PDA and RMM, they are displayed in this page.

In case the PDA generates warnings about any of the previously described situations (section 7.1), the Web Dashboard and its *Messages* tab informs data subjects about the data privacy problem that was identified (as shown on the left-hand side of Figure 38). In this example, the message indicates that one of the Data Processors (e.g., Italian Ministry of Economy and Finance) has permissions to access the email and phone number but the transaction also contains the user's address. Additionally, the Web Dashboard presents data subjects with a direct button (*Edit Permissions*) to check his/her permissions and to resolve the respective issue (as shown on the right-hand side of Figure 38).

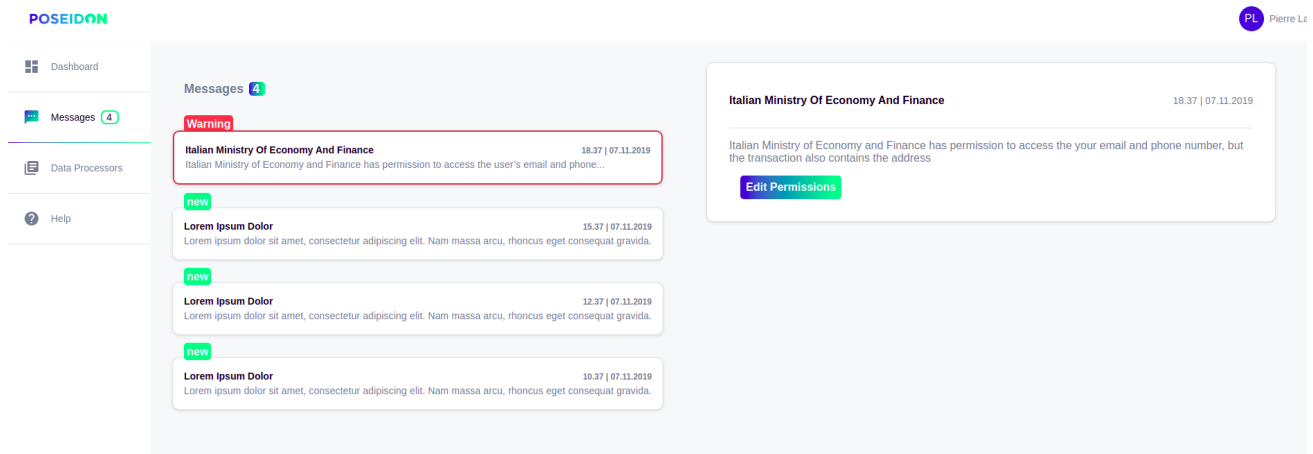


Figure 38: PDA notification and button to address the respective issue

Similarly to the PDA, if the RMM generates warnings about any of the previously described situations (section 7.2), the Dashboard also informs data subjects about the problem that was identified (as shown on the left-hand side of Figure 39). In this example, the message shows that the PoSeID-on platform has detected an abnormal behaviour from one of the Data Processors (e.g., Italian Ministry of Economy and Finance) and asks the user to verify the personal data shared with the Data Processor.

Again, the Web Dashboard also presents data subjects with a direct button (*Check Information*) to follow up on the message and check the information shared with the Data Processor (as shown on the right-hand side of Figure 39).

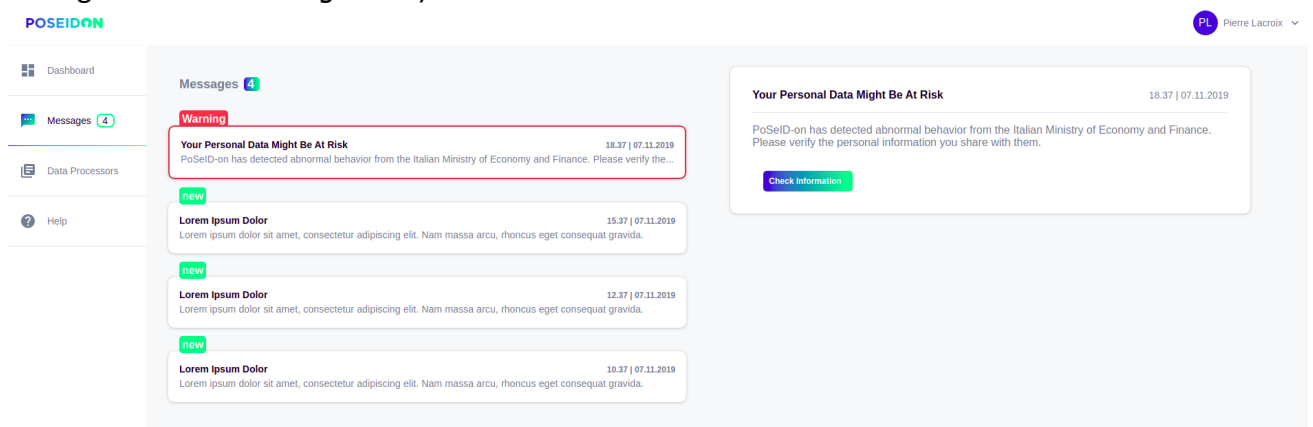


Figure 39: RMM Notification and button to address the respective issue

8 Conclusions

This document has been created to briefly provide more detailed information about the Use Cases/pilots of PoSeID-on project, accordingly with what emerged from the Task 2.1 “Use cases analysis and user scenarios”. All the Use Cases will match PoSeID-on technology, that could be developed according to the need of the single pilot. The platform used by each Use Case is the same (PoSeID-on platform), but the different pilots could take advantage of different functionalities, made available by PoSeID-on itself.

The description of the platform starts by exposing the users’ needs it must satisfy and the functionalities that have therefore to be granted. A general introduction to these subjects is provided in the second paragraph.

A more detailed view of how the platform performs is then made available through the following four paragraphs, each of them treating a different Use Case. Thanks to these dedicated insights a realistic projection of the PoSeID-on platform working is provided.

For a broader and more specific explanation of the technical and functional requirements, as well as of the architecture of the platform, the Deliverable 2.2 “System Requirements and Architecture” must be considered as the only official source of information on the matter. The document is an official deliverable.