Cyber
Security
for Europe

D5.1
Requirements Analysis of Demonstration Cases Phase1

Document Identification	
Due date	31 May 2019
Submission date	31 May 2019
Revision	3.0 (30 April 2020)

Related WP	WP5	Dissemination Level	PU
Lead Participant	NEC	Lead Author	Alessandro Sforzin (NEC)
Contributing Beneficiaries	ABI-Lab, AIT, ATOS, BBVA, CTI, CYBER, DAWEX, DTU, DUT, ENG, ISGS, i-BP, NEC, SIE, SINTEF, TDL, UCY, UMA, UMU, UPRC, UPS-IRIT	Related Deliverables	D4.1

Abstract: This document presents deliverable "D5.1 – Requirements Analysis of Demonstration Cases Phase 1". For all demonstration cases, it describes a set of identified use-cases together with their functional and non-functional requirements. Security and privacy requirements are treated separately from the above categories to highlight the importance of addressing the cybersecurity issues pinned down in the selected sectors. Additionally, the document serves as starting point for WP3 – "Blueprint Design and Common Research" to plan the technological advances that will allow CyberSec4Europe to address the identified cybersecurity challenges, and for WP4 – "Research and Development Roadmap" to plan the research roadmap of the project.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

CyberSec4Europe's objective is to lead the European cybersecurity research and innovation efforts with technology advancements catering to the complex reality of the single market, as well as the security of European citizens and society as a whole. To this end, the project's consortium includes a well balanced combination of industrial participants and research centers that will collaboratively identify and analyze cybersecurity industrial challenges in selected sectors, and will cooperate to develop appropriate solutions to address those challenges.

This document presents a comprehensive set of use-cases and their requirements, covering the seven representative CyberSec4Europe demonstration cases. A thorough analysis of the demonstration cases produced a rich set of functional and non-functional (including security and privacy) requirements that will guide research, technology development, and design in WP3, as well as the definition of the research roadmap in WP4. The document introduces not only those requirements that are essential to ensure the use-cases correct and efficient operations, but also those that may not be met concomitantly, even though they would contribute to the research and innovation results that the project wants to achieve.

This document additionally highlights security and privacy requirements for each demonstration case in order to put special emphasis to those cybersecurity issues that the project needs to address in the selected sectors.

Since the project is in its initial phase, the use cases and related requirements are represented at a high-level stage. Consequently, this document further focuses on providing a coherent narrative encompassing them. A more detailed specification will be delivered in subsequent iterations of this document.

Document information

Contributors

Name	Partner
Marco Crabu	ABI-Lab
Antonio Marrone	ABI-Lab
Marco Rotoloni	ABI-Lab
Teresa Spada	ABI-Lab
Mario Trinchera	ABI-Lab
Stephan Krenn	AIT
Rodrigo Díaz	ATOS
Juan Carlos Perez Baun	ATOS
Salvador Perez Franco	ATOS
Iñaki Aramburu Carmona	BBVA
Vasia Liagkou	CTI
Liina Kamm	CYBER
Peeter Laud	CYBER
Jeremy Decis	DAWEX
Alberto Lluch	DTU
Jolien Ubacht	DUT
Roberto di Bernardo	ENG
Giorgio Cusmà Lorenzo	ISGS
Médéric Collas	i-BP
Victor Poyet	i-BP
Rahul Bobba	NEC
Alessandro Sforzin	NEC
Jorge Cuellar	SIE
Karin Bernsmed	SINTEF
Per Håkon Meland	SINTEF
Aida Omerovic	SINTEF
David Goodman	TDL
Elias Athanasopoulos	UCY
Cristina Alcaraz	UMA
Rodrigo Roman	UMA
Antonio Skarmeta	UMU
Elma Kalogeraki	UPRC
Panayiotis Kotzanikolaou	UPRC
Spyros Papastergiou	UPRC
Abdelmalek Benzekri	UPS-IRIT
Romain Laborde	UPS-IRIT

Reviewers

Name	Partner
Marco Crabu	ABI-Lab
Evangelos Markatos	FORTH
Welderufael Tesfay	GUF
Ahad Niknia	GUF (High-level review and preparation for submission)

History

0.1	2019-02-27	NEC	Initial Outline
0.2	2019-03-15	NEC	Executive Summary
0.3	2019-04-01	NEC	Introduction
0.4	2019-05-10	NEC	Conclusions
0.5	2019-05-08	ABI-Lab, AIT, ATOS, BBVA, CTI, CYBER, DAWEX, DTU, ISGS, i-BP, NEC, TDL, UMU, UCY, UPRC, UPS-IRIT	Contributions to sections 3, 5, 6, 8
0.5.1	2019-05-09	CYBER, SIE, SINTEF, NEC, UCY, UMA, UPRC	Contributions to sections 2, 4, 7
0.5.2	2019-05-10	ENG, NEC, UMU	Contributions to section 9
0.5.3	2019-05-10	NEC	Quality check
0.6	2019-05-10	NEC	First complete version
0.6.1	2019-05-24	ABI-Lab, AIT, BBVA, NEC, ATOS, CTI, CYBER, DAWEX, DTU, DUT, ENG, ISGS, i-BP, NEC, SIE, SINTEF, TDL, UCY, UMA, UMU, UPRC, UPS-IRIT	Addressed comments of PC review.
0.6.2	2019-05-30	ABI-Lab, ATOS, CYBER, DAWEX, DTU, ENG, i-BP, NEC, SIE, SINTEF, TDL, TUD, UCY, UMA, UMU, UPRC, UPS-IRIT	Addressed comments of internal reviewers
1.0	2019-05-31	NEC	Quality check.
1.0.1	2019-08-26	ATOS, BBVA, CYBER, DAWEX, DTU, ISGS, NEC, SINTEF, TUD, UCY, UPRC	Updated requirements categories for sections 6, 7, 8
1.0.2	2019-09-03	AIT, CNR, CTI, C3P, ENG, GEN, NEC, OASC, SIE, UCY, UMA, UMU, UPRC	Updated requirements categories for sections 4, 5, 9
1.0.3	2019-09-03	AIT, CIT, UMU, UCY, UPRC	Updated T5.3 use-cases
1.0.4	2019-12-20	TDL	Updated T5.1 use-cases
2.0	2019-12-20	NEC	Quality Check.

2.0.1	2020-03-24	AIT	Addressed reading review comments to section 5
2.0.2	2020-04-08	SIE, NEC	Addresses reading review comments to section 4
2.0.1	2020-04-09	ENG	Addressed reading review comments to section 9
2.0.2	2020-04-17	TDL	Addressed reading review comments to section 3
2.0.3	2020-04-17	ATOS	Addressed reading review comments to sections 6 and 8
2.0.4	2020-04-23	UPRC	Addressed reading review comments to section 7
2.0.5	2020-04-24	NEC	Final check.
3.0	2020-04-24	NEC	Version ready for resubmission.
3.0	2020-04-30	GUF	Final check and Preparation for submission

List of Contents

List of Figures

List of Tables

List of Acronyms

ABC	Attribute-Based Credential
AGID	Agenzia per l'Italia Digitale
AIS	Automatic Identification System
AISP	Account Information Service Provider
AOS	Advanced Object detection System
API	Application Programming Interface
ASPSP	Account Service Payment Service Provider
BIT	Business Information and Tracking
CAD	Codice Amministrazione Digitale
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CCN	Common Communication Network
CMS	Content Management System
CSS	Container Status System
DP	Dynamic Positioning system
EBA	European Banking Authority
EBC	European Central Bank
ECDIS	Electronic Chart Display and Information Systems
ECHR	European Convention on Human Rights
EDI	Electronic Data Interchange
EDPB	European Data Protection Board
eIDAS	electronic IDentification Authentication and trust Services
EMCS	Excise Movement and Control System
EPC	European Payments Council
EU	European Union
FFS	Freight Forwarder System
FI	Financial Institution
FIM	Federated Identity Management
GDPR	General Data Protection Regulation
GDM	Global Data Marketplace
GOS	Gate Operating System
GSS	Gas Supply System
GUI	Graphical User Interface
ICT	Information and Communications Technology
IdP	Identity Provider
IdM	Identity Management
IMT	Incident Management Team
IR	Incident Reporting
IRT	Incident Reporting Team
IT	Information Technology
JIT	Just-In-Time system
LOD	Linked Open Data
LoLo	Lift-on-Lift-off vessels
LPA	Local Public Administration
MITM	Man in the Middle
NCA	National Competent Authorities
NIS	Network and Information Security
NVR	Network Video Recorder
OAuth	Open Authorization

OBSIDIAN	Open Banking Sensitive Data Sharing Network for Europe
OES	Operator Essential Service
OSS	Onboard Safety Systems
PA	Public Administration
PET	Privacy Enhancing Technologies
PISP	Payment Initiation Service Provider
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
REST	Representational State Transfer
RFID	Radio Frequency Identification
RTS	Regulatory Technical Standards
RTU	Remote Terminal Unit
SAML	Security Assertion Markup Language 2.0
SC	Smart Card
SCADA	Supervisory Control and Data Acquisition
SDVA	Social Driven Vulnerability Assessment
SIS	Ship Information System
SP	Service Provider
SPARQL	Recursive acronym for SPARQL Protocol and RDF Query Language
SSDLC	Secure Software Development Life Cycle
SSM	Single Supervisory Mechanism
TOS	Terminal Operating System
UC	Use Case
VIS	Visitor Information Service
VTMS	Vessel Traffic Management System
VTS	Vessel Traffic Service
WMS	Warehouse Management System
WP	Work Package
W3C	Wold Wide Web Consortium

Requirements Categories

This document uses a standard categorization to list each demonstrator's requirements. This categorization gives a common narrative to all demonstrators' requirements, thus facilitating readability and the interaction with WP3 and WP4. The list is based on RFC4949, with some adjustements to better fit the demonstrators' needs.

GENERAL AREA	CATEGORY	DESCRIPTION
Access Control and Authorization	AC	Access Control and Authorization
Accountability	Acc	Accountability
	NoA	Notification to authorities
	Rev	Revocation of credentials
	SLog	Secure Logging and Event Monitoring
	Transp	Transparency
Authentication	AuthnE	Entity Authentication
	AuthnF	Federated (Entity) Authentication
	AuthnM	Message Authentication
Availability	Avail	Availability
Confidentiality	CE	End-to-End Confidentiality
	Conf	Confidentiality
Development and Implementation	Resil	Resilience
	SC	Secure Coding
	SDLC	Secure Development Lifecycle
Hardware Security	HWToK	Hardware Support (Trusted platform modules, security cards, etc.)
Identity Management	IdM	Identity Management
Integrity	Dint	Data Integrity
	FT	Fault Tolerance
	noR	Non-Repudiation
	Sint	Operational Integrity
Policies	Config	Security Policy Configurability
	Trust	Trust
Privacy	Anon	Anonimity
	DPriv	Data Privacy
	GDPR	General Data Protection Regulation
	NoS	Notice to the data subject (the user)
	Unlink	Unlinkability
User Experience	Funct	Functionalities and Architecture Requirements
	Perfo	Performance
	UI	User Inteface
	Usab	Usability and Maintainability

1 Introduction

CyberSec4Europe is a project that wants to lead the European Union cybersecurity research and innovation efforts. The project comprises research centers and industries providing research excellence and industrial expertise. Their collaboration will not only help in identifying and analyse relevant cybersecurity challenges in today's European society, but also study and propose adequate solutions addressing those challenges.
The project has identified seven key research and innovation demonstration cases covering a wide spectrum of prominent research areas in both the public and private sectors. These demonstration cases constitute the core of the project and they will be mapped to technological and research challenges that a coordinated effort between research and industry partners will address. It is expected that the results of this cooperation will be adopted as technological components that the demonstration cases will integrate in their lifecycle.
The project's methodology to achieve these ambitious goals is to structure its lifetime in two cycles of research and development:

- The first iteration will provide an initial definition of the research challenges and roadmaps that will drive the second iteration of the project.
- The second iteration will then further refine the research goals of the project to exhaustively address the identified challenges while also making them relevant beyond the scope of the project.

The purpose of this document is to gather an initial set, as comprehensive as possible, of requirements related to the seven domains defining the demonstration cases. These requirements will play a key role in identifying the technological and research roadmaps of the project. For each demonstration case, the document first presents a number of use-cases identified by analyzing each domain in collaboration with the industry participants. Based on the description of those use-cases, the document outlines a list of functional and non-functional requirements describing the conditions that ensure the system's correct operations.
Additionally, this document serves as an overview of the demonstration cases to WP3 and WP4 so that they can design the technological components and outline the research roadmap of the project.

1.1 Structure of the Document

The document is structured as follows[1]:

- Section 2 gives a summary of all the demonstration cases.
- Section 3 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Open Banking* demonstration case.
- Section 0 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Supply Chain Security Assurance* demonstration case.
- Section 5 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Privacy-preserving Identity Management* demonstration case.
- Section 0 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Incident Reporting in the Financial Sector* demonstration case.
- Section 7 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Maritime Transport* demonstration case.

[1] The structure of this document has been inspired by a template by Professor J. Alberto Espinosa of the Kogod School of Business, American University, which can be found at his website here.

- Section 8 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe's *Medical Data Exchange* demonstration case.
- Section 9 presents the use-cases, together with their functional and non-functional requirements, identified in the context of CyberSec4Europe *Smart Cities* demonstration case.
- Section 10 concludes the document.

2 Summary of the Demonstration Cases

In this section, we provide a brief summary of all CyberSec4Europe demonstration cases. The goal is to give an overview of what cybersecurity challenges the remainder of the document covers.

2.1 Open Banking

This demonstration case will allow users to carry out financial transactions, including cross-border, using the new services available under PSD2 securely and with confidence from their mobile devices. Such services include being able to make payments to merchants by giving them access to one of their bank accounts and allowing the merchant to process a payment through an intermediary service with access to their bank account. In an open banking environment, users should also be able to terminate their relationship with the merchant, so they no longer have access to their bank account and work with a third party to transfer all their account information to another financial institution.

The overall result of this demonstration case will be to address, when users are seeking to obtain account information, the risks and vulnerabilities emerging from social engineering and malware attacks, provide protection for bank administration security policies as well as overcome weaknesses in the design and/or implementation of APIs in use and to prevent fraud and data loss in relation to the access and request of payment by third parties in an open banking environment.

2.2 Supply Chain Security Assurance

The demonstration case will allow involved stakeholders to secure the supply chain and trace the movement of components and goods during all stages of the supply chain. They want to guarantee quality and integrity of the parts and products. The resulting system should support nonrepudiation, detect manipulations and errors in the supply chain and resolve conflicts quickly, and preferably, avoid errors and prevent counterfeiting in the supply chain. In the case of low quality or counterfeit components that could lead to problems with the final product and partners have to identify and resolve the issue or conflict quickly. Players will only have to reveal the data that is needed to ensure the integrity and the security of the supply chain, keeping all other information private and internal.

The overall result of this demonstration case will be to provide a blueprint for supply chain solutions for multiple sectors. In particular, cross-organizational and transnational workflows are in scope. Hence, CyberSec4Europe, with its consortium of organizations and companies of different regions, legislations and business sectors, provides the fertile ground to elaborate and testify a consolidated approach and technology. One specific application will be for an energy use case involving transformers for power distribution, where the supply chain for the transformers will be critical to ensure proper operation of transformers as crucial components in power networks.

2.3 Privacy-Preserving Identity Management

This demonstration case will enable an identity infrastructure to fulfil the need for strong privacy-preserving authentication with a distributed and scalable platform for privacy-preserving self-sovereign identity management. The platform will allow users to collect and manage attributes and claims from identity service providers, authenticate to service providers, provide consent for and control the personal data usage in a seamless and privacy-preserving fashion.

The demonstration case will also showcase an example of the secure and trustworthy exchange of higher education certificates between organisations, such as educational institutes, universities, state agencies, private sector organisations, as well as with individuals. It will allow higher education graduates to share documents and prove their expertise during a preselection stage. The verification of the education credentials will keep graduates' information private until needed later, such as for recruitment. Graduates will be able to prove their competencies as well as other qualifications, hiding information not relevant to the situation, which is an example of applying the data minimisation principle as required by the GDPR.

This demonstration case will also provide transversal support to the other demonstration cases and empower end users and organisations to control their privacy and increase the trust in Internet services.

2.4 Incident Reporting in the Financial Sector

This demonstration case will develop a platform that enables organisations or their entities to report incidents according to the different procedures and methods specified by applicable regulatory bodies, such as PSD2 and the ECB Cyber Incident Reporting Framework. The platform will specifically support cybersecurity information data sharing in a bidirectional way, allowing for a centralised or a decentralised approach, i.e. a peer-to-peer approach.

The resulting prototype will cover trustworthy information sharing including secure and efficient protocols for information exchange, big data analysis of cybersecurity information and quantitative risk assessment, the application of machine learning and AI to prevent attacks and threats, but also to assist in decision support and improve reaction to incidents, secure and privacy-preserving efficient information storage possibly using distributed, blockchain based mechanisms as well as usable interfaces for the design and operation of cybersecurity procedures.

2.5 Maritime Transport

This demonstration case identifies the current cybersecurity challenges of the maritime sector and will design and develop a threat management system capable of continuously managing cybersecurity threats against Internet connected critical cyber infrastructures in the maritime sector. Security services will cover the whole ecosystem of maritime sector critical cyber infrastructures, including both those residing at the port side and the ship side.

The demonstration case will develop advanced threat models for the maritime environment, able to capture and assess new threats that may involve the whole maritime sector ecosystem and to assist the relevant stakeholders, such as ship operators and port operators, to be in line with the related regulations and best practices. It will also help port and ship operators to manage their security risks more effectively and to increase the resilience of critical maritime infrastructures, ultimately offering advanced security to maritime transport "users" such as citizens and manufacturers who use maritime transport services.

2.6 Medical Data Exchange

This demonstration case will integrate and validate in a realistic environment the research outcomes on the cybersecurity and sensitive and personal data protection for medical data sharing, enhancing the multilateral trust among stakeholders generating and consuming data in the medical business sector through theDAWEX data marketplace platform, improving its trustworthiness and creating new business opportunities as a result.

It will allow the secure and trustworthy exchange of sensitive data between several kinds of players with different aims and claims, regarding the security, data protection and trust issues: companies, public organizations and citizens, aligned with applicable legislation and the strategic policy framework (the GDPR, NIS Directive, blueprint for rapid emergency response, ENISA recommendations on security and privacy etc.).

2.7 Smart Cities

This demonstration case will connect the cyber security challenges of smart cities through Open & Agile Smart Cities (OASC). OASC is an international city network with the objective to “create an open smart city market based on the needs of cities and communities”. The demonstration case will also deploy prototypes addressing cybersecurity challenges mainly related to privacy management in data exchanges among city stakeholders and cyber security assessment that will be elaborated with OASC during the validation phases of the project.

Furthermore, the demonstration case will include a dedicated environment enabling ideas, needs, best practices and lessons learned exchange among cities and cities’ stakeholders to ease the identification, uptake, collaboration and deployment of cyber security services for smart cities, including novel business models to pool resources and decrease the individual cost supported by each city. This environment then will also act as a trusted marketplace for cybersecurity services, using a "pooling" delivery model of services and resources by connecting and leveraging existing catalogues for smart city solutions, for example the OASC Catalogue. This aspect of the demonstration case will address the novel governance model of the CyberSec4Europe competence network. The demonstration case will also include a ‘lifelong training’ mechanism and environment to decrease the impact of social engineering attacks.

3 Open Banking

In this section, we describe the requirements for the CyberSec4Europe demonstration case entitled Open Banking. We first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements featuring use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

This demonstration case investigates four different scenarios:

- Sharing of Identity Verification and Fraudulent Activity;
- An Open Banking Sensitive Data Sharing Network;
- Privacy Preserving Verifiable Credentials;
- An Open Banking API Architecture.

Each one of these addresses security concerns that have arisen as a result of the highly disruptive digital transformation in banking and financial services, from both the coming into force of new regulations as well as the introduction of new technologies. It could be said that Open Banking is just about data, and all that matters is how you use it. Ironically, while the GDPR is intended to protect citizens' data, PSD2 is designed to remove the barriers to accessing bank information and the treasure trove of sensitive financial data contained therein. Not surprisingly then, our four use cases all reflect in one way or the other the concerns arising from the emerging landscape of financial services about protecting access to and the potential loss of sensitive financial data.

The relationship of this Open Banking task to the overall objectives of CyberSec4Europe is that it addresses a set of real world security issues associated with a vitally important industrial sector, and in the process also highlights a number of key new EU regulations and directives that have far-reaching impact, such as the GDPR and PSD2. In addition, the intention of this task, once the demonstrators are established, is to extend the reach of the initiatives beyond the task consortium partners to involve other banking/finance institutions and Fintechs in exploring the security solutions as they evolve and mature.

(A) Sharing of Identity Verification and Fraudulent Activity

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled Sharing of Identity Verification and Fraudulent Activity. We first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

(B) Open Banking Sensitive Data Sharing Network for Europe (OBSIDIAN)

This section describes the requirements for the set of use cases associated with developing an **Open Banking Sensitive Data Sharing Network for Europe** for the CyberSec4Europe demonstration case Financial Transactions. We first provide an overview of the demonstration case's context. We then describe it in detail by providing its requirements and illustrating them with concrete use cases. We finally list the challenges and issues to take into account to succeed in demonstration use case's implementation.
Banks are facing several types of risks, which are growing with banking's digital transformation. These may include data breaches, banking fraud, money laundering and other illegal activities such as terrorist financing.

Today financial fraud is globalized. As bank strategies are focused on digitalizing critical processes like opening a bank account or adding a transfer beneficiary to a bank account, it is becoming very easy for a hacker to realise several fraudulent transactions from his living room within a short time and without fully revealing his physical identity. Moreover, criminals and their illegal activites can affect several banks without having to change his mode of operation, given that today banks do not share any information on effective frauds and associated data. Finally, with new technologies like Instant Payment which provide bank users with real time money transfer services, it will be even more difficult to fight against fraud, as a bank will not have any delay time to make a recall in the case of a fraudulent transaction.

Similarly, the lack of information sharing between banks (starting with institutional IBANs) makes it very difficult to fight against fraud because there are many false positives. In an open economy, we must also share sensitive data related to the fight against money laundering or terrorist financing in order to be more effective in our detection systems and protect the European market.

Sharing proven data and information about occurrences and non-occurrences of these risks between banking actors is an opportunity to globally improve cooperative detection models and resilience facing fraudulent activities, by reducing false positives / negatives. The CyberSec4Europe partner network could be theright place to demonstrate how info-sharing such security-enhancing practices would work and make it possible to engage a decision process at the right (i.e., European) level.

To achieve the expected outcome of the set of use cases associated with OBSIDIAN, we have created the conditions to increase collaboration across the following areas:

- business specification: which data / information to share and for which purpose;
- technical specification: how (technical protocol, needed infrastructure) to share with the right level of security / privacy;
- legal/political validation: validating sharing compliance with the latest regulations such as the GDPR to engage policy decision makers by making them aware of the overall implications.

(C) Privacy Preserving Verifiable Credentials

This section describes the requirements for the set of use cases associated with verifiable claims. PSD2 introduces two new payment services provided by new actors.

- **Payment Initiation Service Providers (PISPs)** will initiate online payments to third parties on behalf of the payers. These entities, which do not necessarily have a relationship with the payers' banks and are called Account Service Payment Service Providers (ASPSPs), shall access to the online account of the payers.
- **Account Information Service Providers (AISPs)** are able to give users a consolidated view of all their payment accounts even if they are managed by multiple ASPSPs.

Customers are entitled to a high level of security in mobile banking. However, these new actors raise new security issues. For example, a bank customer may give a PISP full access to their online bank accounts to initiate payments. If so, the provider would also have access to all the bank information associated with the user. Since no formal relationship with the ASPSP is required, it makes the protection of customers complicated for the banks. In addition, in this example AISPs would have access to all incoming and outgoing payments in order to provide a consolidated view of the customer's bank accounts. As a consequence, AISPs will gain access to sensitive information data such as rent and salary or insurance and health insurance payments. The task of the banks to protect the privacy of their customers becomes much more complicated in such a situation. Finally, it would be extremely difficult for users to understand what is happening to their data, where it is being saved and what their rights are. Nor is it clear in the case of any data loss, whom the responsibility would lie with.

3.1 Goals

3.1.1 Sharing of IdentityVerification and Fraudulent Activity

Banks and financial institutions perform customer due diligence as part of the onboarding process. The formal processes are called KYC (Know Your Customer) and AML (Anti-Money Laundering) and consist of sourcing and verifying customer data to make a decision on providing services to the applicants. The purpose of these processes is to verify whether a customer is who they claim to be and check against activities pertaining to money laundering or funding of nefarious activities. These processes also assess whether customers can perform fraud. The current problems can be summarized as below:

- **Cost of Compliance and Customer Fraud**: Customer due diligence is a part of the AML compliance. A recent report estimates the average cost of compliance at US$17.2 million in Switzerland to US$23.9 million in Germany. These costs impact the bottom and top lines of financial institutions;
- **Lengthy Onboarding Time**: Average KYC processing time ranges between a few days to a few weeks. The costly and cumbersome checks on introduce friction in customer onboarding and in some cases lead to abandonment and lost opportunities;
- **Lack of Data Sharing**: When a bank does a due diligence (e.g. KYC) on a new customer, there is no opportunity for customer to reuse the KYC verification when applying for services at another bank. There is an inherent lack of trust and communication which leads to banks and financial services repeating these processes leading to a poor customer experience. Blockchain technology is well suited to address this problem by created a trust-minimized data sharing infrastructure.

3.1.2 Open Banking Sensitive Data Sharing Network for Europe (OBSIDIAN)

We propose to experiment with the establishment of a trusted network to provide banks with a channel for sharing and exchanging critical information on effective fraud, institutional IBANs, money laundering and terrorist financing data using the latest open online banking services.

First, by making such information sharing possible, banks could improve their ability to detect and react in real time to fraud cases. For example, if a bank which had detected a transfer fraud was able to share with other banks the information about the IBAN implied in the transfer, these banks could take this information into account in time to prevent the fraudster from using this IBAN to realize other fraudulent transactions.

The PSD2 Regulatory Technical Standards (RTS) implemented in September 2019 do not effectively combat a wide range of fraud types as they focus solely on the payer. For example, fraud such as real time phishing, social engineering, technician fraud, supplier fraud scams (customers buying objects that do not exist), manipulated agency, cheque fraud, all of which we face on a daily basis, will not be reduced by this regulation.

On the other hand, another consequence of the lack of information sharing activities between banks is the rising leadership in the EU of non-European ICT providers in the field of risk scoring, thus leveraging globalised fraud information centralisation. Several of these ICT providers[2] can increase the risk management services aiming at scoring transactions in a bank information system to detect fraudulent ones. But:

- few if any of them offer services featuring all fraud typologies (transfer fraud, cash machine fraud, check fraud, payment fraud etc);
- their solutions are based on blackbox architectures to protect their competitive advantage.

There is also a sovereignty issue, given that this lack of cooperation is an opportunity for these providers:

- to become leaders in the field of centralisation and correlation of fraud information by contracting one-to-one with each bank;
- to increase their leadership by fueling their product roadmaps with a sharp knowledge of globalised fraud use cases, and then becoming essential actors by developing evident addiction to their services.

[2] IBM, threatmetrix, Ping identity, …

Finally, several organizations aiming at developing cooperation between financial actors already exist[3] but the data they share is not effective fraud data (for example, an IBAN signature used to realise a fraudulent transfer). These organizations are focused more on delivering, for example, cyber threat intelligence services and less on sharing effective fraud information.

3.1.3 Privacy Preserving Verifiable Credentials

The goals of this use case are to:

1. Identify / authenticate with a high assurance level the bank customer to their PISPs and AISPs
2. Manage the delegated access privileges a customer gives to their PISPs and AISPs
3. Make customers aware of the usage of their data, delegated rights, etc.

Registration and authentication processes on websites have been significantly simplified by federated identity management systems, which encourage single sign-on. An identity provider (IdP) centralises all the identity attributes of each of its users and provides them with a single authentication process they can use to identify and authenticate to any service on the Internet that is federated with the IdP. Based on web-based standard protocols (e.g., SAML, OpenID Connect), this process replaces the tedious task of manually declaring an identity by registering at each service provider (SP), with an automatic exchange of identity information between the IdP and the SP. Identity federation also simplifies user authentication in a password environment, since the user only authenticates to the IdP, thereby reducing the number of credentials to remember.

In the world of Open Banking, the PSPs (i.e., the banks), the ASPSP, the AISP and the PISPs can play the IdP role. They can build a circle of trust and operate a federated identity management (FIM) system. However, today's FIM systems have a significant structural weakness: namely, putting the IdP at the centre of the identity ecosystem.

- First, the trust model requires (1) the IdP to trust the SP to preserve the privacy of the user's identity information that it is asserting, and (2) the SP to trust that the IdP is the authoritative source of (all of) the user's identity information. Both of these trust requirements are unreasonable. No single IdP is the authoritative source of all a user's identity information. For example, a user may hold several accounts in several banks, and users may want to present their identity information to SPs that IdPs do not fully trust.
- Secondly, the IdPs are the centre of the identity eco-system, and issue short-lived identity assertions or tokens on demand to trusted SPs. Consequently, they know which SPs the user is visiting and when, which allows them to track the user. In addition, besides violating the user's privacy, it also introduces a severe security vulnerability as a recent Facebook hack highlighted. This allowed the attackers to access all the user's accounts at all the SP websites that trusted Facebook as the user's IdP. Since PSPs, like Facebook, share and store a huge amount of information about lots of users, such attacks have a big impact.

Verifiable credentials are the electronic equivalent of the physical credentials we have today such as plastic cards, passports, tickets, qualifications etc. Verifiable credentials are cryptographically protected and are stored in end users' devices such as mobile phones, laptops etc allowing users to carry them around with zero portability effort. Like plastic cards, verifiable credentials can be presented to whomsoever the user chooses, without asking the permission of anyone – unlike a user's identity attributes in federated identity management systems, which are only released with the permission of the IdP.

Verifiable credentials are not a new concept, but are just becoming standardised by the W3C, so this is an opportune time to demonstrate their potential in terms of enhancing an end user's privacy, security, trust and usability of the Internet – and financial systems in particular.

[3] https://www.first.org/, https://ec.europa.eu/anti-fraud/

3.1.4 Open Banking API Architecture

The following section describes the essential components for an adequate governance of the exposed services and the functional characteristics that could support the evolution towards Open Banking for open financial services.

In particular, a shared map of the macro-components and functionalities for the Open API was developed, starting from the study of different sources in the literature, from the analysis of case studies and market models and from the collection of ideas in the various moments of interactions that took place in the meetings of the working table.

The map is designed as a model to support API exposure with a view to openness. It represents a useful starting point for moving towards future scenarios, but clearly it must be understood as a necessary but not sufficient condition for Open Banking, since the technological, infrastructural and architectural adaptation must in any case be accompanied by a broader rethinking of the organizational aspects, governance paradigms and business logic support models.

3.2 Stakeholders

Sharing of Identity Verification and Fraudulent Activity
European banks and financial institutions will have an economic interest in the sharing of customer due diligence and fraudulent activity. There is an opportunity to reduce customer friction in the onboarding process and assist in the detection and curtailing of fraudulent activities

Open Banking Sensitive Data Sharing Network for Europe (OBSIDIAN)
European banks will have an economic interest in such a trust network as it would mitigate their fraud losses and improve trust and loyalty of their customers by better protecting them from attempted frauds. Extended use cases of such a trust network could include not only black list but also white list information sharing, that could be used to improve user experience with less friction linked to security procedures.
The trust between members of this network could be created by leveraging existing certification authority ecosystems. These kinds of actors would have a business motivation to participate and in addition:

- those in charge of regulation writing and privacy concerns would be involved to create the legal framework (like the **European Data Protection Board**);
- **Europol,** as well as Interpol and LEAs (Law Enforcement Agencies), will also have an important interest in being able to use data related to money laundering, terrorist and criminal financing activities.

Such a network for exchanging data on risks such as the fight against money laundering and the fight against terrorist financing would be much more appropriate to the current challenges, considering that these risks do not stop at the borders of Member States.

Privacy Preserving Verifiable Credentials
The bank customers (the payers and the payees) as well as the trust intermediaries such as the banks and the PSPs (AISPs, ASPSPs, PISPs).

Open Banking API Architecture
European banks and third service providers will have an economic interest in the architecture network. In particular, banks are able to easily connect other APIs in the market in order to extend their service offerings by introducing native FinTech solutions in a secure plug-and-play manner. Through embracing the Open Banking API economy, banks are able to further enhance and transform current offerings, increasing their appeal to existing and prospective customers alike. However, Open

Banking APIs can also create a threat for banks, as they enable FinTech firms to tap into a bank's financial data. For example, a FinTech startup may decide to use a bank's "Customer Data API" in order to build a mobile application where customers budget their finances, manage their debt, and get real-time investment and financial advice through chat. The majority of traditional banks do not offer such debt and real-time finance management services. This means that by opening up their APIs, the bank has enabled the FinTech startup to fulfill this existing gap and drive a wedge between the bank and the customer.

3.3 Actors

In this section we provide a list of actors with brief descriptions. Actors are all the entities that interact with the overall Financial Transactions ecosystem. They can be of two types:

(i) Primary actors, which are actors that have goals which this demonstration case needs to fulfill; and

(ii) Secondary actors, which don't have specific goals associated with this demonstration case but are needed for the execution of its use cases.

3.3.1 Primary

The actors involved in these use cases are:

- **Commercial/Corporate / Retail Banks**: these banks transact with customers, play a direct part in settlements and are regulated by a national central bank. This category includes:
  - **Settlement banks** which are the last banks to receive and report the settlement of a transaction between two entities;
  - **Internet banks** — also known as virtual banks, online banks, or web banks — lack any physical branch locations and exist only on the Internet;
  - **Account Service Payment Service Providers (ASPSP)** when referred to as a bank by PSD2.
- **Service Providers**: PSD2 introduced two new payment services provided by new actors.
  - **Payment Initiation Service Providers (PISPs)** initiate online payments to third parties on behalf of the payers. These entities, which do not have necessarily a relationship with the payers' banks (ASPSPs), may access the online account of the payers;
  - The **Account Information Service Providers (AISP)** allow users to get a consolidated view on all their payment accounts even if they are managed by multiple ASPSPs.
- **European Payment Council (EPC)**: the decision-making and coordination body of the European banking industry in relation to payments, consisting of banks and their associations, with responsibility for the development of the Single Euro Payment Area (SEPA);
- **European financial governance bodies**: for example, the European Banking Authority (EBA);
- **Europol**: the law enforcement agency of the EU that handles criminal intelligence and combats serious international organized crime and terrorism through cooperation between competent authorities of EU Member States;
- **Regulatory and privacy bodies**: for example, the European Data Protection Board (EDPB), as well as the Data Protection Authorities (DPAs), the agencies responsible for overseeing the GDPR within each Member State;
- **Identity verification service providers:** These are organisations that verify customer credentials (e.g. ID Now);
- **Credit rating agencies:** These are organisations that provide credit risk assessments (e.g. Schufa in Germany);
- **Customers**: Users of the system who apply for a service (e.g. bank account) and are part of the onboarding process.

3.3.2 Secondary

- **Consultancy agencies**: audits and certifies the supply chain process in settlement transactions. Also those providing services to financial institutions;
- **Government agencies**: governmental entity that interacts with the flow of money entering/leaving a country (e.g., treasury, customs office, etc.);
- **ICT and equipment providers**: providing others with tools to carry out their operations (e.g., IT companies) and some of the needed technologies to implement the targeted fraud network;
- **Open Banking pure players**: these include Fintech companies;
- **End users**: these include bank customers or open banking service users;
- **Fraudsters, hackers, mischief makers, malicious users, bored teenagers**: the list is endless.

3.3.3 Use Cases Numbers

ACTORS	OB-UC1	OB-UC2	OB-UC3	OB-UC4
Banks	X	X	X	X
Service providers	X		X	X
EPC		X		
Europol		X		
Governance bodies		X		
Regulatory bodies		X		

Table 1: Open Banking - Mapping of actors to use cases

3.4 Functional Requirements

In this section we provide a brief description of the functionalities of this demonstration case, along with a list of use cases implementing them.

3.4.1 Overview of Functionalities

3.4.1.1 Sharing of Identity Verification and Fraudulent Activity

The blockchain-based system will have the following functionalities and benefits

- **Shared Distributed Ledger:** A tamper-resistant distributed ledger with no single point of control used for sharing the results of customer due diligence and fraudulent activity
- **Confidentiality and Privacy:** Personal identifiable information is never stored on the Blockchain. Only metadata consisting of commitments or hashes are recorded on the blockchain and shared across multiple financial institutions. The confidentiality also extends to banks and financial institutions where no sensitive business information is recorded. Customers are always be in control of their personal data and consent to sharing personal data and outcomes of processes such as KYC
- **Scalability:** Existing blockchains transaction processing speed is vastly inferior to the transaction processing requirements of modern financial systems. The proposed solution is designed to scale and meet modern banking throughput requirements

- **Governance**: A blockchain is a decentralized system that removes the need of a trusted third-party overseeing its operations. However, banks and institutions can exert a certain degree of control over their systems and networks to enforce business logic and policies.

3.4.1.2 OBSIDIAN

The proposed network will focus on four core functionalities:

1. Banks experiencing potential fraud attempts will request confirmation of the right decision to take (i.e., monitoring / rejecting / validating the transactions) from the proposed network. The requests provide the core transaction data (IBAN et al) in a format which guarantees privacy and security network requirements.
2. Banks must confirm transactions for which the quality of the user experience (real time, trust) is critical. In order to succeed in providing such a user experience, banks should request the proposed network to gain the needed quality.
3. In its daily fight against money laundering, banks' security experts should cooperate with the network expert ecosystem in order to provide their fraud fight models with extended qualified data to improve global detection skills.
4. In their ongoing fight against the financing of terrorism and criminal activities, open banking actors will use the proposed network to share their cases analysis in order to create the conditions to build some global detection patterns and improve their response times when facing new incidents.

3.4.1.3 Privacy Preserving Verifiable Credentials

To address some of the security considerations in realising PSD2, the focus will be on the core functionalities associated with the role of verifiable credentials in the following transactions and flow:

1. A user wants to get a complete picture in a single view of their financial world from personal current and saving accounts to pensions, insurance, mortgage and investments, which are distributed across three countries. The user, like many others, is accustomed to carrying out most of their bank transactions on their mobile phone.

2. The user wants to make a payment to a merchant by giving them access to one of their bank accounts. The user then wants to allow the merchant to process a payment through an intermediary service with access to their bank account.

3. The user decides that they want to terminate its relationship with the merchant and no longer wants to allow them to have access to their bank account. At the same time, the user decides they would like to work with a third party to transfer all their account information to another financial institution.

The core components that this use case relies on are FIDO2 and the W3C work on verifiable credentials:

- The goal of the **FIDO2** Project is to standardise an interface for authenticating users to web-based applications and services using public-key cryptography. FIDO2 consists of the W3C Web Authentication (**WebAuthn**) standard and the FIDO Client to Authenticator Protocol (CTAP). Taken together, WebAuthn and CTAP specify a standard authentication protocol where the protocol endpoints consist of a user-controlled cryptographic authenticator (such as a smartphone or a hardware security key) and a WebAuthn Relying Party (also called a FIDO2 server). A web user agent (i.e., a web browser) together with a WebAuthn client form an intermediary between the authenticator and the relying party. A single WebAuthn client device may support multiple WebAuthn clients.

- The **W3C VC** places the holder of a credential at the centre of the identity ecosystem, giving individuals control of their identity attributes. This contrasts with the federated identity management (FIM) model, as adopted by SAML and OpenID Connect, which places the identity provider (IdP) in the central role as the dispenser of identity attributes and the determiner of which service providers (SPs) it will give them to. In the federated model a user's privacy is violated, since the IdP knows every SP that the user visits. The **W3C VC** model, on the other hand, parallels the way identification cards are used today: the user holds plastic cards in their wallet, and can present them to anyone at anytime without requiring the permission of the card issuer. Such a model is decentralised and gives much more autonomy and flexibility to the participants. The W3C VC standard defines the syntax and semantics of Verifiable Credentials. Many different protocols are being specified for carrying VCs from the issuer/IdP to the holder, and the holder to the verifier.

3.4.1.4 The Open API Architecture

The architecture, as described in Figure 1, identifies five basic areas within the defined macro-components for the Open API, which represent the main elements that contribute to the dynamics of exposure and governance of the Open Banking stakeholders.

- **API Security**: Components useful for ensuring the necessary security features for interaction with the Open Banking Architecture (OBA) including **Identity Provider.**
- **API Platform**: Components with responsibility for orchestration, policy enforcement, monitoring and aid to the government including the **API Gateway**, **API Manager** and the **API Portal**
- **Knowledge Base**: Collection, organization and distribution of knowledge through the API Catalogue and Documentation Management
- **Baseline**: Components constituting the reference point on which the implementation of the Open Bank is based
- **Ecosystem**: Open banking implies the use of external services, data and features developed by parties outside the bank.

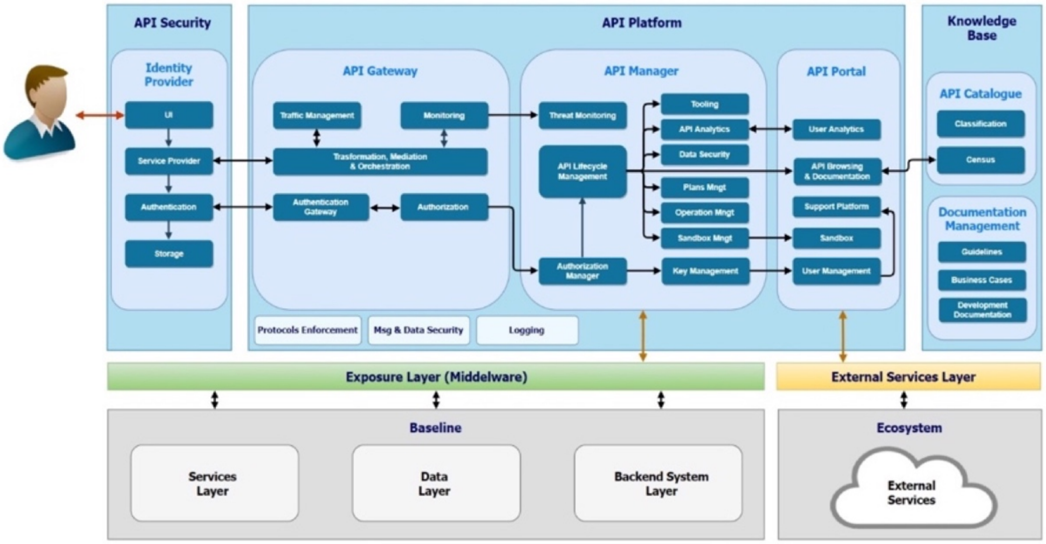


Figure 1: Open Banking - The Open Banking API architecture

3.4.2 Use Case List

- **OB-UC1 - Sharing of Identity Verification and Fraudulent Activity:** This use case describes a system for sharing data between banks without the reliance on a trusted party.
- **OB-UC2 – OBSIDIAN**: consists of four components:
  - **Posting fraud information to the network**: The preparation, reporting and scoring of fraud information as well as facing such an attempted fraud and dealing with false positives.
  - **Establishing user experience trust levels**: The preparation and reporting of effective information on institutional IBANs (white list IBAN) for publication and defining access authorization to the information.
  - **Network access to data and money laundering information**: The preparation and reporting of money laundering information and defining access authorization to that data.
  - **Sharing terrorist financing information in the network**: The preparation and reporting of information related to terrorist financing and defining who and under what circumstances access to that data is authorized.
- **OB-UC3 - Privacy Preserving Verifiable Credentials**: The recognition of customers' entitlement to a high level of security in mobile banking that is compliant with the requirements of the GDPR.
- **OB-UC4 – Open API Architecture:** consists of three components:
  - **Illegal access to the system**: A hacker / malicious user tries to gain illegal access to the system.
  - **Unauthorized information change**: A hacker / malicious user tries to tamper with the data.
  - **Unauthorized escalation of privilege**: A hacker / malicious user tries to gain unauthorized access to information.

3.4.3 OB-UC1 – Sharing of Identity Verification and Fraudulent Activity

This use case aims at investigating efficient ways to create a trust-minimized data sharing platform using blockchain technology. A blockchain has certain unique properties that differentiate it from centralized or distributed databases. These properties are described as follows:

- **Shared record keeping**: All stakeholders share a record of transactions without relying on a central entity
- **Multi-party consensus**: All stakeholders come to an agreement on the recorded data
- **Tamper-resistance**: No single stakeholder can unilaterally alter the records.
- **Secure smart contracts**: Automate processes (e.g. identity verification/ validation) and share recorded outcome

Combined together the above properties provide a shared trust-minimized ledger with high data integrity and consistency. Without using a blockchain, the stakeholders would need to rely on a trust framework or centralized system for information sharing.

3.4.3.1 Use Case Diagram

Figure 2 depicts a scenario that is greatly simplified for the purpose of clarity, that is, the number of entities involved and their interactions is limited.

The blockchain architecture:

- Enables customers to register and create unique digital identities
- Allows for the deployment of smart contracts, records the results of customer due diligence, and enforces specific financial policies.
- Records customer consent to share data between partner banks and institutions

3.4.4 **OB-UC2 – OBSIDIAN**

Posting fraud information to the network

There are six stages to this use case:

(1) Preparing effective fraud information in order to post it to the network describes a set of tasks to be completed by a network member in order to convert the data about a fraud she has experienced in her context in a format sharable with other members of the network (anonymization, certification).

(2) Reporting fraud information in the network is the process used by a member of the network to report to the network the data computed at the first stage.

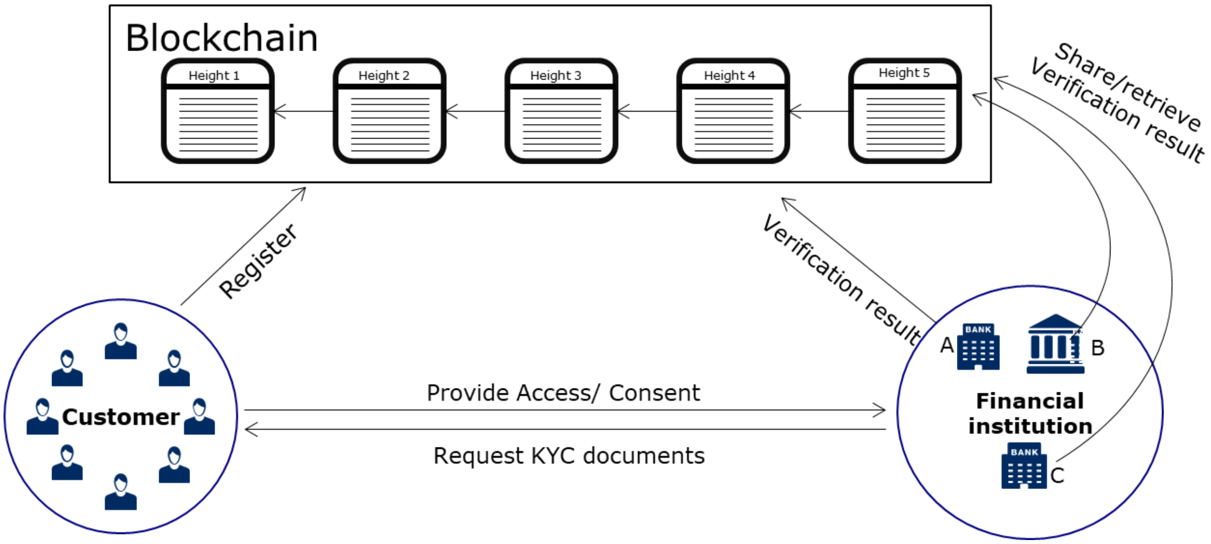


Figure 2: Open Banking - Simplified view of a blockchain based data sharing infrastructure

(3) Scoring a transaction with information provided by the network is the process used by a member of the network to request the network to score the data (IBAN et al) used in a transaction.

(4) Facing a fraud confirmed by information provided by the network describes the actions performed by a network member when he detects an effective fraud which is confirmed by information provided by the network. These actions include updating network information based on the new fraud case.

(5) Dealing with a false positive provided by the network describes the actions performed by a network member when he experiences a false positive when scoring a given transaction with information provided by the proposed network.

(6) Defining precise rules for data and fraud network access describes exactly and in what context an entity is authorized to access the proposed network. It also defines the technical authorization system put in place to restrict access. Finally, it defines which interlocutors within the entity are authorized to access the data.

Establishing Quality User Experiences

There are three stages to this use case:

(1) Preparing effective information on institutional IBANs (white list IBAN) for publication on the network describes a set of tasks performed by a network member to convert data on institutional IBANs known to it into a format that can be shared with other network members (anonymization, certification, etc.) in order to help partners reduce the number of false positives they detect in the fight against fraud.
(2) Reporting institutional IBANs information in the network is the process used by a network member to report to the network the data computed in UC10.
(3) Defining exact rules for data and institutional IBAN network access describes precisely and in what context an entity is authorized to access the network. It also defines the technical authorization system put in place to restrict access. Finally, it defines which interlocutors within the entity are authorized to access the data.

Network Access to Data and Money Laundering Information

There are three stages to this use case:

(1) Preparing effective information on money laundering for publication on the network describes a set of tasks performed by a network member to convert the money laundering data it detects into a format to be shared with other network members (anonymization, certification, etc.).
(2) Reporting money laundering information in the network is the process used by a network member to report to the network the data computed in (1)
(3) Defining precise rules for data and money laundering network access describes exactly and contextually an entity is authorized to access the network. It also defines the technical authorization system put in place to restrict access. Finally, it defines which interlocutors within the entity are authorized to access the data.

Sharing Terrorist Financing Information in the Network

There are three stages to this use case:

(1) Preparing effective information on terrorist financing for publication on the network: this use case describes the different tasks performed by a network member to convert the terrorist financing data it detects into a format shared with other network members (anonymization, certification, etc.).
(2) Reporting terrorist financing information in the network: this use case describes the process used by a network member to report to the network the data computed in UC14.
(3) Defining exact rules for data and terrorist financing network access case describes precisely and contextually an entity is authorised to access the network. It also defines the technical authorization system put in place to restrict access. Finally, it defines which interlocutors within the entity are authorized to access the data.

3.4.5 OB-UC3 – Privacy Preserving Verifiable Credentials

This use case recognises customers’ entitlement to a high level of security in mobile banking that is compliant with the requirements of the GDPR. The intention is to use verifiable credentials protect users’ data and privacy down to the attribute level. Current approaches using FIMs fail to provide that level of protection and security and the use case will take the following approaches to demonstrate the importance of being able to use verifiable credentials.

(4) Users are in control of the use of their verifiable credentials, whereas the FIM IdPs are in control of the users' identities i.e. users can present verifiable credentials to whichever verifier will accept them, whenever they wish, whereas FIM users can only present their identity attributes to SPs that the IdP is willing to trust. IdPs are usually not willing or able to release all the user attributes that SPs require for fine-grained authorization.

(5) Since no single FIM IdP is the authoritative source of all a user's identity attributes, this necessitates the pulling of user identity attributes from other attribute authorities. In order to solve this 'attribute aggregation' problem, the assignment of a persistent globally unique identifier to each user is proposed by many. But this has privacy implications for the user, as it provides a correlating handle that can be used to track the user everywhere. Verifiable credentials allow a user to present multiple credentials from multiple issuers as required by the verifier, without the need for a globally unique identifier.

(6) Verifiable credentials provide "least privileges" because the user only reveals to the SP those identity attributes that are necessary for the required service at the time of access, whereas with FIM systems, all the user's identity attributes are presented at login time, before the actual service has been chosen.

(7) Verifiable credentials are more privacy protecting. FIM IdPs know which SPs the user is visiting and when, which allows IdPs to track users in violation of their privacy. Verifiable credentials stop the issuer from tracking users' movements. Furthermore, verifiable credentials provide "selective disclosure" so that the user only needs to reveal part of a verifiable credential e.g., only the date of birth from a driving licence.

(8) Verifiable credentials are more secure. FIM systems facilitate phishing attacks, whereby an untrustworthy SP redirects the user to a masquerading IdP, which then steals the user's authentication credentials. Verifiable credential ecosystems are not open to phishing attacks because there is no redirection, and there are no usernames and passwords to be phished. The recent Facebook hack highlights another security weakness with FIMs. If an IdP is compromised, it allows the attacker to login to every trusted SP where the user has an account. Finally, because most FIM IdPs issue bearer assertions or tokens, they can be stolen and used by an attacker. VCs on the other hand use cryptographically secured credentials that attackers cannot use.

(9) Verifiable credentials make verifiers (SPs) compliance with GDPR [8] easier as follows:
- Clause 6(1)(a) – the data subject has given consent by sending his/her verifiable credentials;
- Clause 7(1) – the verifier can demonstrate consent because the set of verifiable credentials is signed by the user;
- Clause 6(1)(b) – the verifier requests only those verifiable credentials that are necessary for performing the contracted service with the data subject;
- Clause 5(1)(c) – the requested verifiable credentials are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
- Clause 5(1)(d) – the verifiable credentials are accurate and up to date;
- Clause 5(1) (f) – verifiable credentials are cryptographically protected and can be processed in a manner that ensures appropriate security of the personal data;
- Clause 11 – the verifier does not require the identification of the data subject (but only the attributes necessary for the service).

A use case illustrating the role of verifiable credentials in opening a bank account is shown inFigure 3, and the benefits on the key actors in Figure 4.

3.4.5.1 Use Case Diagram

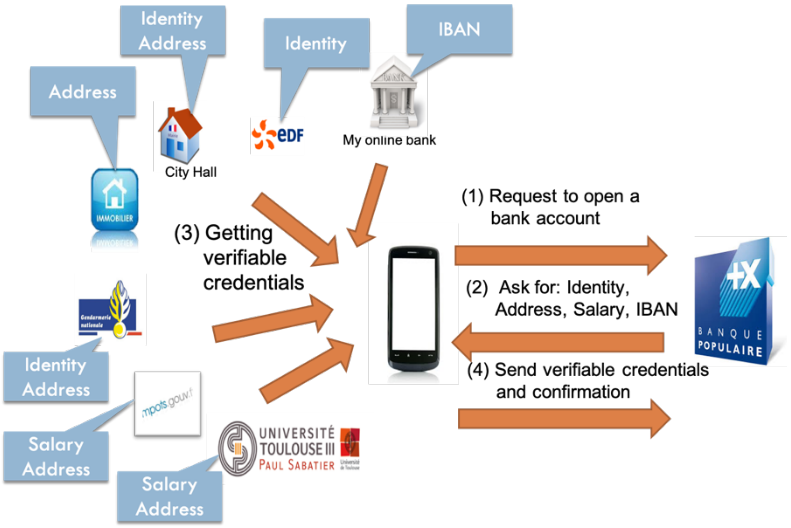

Identity
Address
Identity
IBAN
Address
City Hall
My online bank
IMMOBILIER
(1) Request to open a bank account
(3) Getting verifiable credentials
(2) Ask for: Identity, Address, Salary, IBAN
(4) Send verifiable credentials and confirmation
BANQUE POPULAIRE
Identity
Address
Salary
Address
Salary
Address
UNIVERSITÉ TOULOUSE III PAUL SABATIER

Figure 3: Open Banking – Opening a bank account with verifiable credentials

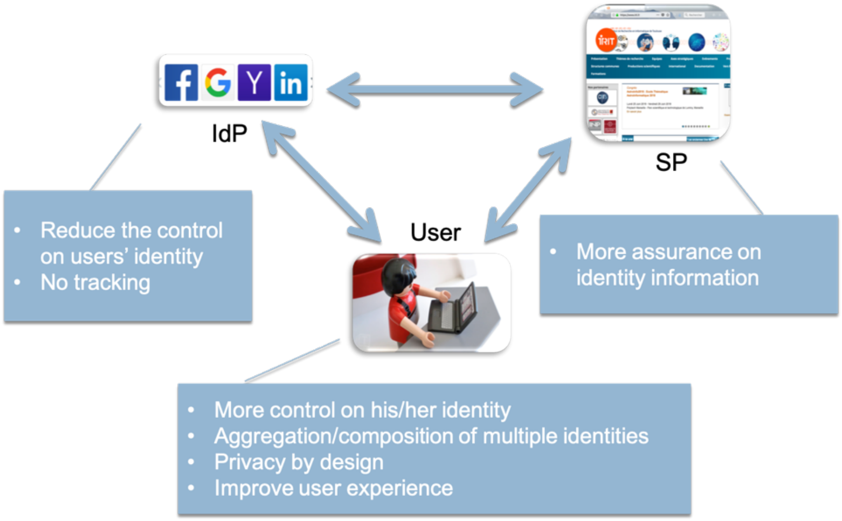

IdP
SP
User
Reduce the control on users' identity
No tracking
More assurance on identity information
More control on his/her identity
Aggregation/composition of multiple identities
Privacy by design
Improve user experience

Figure 4: Open Banking - The goal of verifiable credentials

3.4.6 OB-UC4 – Open Banking API Architecture

Illegal Access to the System

The use case, as shown in Figure 5, aims to find ways to prevent a hacker or a malicious user from targeting the Identity Provider, API Manager or the API Portal of the Open API architecture using the interfaces and communication channels with a view to gaining illegal access to the system by spoofing is identity or using MITM attacks.

3.4.6.1 Use Case Diagram

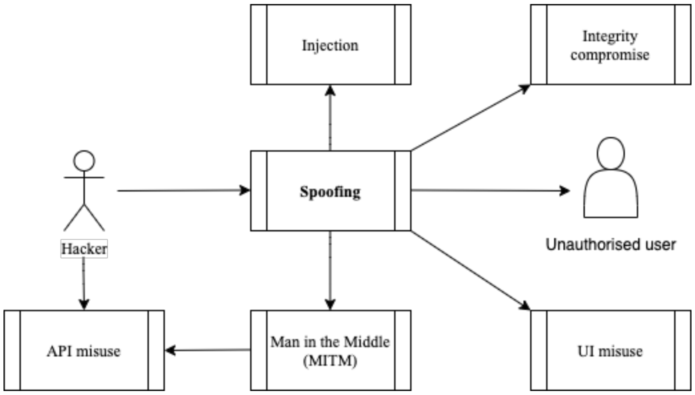


Figure 5: Open Banking - Workflow of an illegal access to the system

Unauthorized Information Change

The use case, as shown in Figure 6, aims to find ways to prevent a hacker or a malicious user from targeting the API Gateway or the API Manager of the Open API architecture using data stored in transit with the intention of making unauthorized changes to the data which would then have its integrity compromised.

3.4.6.2 Use Case Diagram

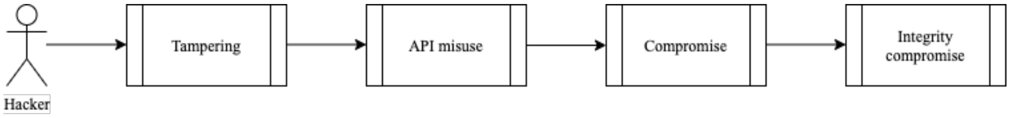


Figure 6: Open Banking - Workflow of an unauthorized information change

Unauthorized Escalation of Privilege

The use case, as shown in Figure 7, aims to find ways to prevent a hacker or a malicious user from targeting the API Gateway, the API Manager or the API Portal of the Open API architecture using the authorisation system or the development environment with the goal of making unauthorized access to functions and information with potentially privileged access to restricted resources.

3.4.6.3 Use Case Diagram

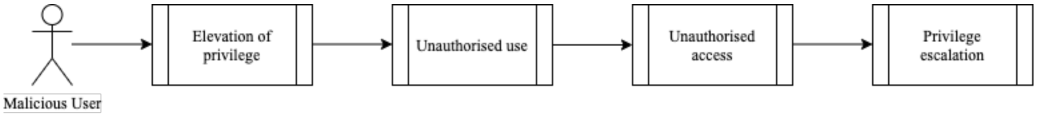


Figure 7: Open Banking - Workflow of an unauthorized escalation of privileges

3.5 Security and Privacy Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-SP01	AuthnE Id	Authentication: Actors must be authenticated and have a verifiable identity in the system	OB-UC1, OB-UC2	High	Yes
OB-SP02	IDM	Identity management: A PKI infrastructure must be in place to provide every actor with unforgeable key-pairs	OB-UC1	High	Yes
OB-SP03	AuthnM noR	Message authentication: Actors must use their digital signature to sign all transactions	OB-UC1	High	Yes
OB-SP04	CE	End-to-end security: Communications to go through secure TLS channels to provide a safe medium within the system	OB-UC1, OB-UC2	High	Yes
OB-SP05	Anon	Anonymity: Anonymisation techniques prevent the leakage of actors' sensitive information	OB-UC1	High	Yes
OB-SP06	DPriv	Privacy-preserving analytics: Actors can leverage privacy-preserving data analytics to extract information that allows them to optimize their business strategies	OB-UC1	Low	No

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-SP07	AC	Access: To provide access controls to ensure that unauthorised users cannot access the system)	OB-UC2 OB-UC4	High	Yes
OB-SP08	AuthnE	Authentication: Authentication mechanisms to be provided to ensure that unauthorised users cannot access to the system	OB-UC2 OB-UC4	High	Yes
OB-SP09	AuthnF	Federated authentication: Mechanisms to be provided to ensure that unauthorised flows cannot occur	OB-UC2 OB-UC4	High	Yes
OB-SP10	AuthnF	Federated identity: Controls to be provided to ensure that unauthorised flows cannot occur	OB-UC2 OB-UC4	High	Yes
OB-SP11	AC	Non-bypassable login function: To avoid changes of login page (e.g. fake forms) to exfiltrate data	OB-UC2 OB-UC4	High	Yes
OB-SP12	Conf	Encryption: To avoid clear storage of sensitive data.	OB-UC2 OB-UC4	High	Yes
OB-SP13	AC	Key-based authorisation: Controls to be provided to ensure that unauthorised flows cannot occur.	OB-UC4	High	Yes
OB-SP14	SC	Access rules & permissions: Systems to be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes
OB-SP15	AC	Access control: Systems to be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-SP16	Conf	Encryption: To provide controls to prevent confidentiality compromises.	OB-UC4	High	Yes
OB-SP17	Acc	Log protection: Controls to be provided to prevent unauthorized actions from being hidden.	OB-UC2 OB-UC4	Medium	No
OB-SP18	SSDLC	S-SDLC: Measures to be provided such that only authorised changes are made to the configuration items in the CMS	OB-UC4	High	Yes
OB-SP19	SDLC	Security policy configuration: Measures to be provided such that only authorised changes are made to the configuration items in the CMS	OB-UC4	High	Yes
OB-SP20	SDLC / IDM	Key lifecycle management: Controls to be provided to ensure that unauthorised users cannot access the system	OB-UC2 OB-UC4	High	Yes
OB-SP21	SDLC	Security policy configuration: Systems to be designed and implemented so that the security features cannot be bypassed to reduce the likelihood that accidental or unauthorised modifications will occur.	OB-UC2 OB-UC4	High	Yes
OB-SP22	SDLC	Security policy configuration: To provide a formal proof that a system cannot reach a non-secure state for all designed policies	OB-UC2 OB-UC4	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-SP23	Resil	Data protection rules: Security functions to be designed and implemented so that a system is able to protect itself from untrusted active entities.	OB-UC4	High	Yes
OB-SP24	Inte	Hashing: Controls to be provided to prevent integrity compromises.	OB-UC4	High	Yes
OB-SP25	Acc	Log protection: Controls to be provided to prevent unauthorized actions from being hidden.	OB-UC4	Low	No
OB-SP26	Acc	Least privileges: To provide least privileges, integrity protection, high availability, high security, and prevent phishing attacks (for example, using verifiable credentials)	OB-UC2 OB-UC3	High	Yes
OB-SP27	Conf	Selective disclosure: To provide selective disclosure and stop an IdP from tracking a user and also help stakeholders conform to GDPR (for example, by using verifiable credentials)	OB-UC3	High	Yes
OB-SP28	Trust policies	Trust model: Simple trust models to be employed whereby verifiers unilaterally decide who they will trust to issue verifiable claims - in order that issuers do not need to trust verifiers and are not required to know who the verifiers are (for example, by using verifiable credentials)	OB-UC3	High	Yes

Table 2: Open Banking - Security and privacy requirements

3.6 Non-Functional Requirements

3.6.1 Look and Feel Requirements

A number of the look and feel requirements are also listed under security and privacy requirements and are cross-referenced below.

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-LF01	Client Interface	Client interface allows actors to easily interact with the blockchain to manage their respective organisation's operations	OB-UC1	High	Yes
OB-LF02 (OB-SP12)	Encryption for data storage	To avoid storage of sensitive data in the clear.	OB-UC2 OB-UC4	Medium	Yes
OB-LF03 (OB-SP14)	Access rules & permissions for unauthorized access	The system should be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes
OB-LF04 (OB-SP15)	Access control for unauthorized access	The system should be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes
OB-LF05 (OB-SP23)	Data protection rules for confidentiality compromise	The security functions should be designed and implemented so that the system is able to protect itself from untrusted active entities access.	OB-UC4	High	Yes

Table 3: Open Banking - Look and feel requirements

3.6.2 Usability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-U01	Error Reporting	The system reports errors and security breaches timely and automatically.	OB-UC1, OB-UC2	High	Yes
OB-U02	Open banking usability	The proposed network will be expected to support open banking usability characteristics, including	OB-UC2	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		real time and high availability requirements.			
OB-U03	Verifiable credentials	Verifiable credentials remove the need for users to have countless user names and passwords, to carry physical credentials around with them, and to enter identity attributes and credit card details manually into websites.	OB-UC3	High	Yes

Table 4: Open Banking - Usability requirements

3.6.3 Operational Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-OP01	Throughput	The system must be able to process tens of thousands of transactions per second.	OB-UC1	High	Yes
OB-OP02	Byzantine Fault Tolerance	The system must be resilient to byzantine faults. It should continue its operations even if multiple banks are offline because of hardware failures or malicious attacks.	OB-UC1	High	Yes
OB-OP03	Scalability	The system must be able to scale to a significant number of nodes to allow several banks in a single country, or in a regional alliance (APAC), to join the same network.	OB-UC1	High	Yes

Table 5: Open Banking - Operational requirements

3.6.4 Maintainability and Portability Requirements

No maintainability and portability requirements have been identified at this point.

3.6.5 Social and Political Requirements

No social and political requirements have been identified at this point.

3.6.6 Legal and Regulatory Requirements

A number of the legal and regulatory requirements are also listed under both look and feel as well as security and privacy requirements and are cross-referenced below.

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-LR01	GDPR compliance	The system must handle data in full compliance with the GDPR.	OB-UC1 OB-UC2 OB-UC3	High	Yes
OB-LR02	Fraud protection	The system must provide protection against financial fraud.	OB-UC1 OB-UC2	High	Yes
OB-LR03	Encryption for data storage (OB-LF02/OB-SP12)	To avoid storage of sensitive data in the clear.	OB-UC2 OB-UC4	High	Yes
OB-LR04	Access rules & permissions for unauthorized access (OB-LF03/OB-SP14)	The system should be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes
OB-LR05	Access control for unauthorized access (OB-LF04/OB-SP15)	The system should be designed and implemented so that the security features cannot be bypassed.	OB-UC2 OB-UC4	High	Yes
OB-LR06	Data protection rules for confidentiality compromise (OB-LF05/OB-SP23)	The security functions should be designed and implemented so that it is able to protect itself from untrusted active entities.	OB-UC2 OB-UC4	High	Yes
OB-LR07	Data sharing	Some European countries (Austria, Switzerland, France) must respect the **bank secrecy** principle. Data sharing will have to use a format compatible with national legislations.	OB-UC2	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
OB-LR08	GDPR compliance	The EDPB will have to be engaged in the build phase in order to validate data sharing.	OB-UC2	Medium	Yes
OB-LR09	GDPR compliance	Verifiable credentials make verifiers' GDPR compliance easier regarding clauses 5(1)(c)(d)(f), 6(1)(a)(b), 7(1) and 11.	OB-UC3	High	Yes

Table 6: Open Banking - Legal and Regulatory requirements

3.7 Mandated Constraints

No mandated constraints have been identified at this point.

3.8 Relevant Facts and Assumptions

3.8.1 **Facts**

No relevant facts affecting the system have been identified at this point.

3.8.2 **Assumptions**

No assumptions about the system have been identified at this point.

3.9 Related WP3 and WP4 Tasks

WP3 defines all common research related to the development of technologies that are leveraged in the demonstration use cases. Here are some tasks of WP3 that provide techniques that are useful for the Open Banking demonstrator.

- **T3.2: Research and integration on cybersecurity enablers and underlying technologies.** This task is the most relevant to task 5.1 as one of the common baseline technologies to be investigated are the ones related to identity management and authentication solutions over multiple non-federated providers solutions (verifiable credentials) as well as distributed access control using blockchain.
- **T3.5: Adaptive security.** This task investigates the development of flexible security solutions that can quickly adapt security controls in response to security changes such as new attacks or changes in security requirements which could be relevant in each of the four use cases.
- **T3.6: Usable security.** This task is also concerned about mechanism to support users` privacy mechanism and as such enabling effective and usable security controls of user attributes, which could resonate with the verifiable credentials use case.
- **T3.7: Regulatory sources for citizen-friendly goals.** The purpose of this task is to design best practices for innovative and GDPR compliant user experience and to investigate the compliance for identity technologies interoperability, as well as the legitimacy of technologies used and processing of personal data in cross-border and cross-sector. This could be pertinent to all four use cases.

- **T3.8 Conformity, Validation and Certification.** This task analyses technologies, system designs and implementations to determine whether the combination of cybersecurity technologies in use achieve the desired security goals, allowing to compare different systems. The task will design a security framework capable of formally defining cyber-physical attack incidents, detecting an intrusion at different levels (physical or cyber), provide a resiliency policy and generate a forensics analysis – all of which could resonate with all four use cases.
- **T3.9 Continuous Scouting.** This task seeks to identify game-changing innovative approaches that are an essential component of innovative Open Banking applications.
- **T3.10 Impact on Society.** This task intends to advance a novel security awareness conceptual model with continuous enhancements is very relevant to the significant changes in Open Banking that are impactful on all citizens – inasmuch as all citizens are highly susceptible to any changes in the changes to the processing of financial transactions.

WP4 is the bridge between WP3 and WP5, and although there is one task that specifically correlates with Task 5.1, there are synergies in other areas when addressing long term roadmap issues. Task 5.1 will contribute to the following WP4 activities:

- **T4.1: Vertical stakeholders' engagement and consultation.** This task is the general roadmap design and applies to all of the tasks in WP5
- **T4.4: Roadmap for industrial challenge 5.1.** This task is the one that is directly related to the output from task 5.1
- **T4.5: Roadmap for industrial challenge 5.2.** This task addresses the roadmap challenges for the management of supply chains, which is a key aspect of the Settlements use case
- **T4.6: Roadmap for industrial challenge 5.3.** This task which is focused on privacy-preserving identity management has a direct correlation with the verifiable credentials use case
- **T4.7: Roadmap for industrial challenge 5.4.** This task involves the challenges associated with incident reporting, particularly in the finance community, which resonates with the OBSIDIAN use case

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3		✓	✓	✓		✓	✓	✓	✓	✓
WP4	✓			✓		✓	✓			

Table 7: Open Banking - Relationship with WP3 and WP4 tasks

4 Supply Chain Security Assurance

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled *Supply Chain Security Assurance*.

This chapter is organized as follows: we first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

4.1 Goals

The demonstration case reflects the need to secure a crucial ongoing transformation in the manufacturing industries: the integration of information technologies (IT) with the existing operational technologies (OT) [Che17, Lop17, Lu17]. The purpose of this digitalisation of the value chain is the optimization of processes in terms of production costs, delivery services, and quality assurance under the customized interaction of new stakeholders such as customers or end consumers [Che17,Lu17].

Under this commitment to digitise and interact with diverse entities, new security challenges arise [Tup18], for example: the secure interconnection of IT-OT networks [Alc19], the influence of the new technologies in the operation processes, and the tracking, auditing and accountability of all processes and entities involved in the value chain. The value chains present different criticality levels according to the product, [Lop17]: “It is not the same to protect […] the construction of a bicycle, as [to secure the production of] a plane or a train”. Attacks against the supply chain can be very devastating, as the whole integrity of the manufactured product is at risk. Without proper security, these kinds of attacks are deemed to increase in number and impact over the next years.

4.2 Stakeholders

The main stakeholders in this demonstration case are:

- The **manufacturer** of a good, which wants to optimise his processes, reduce costs, and have a better overview of the exact state of the supply chain in order to act on time to any problem that could appear. A very similar role is played by the Engineering, Procurement, and Construction contractor (**EPC**), which coordinates the construction of a system.
- The **end consumers** (or **owners**) of the produced good, for instance the operator of a critical infrastructure or an airline that buys an airplane. Since they will be responsible for the quality of the manufactured good, they are interested in verifying the quality of the goods they are buying. In case of any problem due to the poor quality or late delivery of the ordered goods they will suffer costly delays in their businesses.
- The **suppliers**, which deliver parts, components, or raw materials for the production. They are interested in their parts being available on time for production and that the main manufacturer or the product owner accepts them as a reliable partner.
- The **Supervisory Agency (Authority)** must understand the root causes of incidents (say accidents in a plant, in a train or airplane or in a hospital) or of complaints about the poor quality of goods. This agency has the authority to judge on accountability and liability issues, including the compliance of production with required standards and to take measures against a non-compliant entity.

- The **notified body (NoBo)** is a governmental entity that monitors the construction of the product and is notified about the single compliance-relevant steps during the process.

4.3 Actors

In this section we provide a list of actors with brief descriptions. Actors are all the entities that interact with the supply chain ecosystem. They can be of two types: (i) Primary actors, which are actors that have goals which this demonstration case needs to fulfil; and (ii) Secondary actors, which don't have specific goals associated with this demonstration case, but are needed for the execution of its use cases.

4.3.1 Primary

Actors who, at some point along the supply chain, have an ownership stake of the good:

- **End Consumer**: owner of the final good with own criteria to customise and improve production processes. In the case of industrial products, he/she is often also the main responsible for the quality of the final product.
- **Store**: makes goods available to end consumers.
- **Warehouse**: buys goods from manufacturers in bulk and distributes them to retailers.
- **Engineering, Procurement, and Construction (EPC) contractor**: entity responsible for all the activities from design, procurement, construction, commissioning and handover of the project or good to the end consumer or owner.
- **Manufacturer**: manufactures goods.
- **Supplier**: supplies raw materials and components to manufacturers.
- **Supervisory Agency (Authority)**: gathers information about incidents or complaints and decides on accountability and liability issues, evaluating the compliance of production steps and audit trail.

4.3.2 Secondary

Actors who do not own the goods, but play a role in the supply chain process:

- **Logistics services provider**: moves goods between primary actors (e.g., UPS, DHL, etc.)
- **Consultancy agency**: audits and certifies the supply chain process.
- **Financial institution**: processes payments.
- **Government agency**: governmental entity that interacts with the flow of goods entering/leaving the country (e.g., customs office, food safety agencies, drug agencies, etc.)
- **Notified Body (NoBo)**: governmental entity that is being notified on each main step in the design and or production and (in our simplified UCs) accepts the design and construction of the product.
- **Equipment provider**: provides other actors with tools to carry out their operations.
- **Indirect material supplier**: supplies goods that support the supply chain but are not associated with the goods produced by a given supply chain.

4.3.3 Use Cases Numbers

Table 8 maps the actors involved for each use case in the Supply Chain Security Assurance demonstrator

ACTOR	UC1	UC2
End Consumer	X	X
Store	X	
Warehouse	X	
Manufacturer	X	X
EPC		X
Supplier	X	X
NoBo		X
Supervisory Agency		X

Table 8: Supply Chain Security Assurance - Mapping of actors to use cases

4.4 Functional Requirements

In this section we provide brief descriptions of the functionalities of this demonstration case, along with a list of use cases implementing them.

4.4.1 Overview of functionalities

The integration of IT technologies and OT offers a new possibility of optimizing the supply chain in order to handle market changes in a timely manner, reduce delays, ensure to deliver just-in-time production, predict and understand problems. To obtain these improvements it is necessary to monitor process status, the performance across the production plants, transportation systems, warehouses, and to track the parts and products along the whole production and supply. Besides a faster and cheaper production, the new technologies and processes offer the possibility to verify the quality of the parts and products and the ability to demonstrate the compliance of parts and products to authorized parties. Providers and manufacturers run tests on parts, components, products, and the resulting audit protocol is signed for instance by a smart object embedded in the part and the testing equipment.
The genuineness and integrity of products, as well as the compliance with manufacturing standards is demonstrated, certification authorities can access information to verify and certify products. In case of a problem or a dispute about a problem with a product, a judge should be able to resolve the dispute and identify the root cause and the responsible entity. This is particularly interesting because some of the information is kept confidential for the normal use case.

4.4.2 Use Cases List

- **SCH-UC1 - Supply Chain for Retail**: this use-case describes a supply chain system for retail. The supply chain's flows leverage a distributed ledger to carry out their operations.
- **SCH-UC2 - Compliance and Accountability in Distributed Manufacturing**: this use case describes a supply chain system for industrial products and expands the previous use case with questions regarding the compliance of manufacturing and accountability issues.

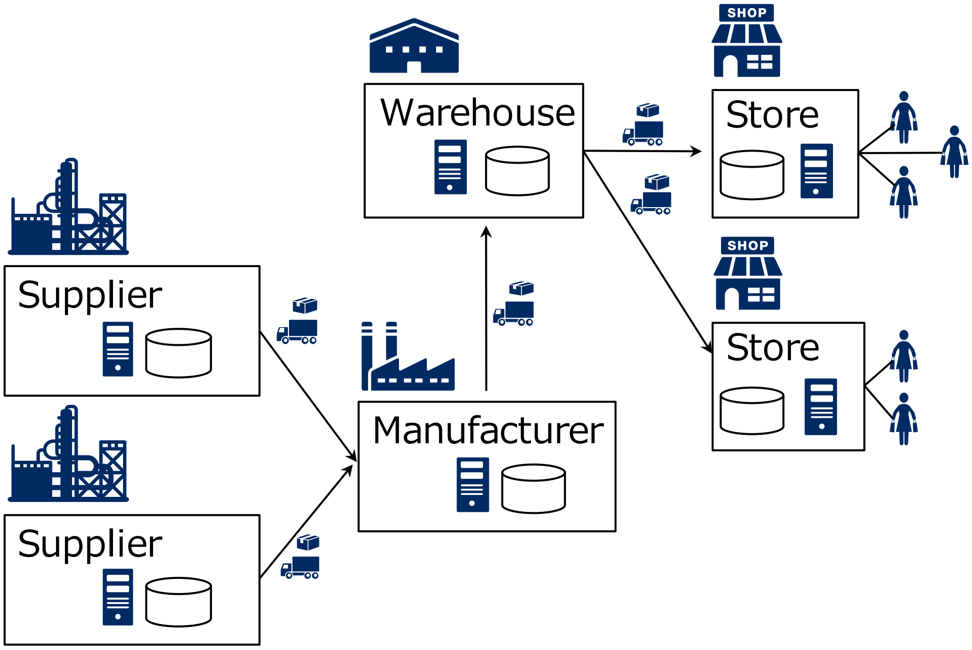
4.4.3 SCH-UC1 – Supply Chain for Retail

Supply-chains are very complex systems moving products or services from suppliers to customers. Nowadays, their complexity has reached the point where organizations can hardly keep track of what is going on at the lower levels of their supply chains. There is much that a distributed ledger can do for the supply chain ecosystem:

- Trust: a distributed ledger technology (DLT) removes the need for a trusted central organization operating and maintaining the system. It allows various players that do not necessarily trust each other, such as shipping companies, logistics and transport operators, insurers, and stores to collaborate within one common platform in order to scale-up their respective businesses.

- Digitisation: a distributed ledger can help by digitising the sales processes, facilitating payments in close to real time, and the development of legal contracts between participants. The latter can be easily done via smart contracts, that is, Turing complete programs that can be uploaded to the distributed ledger. The digitisation process drastically reduces the chance of human errors and eventually will ensure that every member has an identical view of who did what and when, thus removing database inconsistencies.
- Securing information: a distributed ledger offers a secure and highly resilient information sharing platform that is resilient to cyber-attacks by tolerating Byzantine faults in the system. Transfer of information is done via signed transactions. Since owners' signatures are unforgeable, nobody can challenge the legitimacy of any transfer. Additionally, all information is hashed before storage, making it impossible for anyone to alter it without being immediately detected.
- Counterfeiting: Goods can be associated with unique identifiers which, combined with the stored history of transactions, is a very powerful weapon against counterfeiting. The distributed ledger will store unique product identifiers and history of transfers between suppliers. In order to further ensure the genuineness of products, certification authorities can join the distributed ledger to certify products. The distributed ledger will then store the product information and additional data to verify authenticity.

4.4.3.1 Use Case Diagram



-

Figure 8: Supply Chain Security Assurance - Simplified view of a supply chain workflow

Figure 8 shows a simple supply-chain scenario featuring:

- Two suppliers supplying a single raw material
- One manufacturer producing a single type of good.
- One warehouse handling orders and distributing goods to stores as needed. Warehouses can be shared by different manufacturers.
- Two stores in different geographical location to achieve maximum coverage.

The depicted scenario is greatly simplified for the purpose of clarity, that is, the number of entities involved and their interactions are limited.

4.4.4 SCH-UC2 – Compliance and Accountability in distributed Manufacturing

A large industrial manufacturing enterprise with many suppliers or a consortium of several producers must be able to track and monitor not only the location, movements, and availability but also the ***quality*** and ***compliance*** of parts and products, and the conditions of transport or storage.

Manufacturing compliance comprises the set of technical, legal, and corporate requirements, manufacturers must fulfil in order to create and market goods in accordance with regulations and industrial practices. Compliance responsibilities of manufacturers and suppliers are growing due to the establishment of regulatory rules, directives, and supervisory bodies in different industry sectors, along with the emergence of international standards to address the global nature of manufacturing.

The risk of non-compliance has become a pressing concern in recent years, particularly for manufacturers with operations in multiple countries and jurisdictions. Compliance mechanisms and controls include audits, system validations, audit trails, electronic signatures, and documentation of development, manufacturing and testing. Such procedures must result in verifiable certifications which can be used to demonstrate compliance to a regulation such as, for example, the Machinery Directive 2006/42/EC [EU16]. Companies should increase controls over suppliers and be able to track risks and incidents down to their originating point. For this reason, suppliers are required to (1) collect design, manufacturing, and test data, (2) share them to authorities and to their customers to prove compliance. Many of these controls and modes to verify the compliance of the regulatory frameworks are also contemplated by guidelines, recommendations and standards such as "Cybersecurity Framework" [NIS18], "Best Practices in Cyber Supply Chain Risk Management" [NIS-C] and "Cybersecurity Framework Manufacturing Profile (NISTIR 8183)" [NIS17]. This latter clearly establishes the need to: "*define, implement, and enforce policy and regulations*" (PR.IP-5) and "*conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements*" (DE.DP-2).

4.4.4.1 Use Case Diagram

Figure 9 shows a simple compliance audit trail scenario featuring:

- One owner that orders a product from an EPC contractor.
- One supplier supplying components and providing evidence of tests for quality and compliance.
- One EPC / manufacturer producing an industrial good for critical infrastructure or constructing a plant.
- One supervisory agency gathering information about an incident and clearing accountability and liability issues.
- A Notified Body (NoBo) that is being notified on each main step and assesses their conformity with standards or regulations.
- An Audit Trail Data Base (or Data Bases) for accountability information.

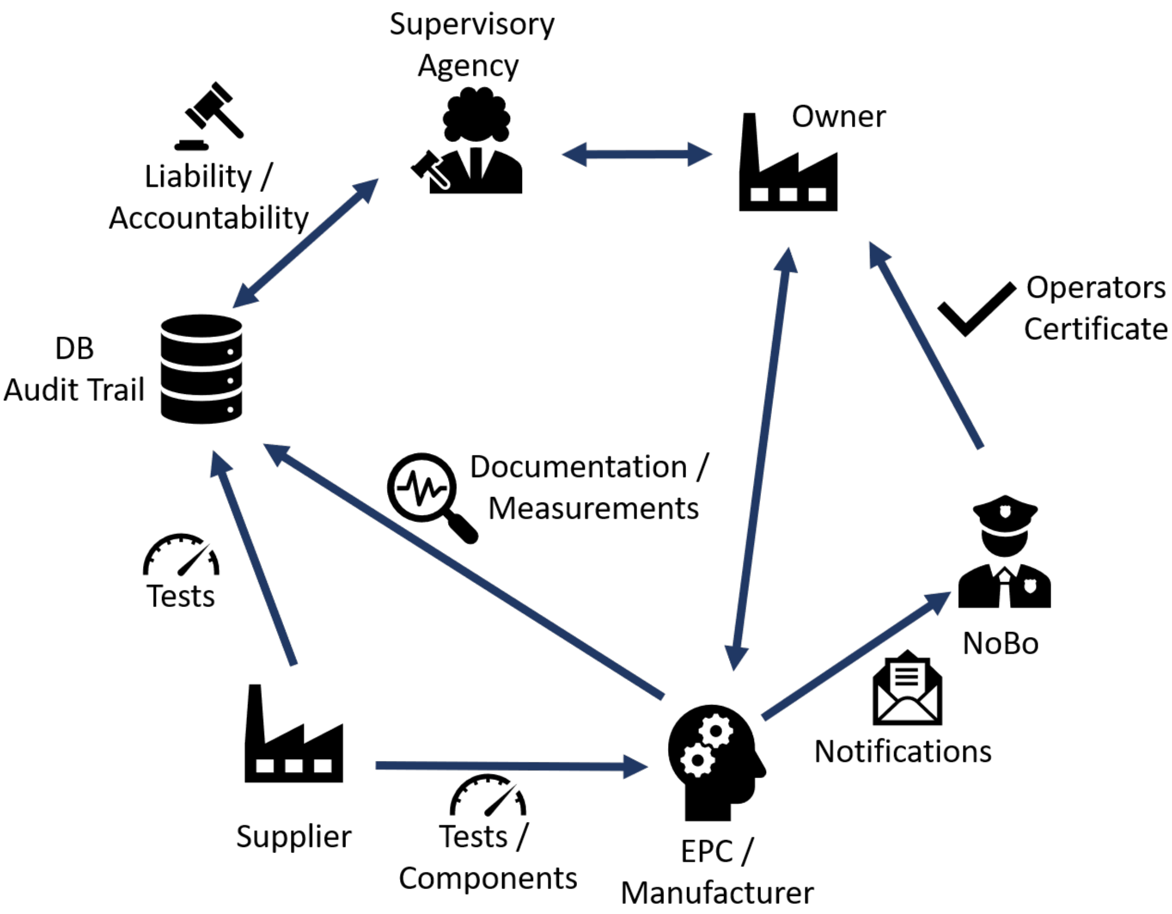


Figure 9: Supply Chain Security Assurance - Simplified view of a compliance audit trail and accountability

4.5 Security and Privacy Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-SP01	AuthnE	Actors must be authenticated and have a verifiable identity in the system.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP02	IdM	A PKI infrastructure must be in place to provide every actor with unforgeable key-pairs.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP03	AuthnM	Actors must use their digital signature to sign all transactions.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP04	CE	Data in transit has to be protected, i.e., communication	SCH-UC1, SCH-UC2	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		needs to run over secure channels.			
SCH-SP05	Conf	Sensitive data must be protected against access from unauthorized entities and the privacy of individuals involved in the production and supply process must be safeguarded.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP06	AC	The supply-chain information system should provide different levels of access and visibility. For instance, manufacturers do not want sensor data that provide information on the origin and/or the status of goods get accessible to competitors.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP07	Anon	Anonymization techniques allow actors to carry out their supply-chain operations without unveiling their identity.	SCH-UC1, SCH-UC2	High	Yes
SCH-SP08	DPriv	Actors can leverage privacy-preserving data analytics to extract information that allows them to optimize their business strategies.	SCH-UC1	Low	No
SCH-SP09	noR	Digital evidence (e.g., via digital signatures) of activities taken by actors needs to be created and maintained by the system in a way that it is tamper-proof. This requirement is a precondition for accountability, but it is often in competition or tension to confidentiality and privacy.	SCH-UC2	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-SP10	Acc	The actions taken within the entire value chain can be traced to verify their compliance with policies and regulatory frameworks. The lawful disclosure of the identities of parties suspected of not acting according to the rules or claiming false information should be provided to authorized entities.	SCH-UC2	High	Yes

Table 9: Supply Chain Security Assurance - Security and Privacy requirements

4.6 Non-Functional Requirements

4.6.1 Look and Feel Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-LF01	UI	Client interface allows actors to easily interact with the distributed ledger to manage their respective organization's operations.	SCH-UC1, SCH-UC2	Medium	Yes

Table 10: Supply Chain Security Assurance - Look and Feel requirements

4.6.2 Usability Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-U01	NoA	The system reports errors and security breaches timely and automatically	SCH-UC1, SCH-UC2	High	Yes
SCH-U02	Config	The system allows all partners to manage and configure the underlying platforms and their policies in a secure, usable, and consistent way.	SCH-UC1	Medium	Yes

Table 11: Supply Chain Security Assurance - Usability requirements

4.6.3 Operational Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-OP01	Perfo	The system must be able to process thousands of transactions per second	SCH-UC1, SCH-UC2	High	Yes
SCH-OP02	FT	The system must be resilient to byzantine faults	SCH-UC1, SCH-UC2	High	Yes
SCH-OP03	Perfo	The system's architecture must support deployments that can be scaled on demand.	SCH-UC1, SCH-UC2	High	Yes
SCH-OP04	SLog	The system must provide logging and monitoring of its operations, in order to support audit and accountability procedures.	SCH-UC1, SCH-UC2	High	Yes

Table 12: Supply Chain Security Assurance - Operational requirements

4.6.4 Maintainability and Portability Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-MP01	Avail	The system must be updated without major impact in the supply chain operations.	SCH-UC1	High	Yes

4.6.5 Social and Political Requirements

No social and political requirements have been identified at this point.

4.6.6 Legal and Regulatory Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-LR01	GDPR	The system must handle data in full compliance with the European General Data Protection Regulation (GDPR). Namely, it will only work on and store metadata needed to ensure correct operations. At no point in time the system will store users' data, thus preventing the disclosure or identification of a user's identity.	SCH-UC1, SCH-UC2	High	Yes
SCH-LR02	Func	The system must provide protection against counterfeiting.	SCH-UC1, SCH-UC2	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SCH-LR03	Func	The system must provide protection against financial fraud.	SCH-UC1, SCH-UC2	High	Yes
SCH-LR04	Transp	The system must have the means and channels to provide information to environmental agencies, United Nation Programmes, local authorities, certification organizations, NGOs or to the general public related to matters that concern the society as a whole. This information will vary depending on the particular regulations or the context of the application, but it could include information about sustainability, environmental fingerprint, labour conditions, compliance with fair trade or organic standards, etc.	SCH-UC2	High	Yes

Table 13: Supply Chain Security Assurance - Legal and Regulatory requirements

4.7 Mandated Constraints

No mandated constraints have been identified at this point.

4.8 Relevant Facts and Assumptions

4.8.1 Facts

No relevant facts affecting the system have been identified at this point.

4.8.2 Assumptions

No assumptions about the system have been identified at this point.

4.9 Related WP3 and WP4 Tasks

The security of the supply chain, as to be developed in Task 5.2, is related to several transversal security technologies and research aspects in security and privacy. Specifically, the relation to the tasks in WP3 is as follows:

- **T3.1: Common Framework Design**. this task addresses the project's lifecycle; it will formulate the realistic progress of the project, impact potential, define the feedback for the project activities and communicate and organise the progress behind the building blocks of the CyberSec4Europe ecosystem. This task will probably not provide any particular technical building blocks for Task 5.2, but will help in organizing and structuring the work.

- **Task 3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies.** This represents a very relevant task for Task 5.2, providing several of the common baseline technologies to be used for securing the supply chain. Specifically, these are: (a) Blockchain, (b) identity management, (c) PET (particularly for Anonymity, Privacy-Preserving Analytics, and GDPR compliance), (d) authentication solutions over multiple providers, (f) IoT Privacy Preserving Middleware Platform, (g) decentralized evidence-based authorization and distributed access control using Blockchain, and (h) privacy- and integrity-preserving storage and processing of critical data with long-term protection requirements.
- **Task 3.3: SDL – Software Development Lifecycle.** This task identifies research challenges, requirements and approaches in all stages of the lifecycle of software. Amongst these are mechanisms to enhance trust in pervasive infrastructures and technologies such as the IoT, cloud, fog, and edge which will be relevant for Supply Chain Security.
- **Task 3.8: Conformity, Validation and Certification.** That task studies the topics conformity, validation and certification, which will be relevant for the Use Case SCH-UC2 - Compliance and Accountability in distributed Manufacturing. Here it will be necessary to analyse the system design to determine whether the proposed architecture does achieve the desired security goals and eventually prove the security of the whole system.

In relation to WP4, Task 5.2 will interact with:

- **Task 4.1: Vertical stakeholders' engagement and consultation.** That task collects requirements for the demonstrator of Task 5.2 and receives feedback from this task for the roadmap.
- **Task 4.3: Mapping and roadmap design.** That task will provide the general roadmap design.
- **Task 4.5: Roadmap for industrial challenge 5.2.** The task is directly related to the results and the evaluation results of Task 5.2.

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3		✓	✓							
WP4	✓				✓					

Table 14: Supply Chan Security Assurance - Relationship with WP3 and WP4 tasks

5 Privacy-Preserving Identity Management

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled Privacy-preserving Identity Management. We first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumptions to be considered while implementing this demonstration case.

5.1 Goals

In an increasingly digital and inter-connected world, identity management systems offer a convenient and user-friendly way for handling different authentication and authorization domains. Over the last two decades, privacy-preserving identity management systems have gained significant attention by the academic community. More recently, this has been encompassed by increasing privacy awareness of the general public following major data breaches, as well as national and European data protection laws such as the General Data Protection Regulation (GDPR).

In a nutshell, a privacy-preserving identity management (IdM) system works as follows. A *user* can obtain a *credential* on a variety of personal *attributes* (e.g., name or birth of date) from an *issuer*, which may be a public authority, an educational institution, an online service provider, etc. Then, at a later point in time, the user can *present* such a credential to a *relying party* (aka service provider) to convince the relying party that she indeed satisfies some policy (e.g., that she is old enough to consume a certain service, or that she has a certain nationality).

On the one hand, the presentation process needs to be performed in a way that gives the relying party high authenticity and integrity guarantees, i.e., it needs to be guaranteed that the user cannot "fake" a presentation without actually satisfying the policy. On the other hand, the user shall receive high privacy guarantees, meaning that no sensitive information than what the user is explicitly consenting to reveal (e.g., her birth date but not her name) is revealed to any party involved in the process.

The general objective of this demonstrator thus is to provide an eID ecosystem offering the citizen/users an efficient and convenient way to manage identities, including the possibility to anchor the trust on a secure and high level of assurance infrastructure that will be used for supporting different levels of privacy preserving and anonymization capabilities.

Note that this is in contrast to many other IdM solutions – e.g., offered by major cloud providers from different sectors such as search engines, social networks, or online retailers – where the provider of the IdM system has full access to the user's attributes and learns detailed behavior patterns about the user. Furthermore, relying parties often do not get end-to-end authenticity guarantees as the IdM provider vouches for the correctness of the attributes, but no formal link to the original issuer can be given.

The goal of this demonstrator is to develop a highly efficient, scalable, and user-friendly IdM system giving formal security and privacy guarantees to all parties, thereby pushing forward the state-of-the-art in privacy-preserving cryptography. The core technologies shall be flexible enough to be deployed in many application domains, such as eHealth (e.g., where a user can reveal different parts of a treatment report to her insurance company, employer, or family doctor), eGovernment (e.g., thereby achieving paper de-materialization by replacing paper-based documents by electronic counterparts without having to give up on security), or others, including, but not limited to, smart cities, eCommerce, or physical access control to restricted areas.

Additionally, and beyond privacy-preserving operations based on modern cryptography, the demonstrator will include state-of-the-art countermeasures for realizing security defenses. In particular, the demonstrator will include hardening techniques for ensuring that possible vulnerabilities will not pose the users' data into risk. Specifically, we plan to leverage credential-hardening techniques for preventing attackers to abuse the system, on behalf of existing users, in the unfortunate event of a data breach involving the exfiltration of user credentials.

Within CyberSec4Europe, these core features and functionalities will be showcased in the educational sector, where, e.g., graduates are able to prove that they hold certain degrees in different university-related process.

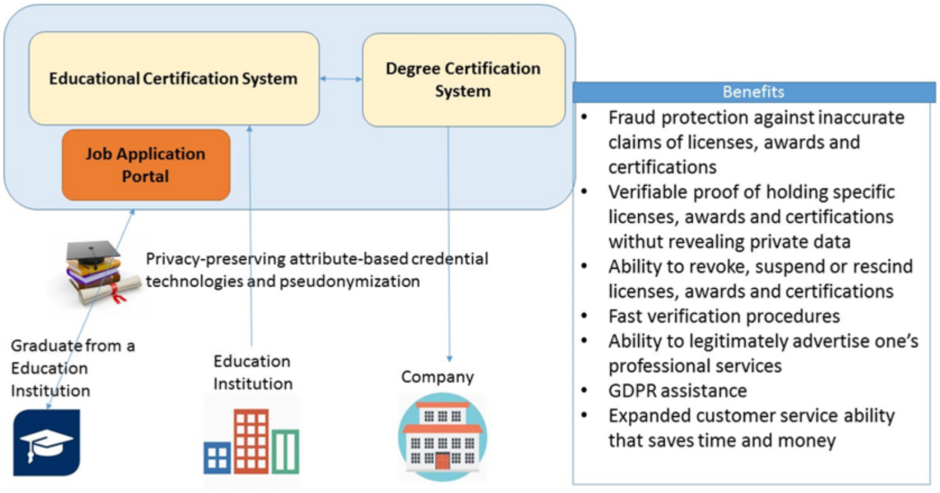
In the remainder of this section, we will aim for a compromise between generality and specificity. To do so, we will describe certain aspects of the use case agnostic of the precise demonstrator domain to ensure that our results are sufficiently generic to also be used in other application domains. Though, on the other hand, we will give clarifying details on how these generic observations apply to our specific domain.

5.1.1 Demonstrator-specific background

In Greece there was an incidence of corruption where some people bought phony degrees from companies that sell “degrees” on the Internet without requiring the buyer to do anything more than pay a fee. In order to avoid such fraud, it would be beneficial to have formally provable credentials on courses taken, and degrees obtained, by a student.

The goal of this demonstrator is therefore to provide a platform for obtaining such credentials from the university when passing an exam or receiving a degree. These credentials can later be deployed in various scenarios, parts of which will be developed as demonstrator within the project.

For instance, when applying for being accepted for a Master’s program at the university, applicants have to prove that they possess certain degrees (e.g., a BSc degree in a relevant field), and that they attended specific courses, in order to fulfill formal requirements. In order to guarantee for an unbiased process in later stages, applicants might wish to only prove that they fulfill the requirements, but not reveal, e.g., the grade they had on a certain course. Similar needs might arise when applying for a job, where certain academic requirements need to be fulfilled; again, at least in the first formal eligibility check, applicants might wish to keep certain information undisclosed, and only reveal them upon invitation. This also reduces the risk of the employer, as they never collect sensitive information about unconsidered applicants, which could later be leaked in case of a data breach. Finally, anonymous credentials could also be useful, e.g., when proving to a public authority that courses accounting for sufficiently many ECTS points were passed, in order to qualify for certain types of study allowance. However, again, it is not necessary to reeal the precise courses, grades, or amounts of ECTS points taken.


Educational Certification System
Degree Certification System
Job Application Portal
Privacy-preserving attribute-based credential technologies and pseudonymization
Graduate from a Education Institution
Education Institution
Company
Benefits

- Fraud protection against inaccurate claims of licenses, awards and certifications
- Verifiable proof of holding specific licenses, awards and certifications withut revealing private data
- Ability to revoke, suspend or rescind licenses, awards and certifications
- Fast verification procedures
- Ability to legitimately advertise one’s professional services
- GDPR assistance
- Expanded customer service ability that saves time and money

Figure 10: Privacy-Preserving Identity Management - Overview

Figure 10 gives an overview of the privacy-preserinv identity management demonstrator.

5.1.2 Relation to project objectives

Even though the specific demonstration case is in the education domain, the result of this demonstrator demonstrates the real-world usability of a broadly applicable, privacy-presering identity-management platform. Given that privacy of individuals is one of the key challenges in a highly interconnected world, the pilot directly contributes to **Policy Objective 2** focusing on meeting next generation cybersecurity challenges. Furthermore, by identifying open research challenges for large scale deployment of such systems, in close cooperation with work packages WP3 and WP4, the demonstrator also contributes to **Technical Objective 2** on the development of common research and innovation roadmap. Finally, given the relevance of strong yet privacy-preserving identities in a Digital Single Market, the task also contributes to **Innovation Objective 1** on the development on solutions increasing the security of the European Single Market.

5.2 Stakeholders

The ambition of this demonstrator is to give a way to graduates of education to digitally authenticate and share awards enhancing the multi-lateral trust. The demonstrator will provide a trustworthy and privacy preserving way to high education institutions to issue and verify official education documents and awards that contain private graduates' information.

The context is to allow secure and trustworthy exchange of higher education degrees, certifications and awards between several kinds of players with different aims and claims, regarding the security, data protection and trust issues: education organizations, companies and citizens. The demonstrator will allow higher education graduates an easy, verifiable means for them to share their awards and accomplishments as well as to promote their expertise.

5.3 Actors

In any identity management system, there exist a number of mandatory actors as well as some optional ones, depending on the specific features of the specific system and the environment within which it is deployed. The mandatory actors are *users*, *issuers*, and *service providers* (also known as *relying parties* or *verifiers*). Further additional actor roles may include *revocation authorities*, *inspectors*, or also *IdM platform providers*.

In this section we provide a list of actors with brief descriptions. Actors are all the entities that interact with the Privacy-preserving Identity Management ecosystem. They can be of two types: (i) Primary actors, which are actors that have goals which this demonstration case needs to fulfill; and (ii) Secondary actors, which don't have specific goals associated with this demonstration case, but are needed for the execution of its use cases.

We differentiate between *active* and *passive* actors. Active actors initiate a process by an action or wish for action. Passive actors react upon a request of an active actor, but don't initiate a chain of actions themselves. Users and inspectors are seen as active actors. Users, generally, wish to login to a service provider and, thus, they must obtain, beforehand, appropriate credentials that satisfy the policies of the service provider. Inspectors may become active in order to reveal a user's identity in case of abuse of the system. For users to be able to get credentials, an issuer has to take some actions in advance: to define, verify credentials, as well as provide the user with an account to retrieve the credentials; however, we consider this as a process initiated by the user due to the voluntariness of participation in such a system. Thus we view only the user and the inspector as actors that may initiate a process.

5.3.1 **Primary**

The following primary actors have immediate goals associated with privacy-preserving identity management systems:

- **Users** wish to obtain credentials on their attributes from issuers, and later present (parts of) these attributes to service providers in a privacy-preserving manner.
  Specifically, in our demonstrator domain, graduates receive certificates on degrees or passed courses, and can later selectively reveal this information, e.g., when applying for a job position, to local authorities, etc.
- **Service providers/ Verifier** want to receive provably authentic information about a user to grant her access to a specific service. They also need to be able to define a (minimum) policy a user must fulfill in order to be granted access.
  In the context of our use case, education organizations need be able to obtain verifiable claims on awards of applicants in order to accept them for a job position.
- **Issuers** certify a user's attributes upon her request after checking whether these attributes indeed belong to the user.
  In the context of our use case, education organizations may, e.g., certify that a user possesses a certain degree, passed certain courses, or applied for a certain job position.
- **Inspectors** are able to revoke the anonymity of a certain presentation and unveil the identity of the user. We model inspectors as active actors as their actions are not triggered by another actor in the system. However, in reality, inspectors may typically become active, e.g., after a court order, i.e., after being triggered by an external entity.
  The need for an inspector is still being analyzed in the context of our demonstrator case.
- **Revocation authorities** provide publicly accessible revocation information such as white lists or black lists that may be used by service providers to decide whether or not to a accept a presentation based on a certain credential. Depending on the application scenario, revocation may be triggered by the issuer, a service provider, or the user herself.
  In our demonstrator case, the revocation authority and issuer will most likely coincide.
- **IdM platform providers** are hosting and maintaining the central infrastructure needed for an identity management system. Depending on the concrete instantiation of the system, their sole responsibility may be to provide certain system parameters, but they may also act as a relay/proxy for messages being exchanged between the different actors, or even take over substantial parts of the computation to achieve a light-weight solution on the user's side.
  The concrete underlying cryptographic technology has not yet been finally decided for our demonstration case and may also be influenced by ongoing research activities, e.g., in other work packages of the project.

5.3.2 **Secondary**

In the context of privacy-preserving identity management, several other actors need to participate despite not having direct goals associated with the specific application scenario.

The secondary actors identified so far will be mainly be applications or platforms into which the different roles of a privacy-preserving identity management platform are embedded, but which in addition offer a broader range of functionalities in order to provide the precise semantics of the demonstrator scenario. In particular, they include the following systems:

- **A Degree Verification System** that performs access control by presenting a policy to the graduates. Only authorized users are given access to the Degree Verification System. Potential users of this application is the CTI personnel. The Degree Certification system provides a web service to education institutions where they their personnel can upload degrees and professional certifications. These degrees and certifications are then made available to the graduates.

- **CTI's Application Portal** is web base information portal. Through this portal, the job participants and researchers will get information about the pilot system and functionality as well as information about its usage. Moreover, this portal also contains the necessary links to the components of the system (Educational Certification System, Degree Verification System) that the participants should access.
- The **Educational Certification System** lets graduates prove that they possess a certain degree or similar
- The **User's Home Application** provides the user with an interface that enables her to browse the credentials that she possesses and create verification tokens if she wants to share a legible document or degree.

5.3.3 Use Cases Numbers

Table 15 provides an overview which actors are (potentially optionally) participating in which of the use cases presented in the following.

ACTORS	IDM-UC1	IDM-UC2	IDM-UC3	IDM-UC4	IDM-UC5	IDM-UC6	IDM-UC7
User	X	X	X	(X)		X	X
Issuer		X		(X)		X	
Service Provider			X	(X)			
Inspector					X		
Revocation Authority			(X)	X			
IdM Platform Provider	X		(X)				X

Table 15: Privacy-Preserving Identity Management - mapping of actors to use cases

5.4 Functional Requirements

In this section we provide a brief description of this demonstration case functionalities, along with a list of use cases implementing them. Note that we here focus on the demonstrator case only, and not on generic IdM systems, as the functional requirements already follow directly from the descriptions above.

- CTI will be responsible for the scheduling and realization of the Documents Certification scenario.
- CTI will be responsible for the communication framework with graduates and the Department of Computer Engineering and Informatics at University of Patras.
- Department's Registration Office employees have to provide a document containing a list of participating graduates together with department related data.
- Department's Registration Office employees have to provide graduate with a document which when signed guarantees their consent to participate in the demonstrator.
- Department's Registration Office employees will distribute to graduates a sealed envelop that contains sensitive access information such as PINs, access tokens, etc..
- Department's Registration Office employees will distribute a one time password in order the graduate to be able to access the Educational Certification System for the first time.
- CTI will contribute to the deployment and operation of the systems required for the demonstrator which will be placed at CTI premises.

5.4.1 Overview of functionalities

We suppose that the Set up phase has been finished and all the systems have been initiated. The scenario describes the procedures required so that the graduates can obtain credentials that certify that they have a legible property e.g., that they took the 1st or 2nd or 3rd degree from the department or that they passed a course.

Obtaining an Educational Credential

An Academic officer is authorized to upload degrees or grades or academic documents like the decision of the PhD committee for a student to start writing her PhD thesis e.t.c in the database of the Educational Certification System. Graduates thought Educational Certification System could get a receipt that they took the 1st or 2nd or 3rd degree from the department.

When a graduate wants to obtain a valid *educational* credential, she browses to the *CTI's Application Portal* and follows the provided instructions. Educational Certification System authenticates the graduate via the one time password (OTP, see setup phase) and initiates an issuance protocol that stores a valid graduate Privacy-ABC.

Graduate will get a valid educational credential in her device by logging in Educational Certification System via ABC technology. The educational credential stored in her device contains attributes related with educational credits.

Data Backup and Restore

This scenario is used in order to handle the loss of a graduate's credential. This scenario allows a graduate to back up her information and to restore backed up data.

If a graduate has backup content, she will be able to restore backed up data from her PC through User Agent application. In order to restore the data, the User Agent application prompts graduate to enter her PIN. Note that the PIN for backup and restore can be selected by the user, thus may be different from the PIN for unlocking the device.

Degree Verification

A group of graduates of Computer Engineer and Informatics that want to be hired can prove that they have a legible degree. We assume that the set up phase has been finished and all the graduates that will participate at the degree verification have at their possession a valid educational credential. This Degree Verification scenario is used for the realization of the verification of the submitted educational certifications for a job position. Each graduate should have the ABC user agent on her computer in order to start the degree verification procedure. Graduates are able to participate anonymously in a degree verification by logging in to the Educational Certification System via ABC technology. Whenever a graduate wants to submit his application she can access the portal. The portal will redirect him to the Educational Certification System where only users satisfying certain policies will be able to access. Graduates thought Educational Certification System could get an anonymous proof that they have a legible property that they took the 1st or 2nd or 3rd degree from the department or that they are msc or phd graduates.

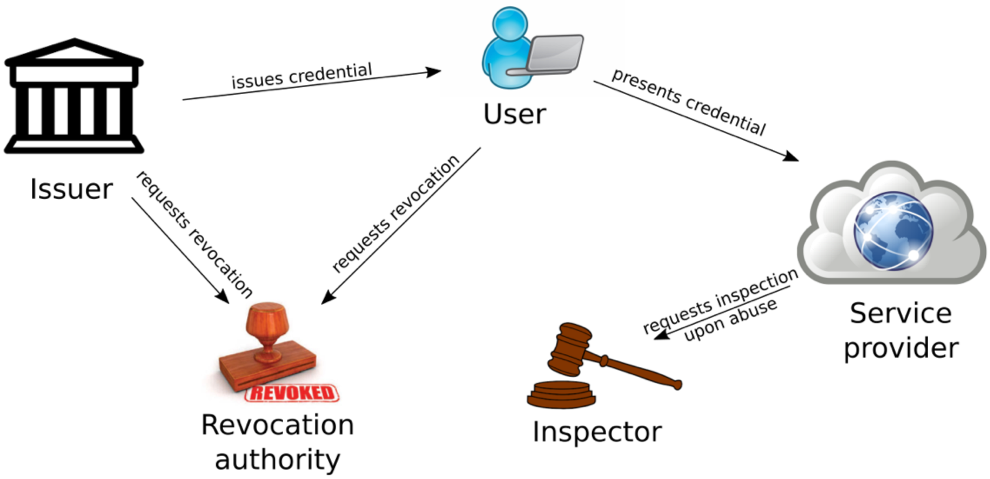


Figure 11: Privacy-Preserving Identity Management - High-level overview of use cases

5.4.2 Use Cases List

In the following we specify the following use cases that are inherent to any privacy-preserving identity management sytem.

- **IDM-UC1 – Registration**: allows a user to join a privacy-preserving IdM system.
- **IDM-UC2 – Issuance**: enables a user to receive a credential on her attributes.
- **IDM-UC3 – Presentation**: lets a user present parts of her attributes to a relying party.
- **IDM-UC4 – Revocation**: lets a user, relying party, or issuer invalidate a credential.
- **IDM-UC5 – Inspection**: allows a judge to de-anonymize a presentation.
- **IDM-UC6 – Certificate renewal**: lets a user request a new credential in replacement of an already existing one.
- **IDM-UC7 – De-registration**: enables the user to leave the IdM system.

An overview of all use cases and how they interrelate is given in Figure 11.

5.4.3 IDM-UC1 – Registration

This use case describes all steps and interactions needed for a user to join a privacy-preserving identity management system. For reasons of identity assurance, and depending on the concrete instantiation and use case, this use case may involve offline (physical) processes like visiting an authority's office, or online steps leveraging existing systems like governmentally-issued eIDs. In the course of the registration, the necessary (master) key material for a user is generated and made accessible to the user, e.g., in software, bound to a hardware token such as a smart card, or through a authority-hosted hardware security module (HSM). Specifically, for our demonstrator case, this use case contains all steps needed for a graduate to register to our demonstrator and to Degree Certification System. The Degree Certification system has stored the uploaded degrees and professional certifications. The graduate is following the instructions of the CTI's Application Portal in order to be considered as a registered user.

5.4.4 IDM-UC2 - Issuance

To obtain a certificate on personal data, a user engages in an issuance session with a certificate issuer, which might be, e.g., a public authority, a university, or a service provider. In such an interaction, the user typically authenticates herself towards the issuer, and the two parties negotiate the specific attributes to be certified

for the user (e.g., age, birth date, place of residence, nationality, expiration date, academic degrees, etc.). At the end of the interaction, the user receives a digital certificate (aka credential) attesting these attributes.
Specifically within the domain of the degree certification use case, this step is needed for a graduate to receive a credential from the Degree Certification System. The attributes attest that she possesses a legible title.
The graduate access the Degree Certification System thought CTI's portal in order to request from it to certify that she has a legible academic degree/title/certificate.

5.4.5 IDM-UC3 - Presentation

A user can prove possession of a credential certifying certain personal attributes to a service provider (aka relying party) by engaging in a presentation protocol. In this protocol, the two parties agree on which attributes the user needs to reveal, e.g., based on a policy of the service provider. At the end of the interaction the service provider receives these attributes with high authenticity guarantees, while the user is guaranteed that no other information was revealed to the service provider.
Specifically, within our demonstration case, this use case is performed when a student needs to generate a verifiable proof that she possesses a certain title or attended specific courses, e.g., to the application portal or a local authority.

5.4.6 IDM-UC4 - Revocation

A user's credential may be invalidated or revoked for many different reasons, e.g., because of abuse or after a name change. Depending on the precise scenario, this process may be triggered by the different actors in the system. Firstly, the user may herself request the revocation of a credential at the issuer, e.g., if she suspects that her secret data was somehow leaked. Secondly, the issuer may revoke a certificate, e.g., because of abuse. Thirdly and finally, the service provider may decide the locally revoke a certain certificate, e.g., again because of abuse. As a result, the user will no longer be able to perform a presentation with the invalidated credential, either globally in the system or with this specific service provider.
Within our demonstration domain, this use case will in particular be needed when attributes (e.g., names) change, or when unauthorized parties gained access to a user's secret credential.

5.4.7 IDM-UC5 - Inspection

This use case allows a dedicated party, often referred to as "judge", to revoke the anonymity of a specific presentation process, e.g., because of abuse.

5.4.8 IDM-UC6 – Certificate renewal

In this use case, a user can renew a credential that she already received earlier. This procedure may be triggered for different reasons, e.g., because the expiration date of a certificate has expired, or attributes such as name have changed. Also, the user may request a re-issuance of a credential that was previously revoked for some reason. The involved process is closely related to issuance (cf. UC2), yet might be more lightweight and require less strict attribute assurance. Also, depending on the concrete type of credential, the use case may trigger revocation of the underlying original credential (cf. UC4) in order to avoid that a user has multiple credentials on the same data.

5.4.9 IDM-UC7 – De-registration

This use case allows a user to completely de-register from the system. In this case, all certificates belonging to this user will be invalidated, and the user's personal information will be deleted to the extent possible by legal regulations.

5.5 Security and Privacy Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-SP01	HWTok	The hardware tokens used for store the degree information should comply with relevant standards, cryptography requirements, authentication protocols and protection profiles (if available) and must correctly implement them.	IDM-UC1, IDM-UC2	Medium	No
IDM-SP02	AuthnE	The service provider/relying party in a presentation shall receive formally provable guarantees that the revealed attributes have not been altered by the user.	IDM-UC3	High	Yes
IDM-SP03	AuthnE	All components of CS4E must use authentication protocols to mutually authenticate. Each communication between the components, between any hardware token (SC), the Degree Verification System and between the verification service consumer shall only take place after a successful mutual authentication.	All	High	Yes
IDM-SP04	AuthnM	In a real-world application scenario, it must be guaranteed that a key indeed belongs, e.g., to a certain issuer, in order to protect against adversaries issuing credentials under non-certified keys.	IDM-UC2, IDM-UC3, IDM-UC6	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-SP05	Unlink	Besides the users' data itself, also metadata about the user such as usage or access patterns can be sensitive information. Any privacy-preserving identity management solution should therefore give users the option to decide which activities should be linkable to each other, and which activities should be provable unlinkable to each other.	IDM-UC3	Medium	No
IDM-SP06	UI AC	In order to maximize the level of privacy as well as for legal compliance purposes, users should have full control over which parts of their sensitive data they are willing to reveal to whom. Furthermore, it is desirable that users can check whether certain relying parties are actually eligible to request certain pieces of information, similar to what was done in previous projects.	IDM-UC3	Medium	Yes
IDM-SP07	Anon	The user's identity must not be leaked to any other party in the system, neither through the presentation itself nor through metadata, expect if the user explicitly consented to reveal his identity.	IDM-UC3	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-SP08	Acc	While high privacy guarantees are essential, perfect anonymity might not always be desirable in order to avoid abuse. Therefore, depending on the specific scenario, a dedicated third party may be necessary that is able to revoke the anonymity of a user, e.g., upon judicial order. However, it is necessary that the existence of this option is clearly communicated to the user, and also that this party is clearly specified.	IDM-UC5	Low	No
IDM-SP09	Rev	In order to prevent abuse through a user or in case of a data leak, it may be required to invalidate a credential, triggered by the user, the issuer, and/or a relying party. In this case, the revocation information (e.g., blacklists) should not leak the identities of the owners of the revoked credentials.	IDM-UC4	Low	No
IDM-SP10	IdM	Depending on the concrete deployment scenario, high assurance guarantees regarding the identities of the credential owners, as well as the certified attributes, are required.	IDM-UC2, IDM-UC6	Medium	No
IDM-SP11	Conf	User credentials, for instance upon a data breach, should be hardened against cracking attempts.	All	Medium	No

Table 16: Privacy-Preserving Identity Management - Security and privacy requirements

5.6 Non-Functional Requirements

5.6.1 Look and Feel Requirements

No look and feel requirements have been identified at this point.

5.6.2 Usability Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-U01	Perfo	In order to increase usability and future market penetration, all developed solutions must be highly efficient. In particular, the time needed for the cryptographic operations and necessary communication when receiving or presenting a credential should not exceed 1000ms, even when stored on a commodity smart card as a trusted service. Furthermore, all user data must be presented in a sufficiently compact form to fit on such devices.	All, in particular IDM-UC3	High	Yes
IDM-U02	Usab	While high privacy and security guarantees are appreciated by end users, broad adoption of security and privacy technologies requires a high level of invisibility towards the end user. For instance, canonical or well-known usage patterns should be affected as little as possible, as little additional steps as necessary should be introduced, not non-commodity hardware should be required, or the responsiveness and efficiency of the overall system should not be negatively impacted by the new solutions.	All, in particular IDM-UC3	High	Yes
IDM-U03	Transp	All privacy guarantees but also the remaining privacy risks shall be communicated to the user in a highly transparent way, e.g., regarding metadata privacy but also regarding the existence of a third party that may revoke anonymity. This is necessary to enable users to take informed decisions about their private data.	All, in particular UC3	High	Yes

Table 17: Privacy-Preserving Identity Management - Usability requirements

5.6.3 Operational Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-OP01	Perfo	Solutions provided and their integration on existing system should take into account privacy and security compliance, perceived ease-of-use, scalability and performance aspects	All, in particular IDM-UC3	High	Yes

Table 18: Privacy-Preserving Identity Management - Operational requirements

5.6.4 Maintainability and Portability Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-MP01	SDLC	All developed solutions should aim for high compatibility with existing de-facto and industry standards for authentication and authorization (e.g., OAuth2).	All, in particular IDM-UC3	Medium	No

Table 19: Privacy-Preserving Identity Management - Maintainabilty and portability requirements

5.6.5 Social and Political Requirements

No social or political requirements have been identified at this point.

5.6.6 Legal and Regulatory Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IDM-LR01	GDPR	Newer European Commission law/regulation about data privacy must be respected.	All	High	Yes
IDM-LR02	Priv	The ePrivacy Regulation (ePR) should be respected. The Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. In particular, Privacy is guaranteed for communications, while metadata have a high privacy component and must be anonymised or deleted if users did not give their consent unless the data is needed for billing.	All	Medium	No
IDM-LR03	IdM	CS4E stakeholders should comply with the security requirements defined in eIDAS regulation. The Degree Verification System shall apply the Article 19: Security requirements applicable to trust service providers.	All	Medium	Yes
IDM-LR04	SDLC	For legal compliance and compatibility with other frameworks, entity assurance frameworks such as ISO/IEC 29115 should be followed.	All	Medium	No

Table 20: Privacy-Preserving Identity Management - Legal and regulatory requirements

5.7 Mandated Constraints

No mandated constraints have been identified at this point.

5.8 Relevant Facts and Assumptions

5.8.1 Facts

No relevant facts affecting the system have been identified at this point.

5.8.2 Assumptions

No assumptions about the system have been identified at this point.

5.9 Related WP3 and WP4 Tasks

Task 5.3 cover a transversal technology that can be related to several areas and research aspects in security and privacy and as such it has relation to multiple different tasks in WP3 and WP4. A smooth collaboration with most of these tasks can be guaranteed by partners that are actively contributing to T5.3 as well as the corresponding other tasks. In the following we give a brief overview of some of the most important synergies with other tasks:

- **T3.1: Common Framework Design** (partners involved: UMU). This task addresses the project lifecycle and how the activities, results and community built and gathered by the project compose into an overall CyberSec4Europe ecosystem of cyber-security development. As such, the T5.3 benefits from this task's efforts to collect and categorize the various efforts developed within the consortium.
- **T3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies** (partners involved: UMU, AIT, UCY, UPRC). This task defines the technology behind several security and privacy enablers. Several of these enablers might be leveraged in either of the phases of our demonstrator, not only those related to privacy-preserving authentication, but also, e.g., those regarding hardening of passwords and credentials.
- **T3.6: Usable Security (Human-centred Cybersecurity)** (partners involved: UMU). This task formulates and develops recommendations and guidelines on how to incorporate usability requirements in security design, as well as a tool-supported method for assessing the effectiveness factor of usability. History has proved that usability is one of the reasons why privacy-preserving authentication mechanisms have not yet been wider deployed, we believe that a collaboration with T3.6 might be beneficial, in particular in the evaluation phase of our demonstrator.
- **T3.7: Regulatory Sources for citizen-friendly Goals** (partners involved: UMU, AIT). The goal of the task includes the design of best practices for innovative and GDPR compliant user experience and the investigation of the compliance for identity technologies interoperability. While the precise kind of collaboration has not yet been defined, we believe that T5.3 as well as T3.7 would benefit from such a collaboration, e.g, by feeding best practices into T5.3 and receiving back experiences from the demonstrators as well as feedback on technical feasibilities and the state of the art.
- **T4.3 Mapping and roadmap design** (involved partners: UMU). This is the general roadmap design task, which will in particular benefit from T5.3 indirectly through the inputs made to task T4.6.
- **T4.6 Roadmap for industrial challenge 5.3 (Privacy-preserving Identity Management)** (involved partners: UMU, AIT, UCY, UPRC). This task directly corresponds to T5.3 in terms of defining a research roadmap during and beyond the lifetime of our project. The task is in steady contact with T5.3 to collect identified challenges, open questions, innovative alternative approaches, etc., both technical and non-technical.

- **T4.9 Roadmap for industrial challenge 5.6 (Medical Data Exchange)** (involved partners: none). This task is dedicated to the design of a research roadmap for the demonstrator detailed in Section **Error! Reference source not found.**. Given the direct need for privacy-preserving identity and access management solutions, interesting real-world research and development challenges for our demonstrator technology might come out of this task as well.

Besides the aforementioned collaborations, there are some more tasks with which potential relations can be identified, yet to a relatively minor extend. These potential synergies are also covered in Table 21:

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3	✓	✓		✓		✓	✓		✓	
WP4			✓	✓		✓			✓	

Table 21: Privacy-Preserving Identity Management - Relationship with WP3 and WP4 tasks

6 Incident Reporting in the Financial Sector

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled Incident Reporting in the Financial Sector.

The demonstration case will allow financial organizations to report security incidents detected in a faster and compliant way. It will permit to follow the mandatory regulatory requirements aimed at overseeing and protecting the EU Digital Single Market. It will be also useful to support the collection of information on cyber-attacks occurred required for mandatory incident reporting. Working in a digital environment, it is crucial to adopt a holistic approach to improve the cyber-resilience of the whole system and to maintain the integrity of the EU Digital Single Market (project **Innovation Objective 1**). The cybersecurity information data sharing is one of the means by reaching this goal, paving the way for a sustainable and synergical cybersecurity system (project **Technical Objective 3** and **Policy Objective 2**). The demonstrator is developed by a technological partner (Atos) with the collaboration of two financial institutions partners (Intesa Sanpaolo and BBVA) (project **Innovation Objective 2**).

We first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

6.1 Goals

Cyber Security is of paramount importance to protect the whole EU Digital Single Market, and this is mirrored in the EU legislative evolution addressing Cyber Security. It is worth mentioning that the Financial industry is one of the main critical sectors affected by new regulations in this sense, including among others the NIS Directive, the GDPR or the PSD2 along with other financial sector regulatory requirements. The importance of Cyber Security in the financial sector should be addressed starting with research and development, keeping in mind the need to implement and leverage tools helpful to mitigate and tackle cyber threats, and improving cyber resilience.

The Digital Single Market landscape and its transformation into a highly interconnected environment have for example led regulators to identify critical sectors and the need to draw the attention to their systemic relevance. The analysis of all the actors involved in a scenario of a large cyber-attack demonstrates that not only cyber-risk does go beyond national borders, but also beyond sectorial boundaries, leading to potentially dramatic systemic risks. It is utmost appropriate to undertake a holistic view, pushing for a collaborative approach towards enhanced cyber resilience.

Bearing in mind the objective of increasing the readiness and awareness in Cyber Security, the current EU legal framework already incorporates the need to comply with **Mandatory Incident Reporting** to different Supervisory Authorities, respecting the relevant impact assessment criteria and thresholds, timing, data set, communication means as defined by each authority both at EU and national level. All these different criteria and patterns cause fragmentation into the overall incident reporting process, and need to be managed along the critical path of managing the incident itself.

These mandatory reporting requirements are particularly strong in the financial market. For instance, when a cyber incident impacts a multinational Financial Group, there is also the additional need for each entity impacted to eventually report to the National Competent Authority, and for the Parent Company Headquarter to gather all the information in a standardised way from each legal entity, in order to assess the overall impact at Group level.

The goal of this demonstration case is to develop a platform that enables financial institutions to fulfil the mandatory incident reporting requirements according to the different procedures/methods specified by applicable regulatory bodies (e.g. PSD2, ECB Cyber Incident Reporting Framework). The created platform will address this common need for standardised and coordinated cyber-security communication cooperation, and it could also pave the way towards a public and private cooperation to reach the common goal of an enhanced cyber resilience across Europe and beyond the EU borders.

6.2 Stakeholders

This section is devoted to the identification of the main stakeholders, that are the entities that will be affected by, or who have an interest (economic, technical, political, legal, etc.) in the Incident Reporting demonstration case. We consider two main categories of stakeholders:

- **Financial Institutions**: FIs are the entities who are forced by different regulations/frameworks to report to different Supervisory Authorities on Cyber Incidents applying different procedures and templates.

  It is worthy to highlight that, under different regulations, a single FI could represent several subjects at the same time, each of them with specific requirements:
  - **Target 2 Participants** (ECB Target2): A distinction is made between critical participants and non-critical participants, depending on the market share in terms of value and/or the type of transactions processed.
  - **Significant Institutions** (ECB SSM): The ECB classifies banks as Significant or Not Significant based upon the criteria of Size, Economic Importance, Cross-Border Activities and Direct Public Financial Assistance.
  - **Payment Services Providers** (PSD2): It applies to banks and financial institutions operating as Payment Service Providers (PSPs).
  - **Operator Essential Service** (NIS): Banks and financial institutions are considered as OES because: (a) they provide a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.
  - **Personal Data Processor/Controller** (GDPR): Banks and financial institutions operate both as Processor, which processes personal data on behalf of the controller, and Controller, which determines the purposes and means of the processing of personal data.
  - **Trust Service Providers** (eIDAS): Banks and financial institutions can operate with their trust services either as a Qualified or as a Non-qualified trust service provider.
- **EU/National Supervisory Authorities**: they are the entities responsible for introducing the different reporting requirements and receiving the corresponding reports. Each regulation/framework imposes a concrete and corresponding supervisory authority:
  - **NIS Directive**: National NIS Authority
  - **GDPR**: National Data Protection Authority
  - **eIDAS Regulation**: National Certification Authority
  - **PSD2**: NCA/ECB/EBA
  - **ECB/SSM**: ECB/Joint Supervisory Team
  - **Target2**: National Central Bank/ TARGET2

6.3 Actors

In this section we provide a list of actors with brief descriptions. Actors are all the entities that interact with the Incident Reporting ecosystem. They can be of two types: (i) Primary actors, which are actors that have goals which this demonstration case needs to fulfil; and (ii) Secondary actors, which do not have specific goals associated with this demonstration case, but are needed for the execution of its use cases. Special attention has been paid to the identification of the actors in the management process from an internal FI perspective.

6.3.1 Primary

The envisaged primary actors of this demonstrator are:

- **Incident Management Team** (IMT): This is the main actor of the Incident Reporting demonstration use case. It corresponds to operator/s of the internal organizational unit affected by the potentially dangerous event. They are in charge of carrying out a more detailed analysis in order to determine the necessity of opening an incident in the application, or if it is an issue that can be solved internally. In case of incident, the Asset Owner / Incident Management Team is responsible for opening the incident and for the collection of the main information related to the incident itself. There are two subtypes, the Bank IMT and the International Subsidiary IMT.
- **Incident Classification Team** (ICT): This actor is the internal organizational unit responsible for classifying all the incidents opened by the Incident Management Team. This includes the identification of the type of incident, the perimeter extension and the estimation of the economic impact. The result of the classification determines if the incident can be managed by the unit until its closure, or if an escalation process is needed because the incident is classified as an emergency or a crisis.
- **Incident Reporting Team** (IRT): This actor has to continuously monitor the evolution of the incident and needs to carry out the intermediate reporting processes to competent authorities until the closure of the incident, according to relevant regulation timeline.
- **Controller**: This actor is responsible for performing the managerial judgement about the incident classification done by the Incident Reporting demonstrator, giving the authorization to proceed with the reporting. The Controller is also the one who authorizes the actual reporting and oversees the whole incident reporting process.
- **Administrator**: This actor oversees the customization of the Incident Reporting Demonstrator to adapt it to the particular needs of a FI or a given market. The Administrator is the demonstrator supervisor from the IT perspective.

6.3.2 Secondary

The envisaged secondary actors are the following ones:

- **EU/National Supervisory Authorities**: This actor is in charge of receiving and processing the incident reports submitted by the demonstrator.
- **EU/National Competent Authorities**: This actor could be considered among the ones of receiving and processing the incident reports submitted by the demonstrator.

6.3.3 Use Cases Numbers

Actors	IR-UC1	IR-UC2	IR-UC3
Incident Management Team	X		
Incident Classification Team	X		
Incident Reporting Team			X
Controller		X	X
Administrator	X	X	X
EU/National Supervisory Auth.			X

Table 22: Incident Reporting - Mapping of actors to use cases

6.4 Functional Requirements

In this section, we provide a brief description of this demonstration case functionalities, along with a list of use cases implementing them.

6.4.1 Overview of functionalities

The main functionalities of this Incident Reporting demonstration case shall enable the financial institutions to leverage such smart engine during the mandatory incident reporting including the coverage of the incident management process. Figure 12 and Figure 13 provide different views about the functional workflows expected in this Incident Reporting Demonstration case.

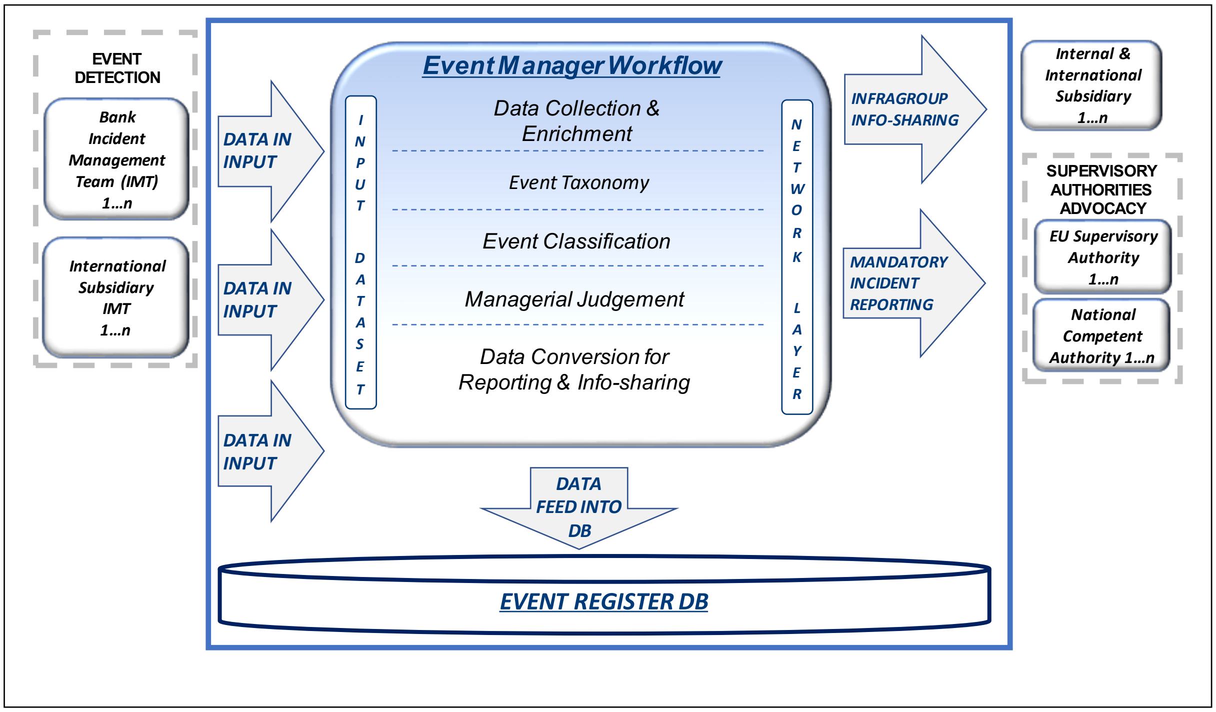

EVENT DETECTION
Bank Incident Management Team (IMT) 1…n
International Subsidiary IMT 1…n
DATA IN INPUT
DATA IN INPUT
DATA IN INPUT
Event Manager Workflow
INPUT DATASET
Data Collection & Enrichment
Event Taxonomy
Event Classification
Managerial Judgement
Data Conversion for Reporting & Info-sharing
NETWORK LAYER
DATA FEED INTO DB
EVENT REGISTER DB
INFRAGROUP INFO-SHARING
MANDATORY INCIDENT REPORTING
Internal & International Subsidiary 1…n
SUPERVISORY AUTHORITIES ADVOCACY
EU Supervisory Authority 1…n
National Competent Authority 1…n

Figure 12: Incident Reporting – Event Management Workflow

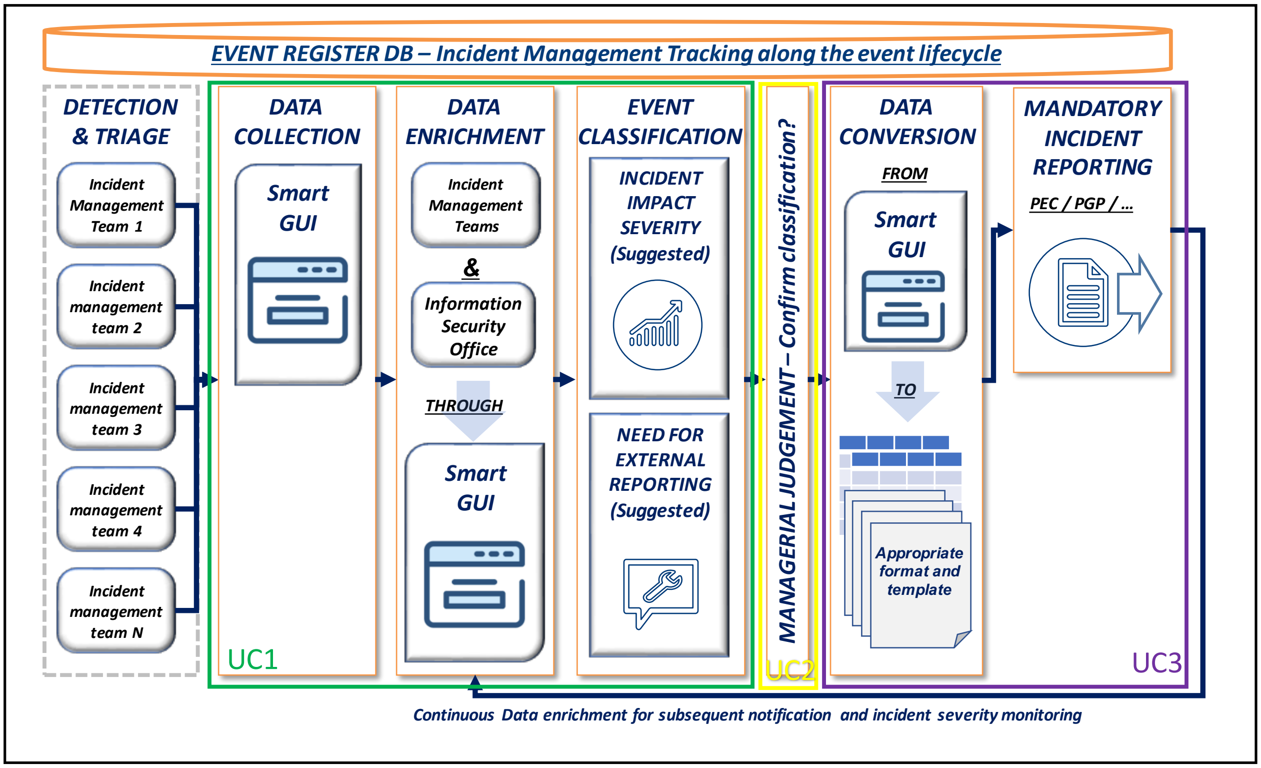

EVENT REGISTER DB – Incident Management Tracking along the event lifecycle
DETECTION & TRIAGE
Incident Management Team 1
Incident management team 2
Incident management team 3
Incident management team 4
Incident management team N
DATA COLLECTION
Smart GUI
UC1
DATA ENRICHMENT
Incident Management Teams
&
Information Security Office
THROUGH
Smart GUI
EVENT CLASSIFICATION
INCIDENT IMPACT SEVERITY (Suggested)
NEED FOR EXTERNAL REPORTING (Suggested)
MANAGERIAL JUDGEMENT – Confirm classification?
UC2
DATA CONVERSION
FROM
Smart GUI
TO
Appropriate format and template
MANDATORY INCIDENT REPORTING
PEC / PGP / ...
UC3
Continuous Data enrichment for subsequent notification and incident severity monitoring

Figure 13: Incident Reporting - Functional Workflow

The Incident Reporting workflow begins with the data collection, followed by the data enrichment and the event classification. These three steps, aiming at defining and quantifying the incident, have a direct correspondence with UC1 (covered in section 6.4.3). The minimum set of information, to be initially collected when a Security Incident is detected, is identified to assess the need for Incident Reporting, depending on different regulatory frameworks considered. The first collection of data could be categorized in three different types of information:

1. General Information;
2. Incident Taxonomy: to identify the causes that generated the incident;
3. Specific information: to assess the need for Mandatory Incident Reporting.

Figure 14 depicts the methodology that should be used at this stage for the classification of critical events.

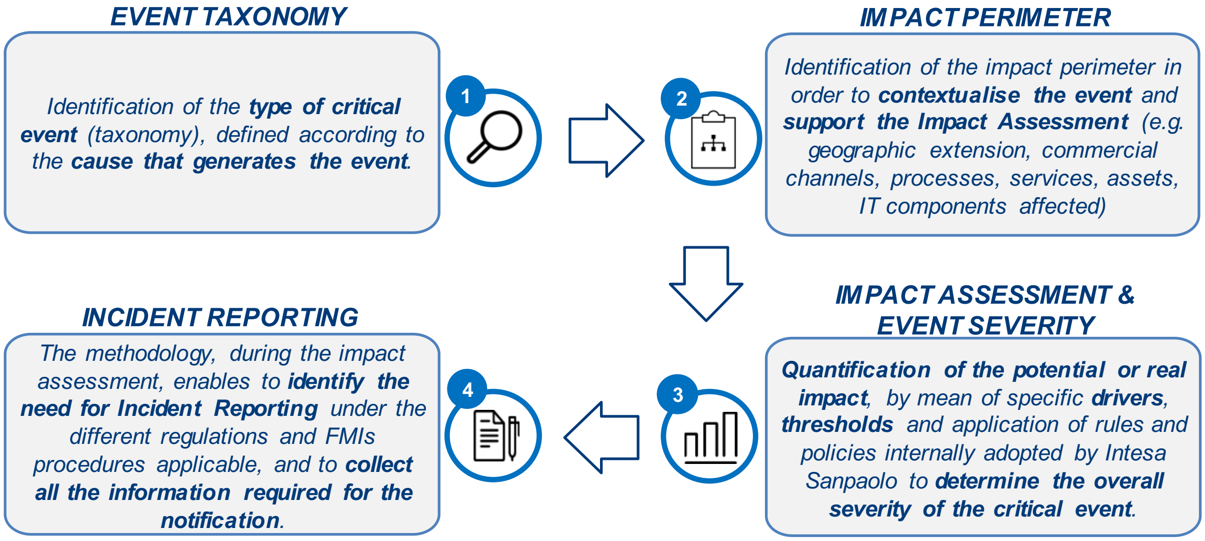

EVENT TAXONOMY
Identification of the type of critical event (taxonomy), defined according to the cause that generates the event.
1
2
IMPACT PERIMETER
Identification of the impact perimeter in order to contextualise the event and support the Impact Assessment (e.g. geographic extension, commercial channels, processes, services, assets, IT components affected)
IMPACT ASSESSMENT & EVENT SEVERITY
Quantification of the potential or real impact, by mean of specific drivers, thresholds and application of rules and policies internally adopted by Intesa Sanpaolo to determine the overall severity of the critical event.
3
4
INCIDENT REPORTING
The methodology, during the impact assessment, enables to identify the need for Incident Reporting under the different regulations and FMIs procedures applicable, and to collect all the information required for the notification.

Figure 14: Incident Reporting - Critical events classification methodology

Once the event has been classified, the next step in the workflow is the managerial judgement done by the Controller. This step is represented by UC2 covered in section 6.4.4.

When the controller authorizes the reporting, the Incident Reporting Demonstrator will prepare and deliver the incident reports considering the formats and processes specified for the targeted Supervisory Authorities. This step is represented by UC3 covered in section 6.4.5.

As a consequence of the workflows described above, we envisage that the Incident Reporting demonstrator use case should include the following high-level functional requirements:

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-F01	AC	Mandatory Incident Reporting shouldn't be automatic, it should still be manual to prevent accidental reporting – 4eye principle	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-F02	Funct	It must collect all the information required related to the cyber incident through different questionnaires.	IR-UC1	High	Yes
IR-F03	Config	It will allow to upload/download/configure templates that will be sent to the incident report team with the fields fulfilled. The user will indicate the regulatory framework and all the variables to insert in the template according to the templates specified in the regulation.	IR-UC1	High	Yes
IR-F04	Funct	It must provide support during the Security Event Classification. The	IR-UC1	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		classification methodology to be included will take into account the criteria and thresholds defined by the European regulators along with the set of information necessary to report the incident, using the appropriate procedures and templates defined by the Competent Authority (National or European).			
IR-F05	Funct	It must suggest the Severity of a Security Event, in order to activate the most appropriate action plan for managing and responding to the Incident or Threat.	IR-UC1	High	Yes
IR-F06	Funct	It must identify the need for Mandatory Incident Reporting, considering the reporting requirements and related assessment methodologies w.r.t. each Competent Authorities.	IR-UC1	High	Yes
IR-F07	Funct	It must suggest to the FI operator about the Mandatory Incident Reporting processes to be followed.	IR-UC1	High	Yes
IR-F08	Funct	It must request the authorization of the FI operator (Controller) to proceed with the reporting.	IR-UC2	High	Yes
IR-F09	Funct	It must produce the appropriate template and communication, in the appropriate format to be sent to the Competent Authority.	IR-UC3	High	Yes
IR-F10	NoA	It must provide communications from the Legal Entity of a multinational Group, or the specific office detecting the incident, to the headquarter Information Security Office.	IR-UC3	High	Yes
IR-F11	NoA	Incidents are forwarded to the applicable competent authorities. It should be able to determine or advice upon which reporting duties apply.	IR-UC3	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-F12	Acc	It must support the tracking for the whole Security Event lifecycle within a Financial Institution Security Event Database.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-F13	SInt	It must enforce a workflow to be used for reporting purposes.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-F14	Config	It must support the customization of the Incident Reporting Workflow by the system administrator, in light of supporting future integration with new coming regulations.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-F15	Funct	It will allow to export, from the graphic user interface, the thresholds and criteria used in the event classification or the incidents detected to different formats (pdf, xls, txt, etc.).	IR-UC1, IR-UC2, IR-UC3	Low	Yes
IR-F16	Config	It should allow the administration of the applicable internal and external competent authorities.	IR-UC3	High	Yes
IR-F17	Funct	It should contain a report module that allows access to the information on the number of incidents that occurred in a given time.	IR-UC1, IR-UC2, IR-UC3	Low	No
IR-F18	Funct	It should have a section where the variables that are going to be present in the creation of the incidents can be configured. In this section the possible values of each field will be catalogued and will allow the addition of new values to the catalogue.	IR-UC1, IR-UC2, IR-UC3	Low	No
IR-F19	SLog	It must have log files that will be saved in the system. The logs must contain all traceability of the demonstrator itself (errors, status, etc.), as well as the actions that each user has made when using the application.	IR-UC1, IR-UC2, IR-UC3	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-F20	Usab	It should have a help button that will show the specific help for each screen in the graphical interface in order to help the user to understand and perform the actions available in it.	IR-UC1, IR-UC2, IR-UC3	Low	No
IR-F21	Usab	It should have the possibilitiy to include a regulatory wiki as part of the help function.	IR-UC1, IR-UC2, IR-UC3	Medium	No
IR-F22	Usab	It should have a section where the users could find the direct link of main Mandatory Incident Reporting Regulations/Guidelines/Directives.	IR-UC1, IR-UC2, IR-UC3	Low	No
IR-F23	IdM	It should allow to the administrator the user management in terms of creating, modifying, deleting, assigning right permissions, searching and so on in order to identify the right reviews (user access, role definition, tasks in charge etc.).	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-F24	Config	It should allow to create and process several rules able to identify and notify specific conditions that could be needed for monitoring the user activities on the demonstrator.	IR-UC1, IR-UC2, IR-UC3	Medium	No
IR-F25	Funct	It should have an interface to allow the integration with third-party technologies	IR-UC1, IR-UC2, IR-UC3	Medium	Yes

Table 23: Incident Reporting - Functional requirements

6.4.2 Use Cases List

Based on the functional workflow described in previous section, we have identified the following high-level use cases:

- **IR-UC1 – Data Collection, Enrichment and Classification**
- **IR-UC2 – Managerial Judgement**
- **IR-UC3 – Data conversion and reporting preparation**

6.4.3 IR-UC1 – Data Collection, Enrichment and Classification

UC1 starts with the data collection phase, where the ITM will input all the information related to the incident through a smart GUI based on questionnaires. All the information required in the "Data Collection" phase should be gathered by the Incident Management Team, that can either receive a notification from an impacted or involved business office/function or detect directly an incident occurrence. If there is a clear evidence that the incident is entailing a possible mandatory incident reporting requirement (e.g. personal data breaches, incidents impacting T2 or payment services…), or if the impacts of the occurred incident seem to be significant, the Incident Management Team should send to the Incident Classification Team all the information gathered in order to assess the incident severity and to report the incident to the competent authority, as appropriate.

Once the incident has been registered, the next step is the enrichment of information about the incident to have a better knowledge about its scope and potential impact. This enrichment will be done also by using the GUI and taking into consideration the information received by the Supervisory Authorities (if any).

After that, the Incident Classification Team validates the information provided and continues with the categorization, classification and identification of the cause that generated the incident, with the final objective of reporting to the FI its impact and severity. As a result of this process, it will be decided if the incident must be reported or not, and to whom.

Each regulatory requirement is linked to specific needs also w.r.t. customers protection, thus upon an incident, the impact assessment must be undertaken against each and every EU and national regulations to verify the applicability of IR regulatory requirements. The first move towards the harmonisation of IR is to create the most exhaustive IR data set, considering all the possible requirements, and define a common taxonomy. The Taxonomy is applicable to both Cyber and Operational critical events.

The impact assessment process is on the critical path of Incident Management and requires a clear coordinated procedure; it is necessary to smooth the process to create an efficient and effective Incident Reporting introducing new tools such as this demonstrator. Figure 15 summarizes the steps included in this use case described.

6.4.3.1 Use Case Diagram

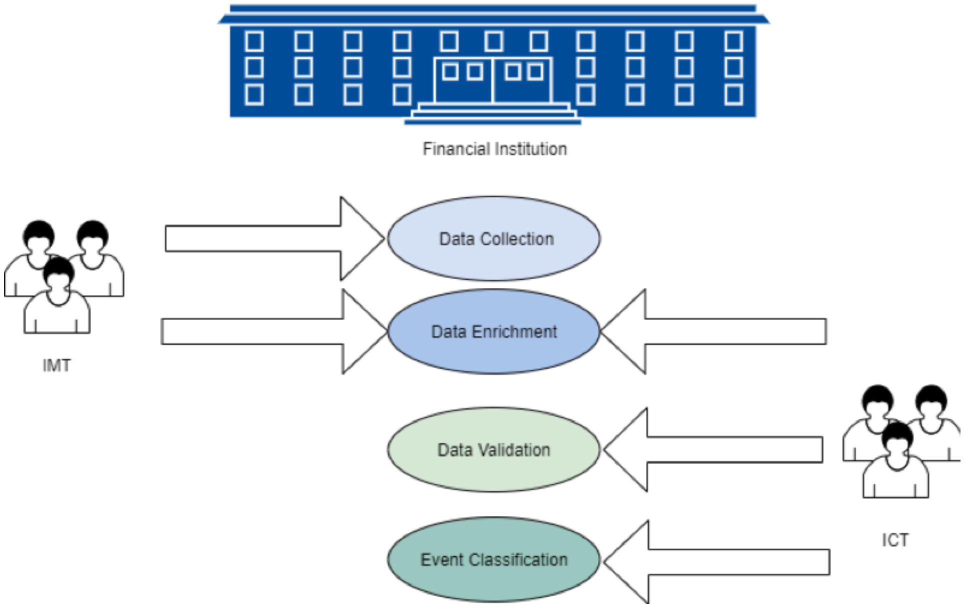


Figure 15: Incident Reporting - UC1 Data Collection, Enrichment, and Classification

6.4.4 IR-UC2 - Managerial Judgement

UC2 covers the authorization process in which the Controller will perform the managerial judgement about the incident classification. The Controller, based on the experience gained, the specificities of the incident and further considerations made, may still assign the overall level of severity through a Managerial Judgement, confirming, increasing or lowering the Incident Severity level, and confirming or not the need for Incident Reporting suggested by the demonstrator. Figure 16 represents the actor of this use case performing the managerial judgement.

Based on the assigned Severity judgement, the most appropriate action plan to be implemented to handle and respond to the incident will be determined.

6.4.4.1 Use Case Diagram

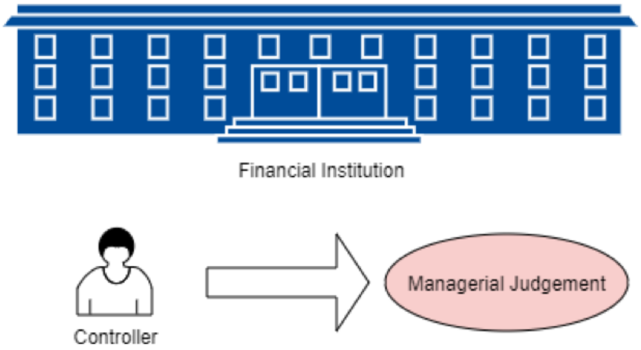


Figure 16: Incident Reporting - UC2 Managerial Judgement

6.4.5 IR-UC3 - Data conversion and reporting preparation.

On the basis of the information collected and the Incident Reporting evaluation output performed in UC2, the Incident Reporting demonstrator should include all the needed information into the appropriate template/communication to be sent to the Competent Authority. First, the data is converted to the formats and templates requested by the Competent Authorities affected by the incident and after that, when the Controller authorizes it, the actual reporting is performed. Figure 17 summarizes the actors and phases involved in this use case.

6.4.5.1 Use Case Diagram

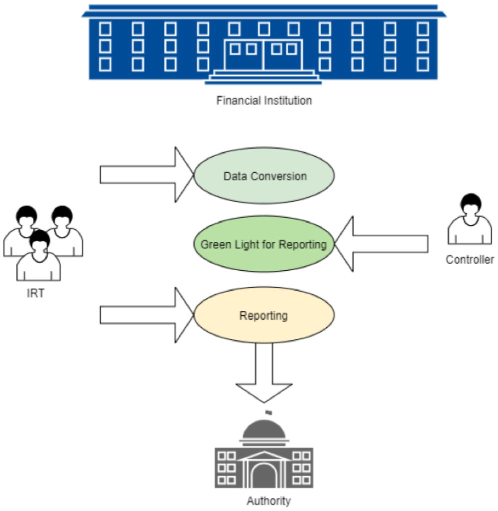


Figure 17: Incident Reporting - UC3 Data Conversion and Reporting

6.5 Security and Privacy Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-SP01	AuthnE	Strong authentication mechanisms must be included to check the rights granted with the user credentials to access to the platform.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-SP02	Conf	It must grant access to information on a need to know base and matching authorisation profiles.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-SP03	Avail	It must warranty that information needed is made available.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-SP04	IdM	It must have a section of roles and users that will allow configuration with the sufficient granularity to be able to ensure limiting or granting permissions to each user based on their functions.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-SP05	Acc	Logging, timestamping and tracking mechanisms must be incorporated at all phases of the Incident Reporting process.	IR-UC1, IR-UC2, IR-UC3	High	Yes

Table 24: Incident Reporting - Security and Privacy requirements

6.6 Non-Functional Requirements

6.6.1 Look and Feel Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-LF01	UI	It must include a GUI that will allow the interaction with the operator.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-LF02	Usab	The GUI must support different languages and provide an easy way to incorporate new ones.	IR-UC1, IR-UC2, IR-UC3	Medium	No

Table 25: Incident Reporting - Look and feel requirements

6.6.2 Usability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-U01	Usab	The GUI must be user-friendly, offering a better user experience, improving the response times and facilitating the navigation between the different functionalities.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-U02	Usab	The GUI must request to the operator all the required information about the incident, including the impact assessment, through different questionnaires.	IR-UC1	High	Yes
IR-U03	Usab	The questionnaires presented to the operator must be self-adaptive, customized depending on the information already provided about the incident.	IR-UC1	High	Yes

Table 26: Incident Reporting - Usability requirements

6.6.3 Operational Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-OP01	SDLC	It must be an “in house” standalone application deployed on the FI premises.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-OP02	Funct	It should provide the possibility to the user to select the currency applicable for creating the incidents.	IR-UC1	Medium	No
IR-OP03	Funct	It should support multiple time zones.	IR-UC1, IR-UC2, IR-UC3	Medium	No
IR-OP04	Funct	It should be able to consider different business calendars.	IR-UC1, IR-UC2, IR-UC3	Low	No

Table 27: Incident Reporting - Operational requirements

6.6.4 Maintainability and Portability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-MP01	Config	It should include configuration mechanisms for incorporating additional regulations that may have effect in different sectors.	IR-UC1, IR-UC2, IR-UC3	Medium	Yes
IR-MP02	Funct	It should be designed in a flexible and modular way to ensure that is able to evolve and cope with regulatory evolution over the time and geographies.	IR-UC1, IR-UC2, IR-UC3	Medium	Yes

Table 28: Incident Reporting - Maintainability and portability requirements

6.6.5 Social and Political Requirements

No social or political requirements have been identified at this point.

6.6.6 Legal and Regulatory Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
IR-LR01	SDLC	NIS Directive, to be adopted by each Member State at latest by May 2018, introduces additional incident reporting requirements for Operators of Essential Services. They shall be identified by each Member State by November 2018. Within the directive, they are only defined the general criteria to be taken into account and the minimum set of information to be provided. Specific procedures should be defined at national level.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-LR02	GDPR	EU privacy regulation entered into force in May 2018, introducing the obligation to report Personal Data Breach resulting in a Risk to Right and Freedom of individuals, to the National Competent Authority. The Regulation and the related Guidelines do not introduce specific thresholds to assess the need for reporting personal data breach, but provide some general criteria in order to assess the Risk to the Right and	IR-UC1, IR-UC2, IR-UC3	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		Freedom and the minimum set of information to be reported. Each Member State should define the operational procedure for reporting to the National Competent Authority, along with the templates for reporting.			
IR-LR03	SDLC	The regulation has introduced since July 2016 the obligations to report security incident for Trust Service Providers. The assessment criteria and the set of information to be provided are defined into the ENISA Guidance on Incident reporting for eIDAS. The National Competent Authority in each MS has adopted the requirement defined in the regulation, eventually defining a template for communication.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-LR04	SDLC	The ECB framework entered into force in July 2017 and foresees specific thresholds to assess the need for reporting a cyber incident to the ECB. Templates and operational procedure for reporting are defined.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-LR05	SDLC	The Directive entered into force in January 2018, and foresees the reporting of Security incident (cyber and operational) for Payment Service Providers, under certain specific conditions, to the National Competent Authority. Due to MS delays in implementing the directive, the EC has extended the period for adoption of the Incident reporting requirement till the end of the first quarter 2018. Templates and procedures have been defined by EBA into the Guidelines on Incident reporting under PSD2, and should be adopted by the National Competent Authority.	IR-UC1, IR-UC2, IR-UC3	High	Yes
IR-LR06	SDLC	Financial Institutions participating in Target2 system have to comply with the operational procedures as defined by the ECB. Critical participants have to comply with the requirement	IR-UC1, IR-UC2, IR-UC3	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		to report Incident causing an interruption of the Target2 system. Templates and procedures are defined into the Operational Guide, and adopted by the Responsible National Central Bank.			

Table 29: Incident Reporting - Legal and Regulatory requirements

6.7 Mandated Constraints

No mandated constraints have been identified at this point.

6.8 Relevant Facts and Assumptions

6.8.1 Facts

No relevant facts affecting the system have been identified at this point.

6.8.2 Assumptions

No assumptions about the system have been identified at this point.

6.9 Related WP3 and WP4 Tasks

One of the partners involved in the demonstrator presented in this task is also actively involved in tasks of WP3 and WP4. In this section, we provide a short discussion of how work presented in this demonstrator is related to tasks of WP3 and WP4.

In particular, WP3 defines all common research. related to development of technologies that are leveraged in the various demonstrators of WP5. Here, we include some tasks of WP3 that provide techniques that are useful for the incident reporting demonstrator.

- **T3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies** (partner involved: ATOS). Most of the enablers provided in this task are focused on security and privacy topics, which are not directly related to the Incident Reporting demonstration case requirements, such as solutions for IoT devices. However, some of them related to identity management and authentication will be explored for its potential integration in the demonstrator for user management.
- **T3.4: Security Intelligence** (partner involved: ATOS): The goal of this task, as it is defined in the CyberSec4EU proposal, is "to define the requirements and mechanisms to share digital evidence between the different expert systems, providing solutions to allow interoperability, either through the unification of languages, formats and interfaces, or through trusted intermediate translators systems respecting the privacy, business requirements and the regulations of the different countries", which is in line with some of the incident reporting demonstrator objectives.
- **T3.5: Adaptive Security (**partner involved*:* ATOS**):** This task is focused on providing flexible security solutions that can be adapted in response to security changes. In the incident reporting demonstrator, it is required to include solutions that can adapt the response to security incidents according to different regulations based on the event impact severity.

- **T3.6: Usable Security (Human-centred Cybersecurity):** The incident reporting involves the human interaction in a double sense, when the information about a security incident is collected and when the report notified to the Supervisory Authorities is processed. Consequently, the recommendations and guidelines provided by this task about usability can be also relevant for the incident reporting demonstrator.
- **T3.7: Regulatory Sources for citizen-friendly Goals** (partner involved: ATOS): In this task, it will be investigated the compliance with EU regulations such as eIDAS or GDPR, which are also considered in the incident reporting demonstrator.

WP4 aims at creating a common roadmap that represents the joint effort of all the various demonstrators of the project. **T4.1 (Vertical stakeholders engagement and consultation)** involves to all vertical stakeholders (end users and industrial participants), including the incident reporting vertical, with the goal of analysing the different industries to identify their main issues and challenges and collect their requirements. **Task 4.2 (Legal and regulatory requirements)** will “identify the unique European Legal and Regulatory Requirements (such as the GDPR, the NIS directive and the ePriva-cy Regulation, PSD2 and eIDAS)” which defines the legal framework where the mandatory incident reporting will be applied and the considerations to be taken in the demonstrator. The research challenges and roadmap related to T5.4 for the incident reporting industrial challenge, are documented in the task **T4.7 (Roadmap for industrial challenge 5.4)**. The task **T4.3 (Mapping and roadmap design)** will indicate the steps and guidelines to be followed by task 4.7.

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3	✓	✓		✓		✓	✓			
WP4	✓	✓	✓				✓			

Table 30: Incident Reporting - Relationship with WP3 and WP4 tasks

7 Maritime Transport

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled 'Maritime Transport'. We first provide a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

In the Maritime Transport sector, various stakeholders present complex interdependencies, which hint to different security goals and requirements. At the same time, the threat landscape of the MT is continuously evolving due to increased technology integration, to operational and to business needs of this sector. Since the MT has been identified as a critical sector for several member states, being a core mean of transportation, one of the goals set for this demonstrator is to develop a novel threat and risk management solution, that will assist in providing increased resilience against cyber threats, by providing a dynamic risk assessment environment and targeted security solutions, such as system hardening services (project **Innovation Objective 1**).

Furthermore, the MT demonstrator aims to strengthen the research and innovation competence within the CS4E partners, but also to broaden these capacities by the engagement of relevant associates from the MT sector in this demonstrator(project **Policy Objective 2**). In addition, in strict collaboration with T4.8, the MT demonstrator aims to assist in the development of a research and innovation roadmap, by actively interacting in the definition and the evaluation of the MT roadmap, and also by acting as a testbed for the methodologies and tools presented throughout the roadmap(project **Technical Objective 1**).

7.1 Goals

The Maritime Transport demonstrator is a representative example of a collaborative and complex process that involves domestic and international transportation, communications and information technology, warehouse management, order and inventory control, materials handling and import/export facilitation, among others. The maritime transport services include various interactions and tasks among the various entities engaged (stakeholders and actors) having different goals and requirements. In particular it includes a number of interactions and tasks that involve several physical (docking of the ship, stevedoring, loading, unloading, storage, transportation, inspection, etc) and cyber (pre-arrival notifications, customs clearance documentation management, ISPS declaration, etc) operations, interconnections and assets.

Obviously, the maritime ecosystem is characterized by significant (inter) dependencies among the involved actors thus we need to treat internal, external and diffused cyberthreats for the entire maritime ecosystem. In this context, the aim of this demonstration case is to contribute to the effective protection of the maritime transport that arises from the interconnections and interdependencies of a set of maritime entities, such as port authorities, ministries, maritime companies, ship industry, customs agencies, maritime/ insurance companies other transport CIIs (e.g. airports) and other CIIs (e.g. transport networks, energy networks, telco networks). Therefore, there is an emerging need for new innovative approach that facilitates the identification, analysis, assessment and mitigation of the organization-wise and interdependent cyber threats, vulnerabilities and risks.

Within the scope of the maritime transport demo case is to identify and to implement targeted security services that will ensure high levels of security for various critical maritime transport services, covering: the threat and risk management; the trust and key management services; the security of the communications in respect to the trust and key management services; and the software hardening of critical systems.

7.1.1 Identification of Critical Maritime Transport Services

The transport sector has been identified as a critical sector for the European Union, since the proper operation of transport services and infrastructures is crucial for the wellbeing of people and citizens, the economy and the society in general. Maritime transport is an important subsector; although the criticality level of Maritime Transport services may differ in the member states, in general maritime services may provide vital operations to people transport (e.g. for commuting, leisure or healthcare related reasons) and goods transport, including fuel, food, consumer goods and in general, the support of the supply chain. In order to identify and analyze the relevant security challenges, the Maritime Transport demonstrator will base its pilot operations by exploring the security challenges involved in a number of critical maritime transport services (see Table 31):

People Transfer	
Passengers Transport Service	It includes all the relevant operations and formalities required for the passengers' maritime transportation.
Cruise Service	It provides sea crossings for tourist travel (i.e. tourist travel as utility).
Goods Transfer	
Tanker Transport Service	It includes the transport of coal tar, carbon black feedstock, creosote oil, fuel oil and other petroleum/black products
LNG (Liquefied Natural Gas) Transport Service	A special instance of fuel transport service. It involves the transport of liquefied natural gas from the liquefaction plant (production/extraction) to the supply station. Once natural gas has been liquefied it can easily be shipped by tanker to receiving LNG terminals. On arrival at the terminal, the LNG is "regasified" (turned back into a gaseous state), before being injected into the natural gas transmission system (by trucks or pipelines).
Vehicles' Transport Service	A massively complex transport service with numerous players, including shippers, transport operators that involve the shipment and receipt of various types of vehicles and equipment such as trucks, vans, truck trailers and threshing machines.
Dry Bulk Cargo Transport Service	It includes the transport of large quantities of goods without packaging or packing where the means of transport itself acts as a container. In particular, dry bulk commodity cargo is is anything (usually raw material) that is shipped in large, unpackaged parcels like coal, iron ore, gravel and grain.
General Cargo & Container Transport Service	The goods are transported in containers or packages (TEU containers, sacks, boxes, barrels, bales, crates, bundles, coils and pallets, etc.).

Table 31: Maritime Transport - A non-exhaustive list of critical maritime transport services

Although those services do not represent an exhaustive list, they can be considered as representative examples of critical services to security and economics, taking into consideration suggestions from the maritime stakeholders and knowledge gained from past European projects and initiatives of the participants involved in this case, dealing with maritime operations (e.g. SUPPORT, CYSM, S-PORT, MEDUSA, MITIGATE and SAURON).

7.2 Stakeholders

The **Maritime Transport** ecosystem is complex environment with numerous players, including shippers and transport operators. Port authorities (which are public or private-public organizations) and port operators (private organizations) along with terminal operators are the main identified stakeholders. The key entities stakeholders involved in this environment are the following:

- **Cargo owners:** Cargo owners are any entity upstream or downstream the maritime transport services who owns the cargo to be transported, both to be exported or imported.
- **Government-related stakeholders:** the following government related stakeholders are identified:
    - **Shareholders**: Many port authorities have a total or partial state ownership and/or having private/public shareholders in their managing board.
    - **Customs**: It is an authority or agency in a country responsible for collecting tariffs and for controlling the flow of goods.
    - **Health and biosecurity inspection**: They represent agencies or authorities appointed by a country government (Health, Food and Environmental Depts or Ministries) usually working closely to customs agencies for controlling items that could contain harmful substances capable of causing and propagating diseases or pathologies or even affect the local environment and checking for the compliance with national laws and environmental issues.
    - **PSC Inspections**: Appointed by a national authority, usually under the control of the Harbour Master, they are in charge of inspecting vessels in order to ensure the accomplishment of national/international regulation in vessel traffic and safety.
    - **State security and protection forces (police, civil protection, army, etc.)**: They are committed to the detection and prevention of illegal traffic, illicit acts and other crimes and to the prevention and response to accidents and crisis.
- **Shipping lines:** A shipping line is a business that transports cargo aboard ships. The business may either be ship owners or not own ships and act as charterers.
- **Marine services providers:**
    - **Linesmen (mooring services):** They are professionals dedicated to ships mooring from the shore side.
    - **Pilotage:** It is a port service that directs the movement of a ship through port waters by visual or electronic observations of recognizable landmarks to provide safe vessel mooring or unmooring.
    - **Towage:** It is another port service consisting of manoeuvring vessels by pushing or towing them in a crowded or complex harbour or a narrow canal, or those that cannot move by themselves, such as barges, disabled ships, log rafts, or oil platforms.
    - **Bunkering:** It refers to the storage and supply of fuel oil to maritime vessels.
    - **Maintenance Services**:It includes a wide set of services for ships such as repairs, supplies (water, electricity, provisioning, etc.).
    - **Slipways:** It is a service for moving ships/boats to/from the water by the use of ramps. in shipyards when a ship is under construction or under repair.
- **Stevedores:** They represent firms or individuals engaged in the loading or unloading of a vessel handling the port equipment (ship-to-shore cranes, yard tractors, forklifts, etc.), in addition to various other dockside duties and responsibilities.
- **Logistics providers:**

  - **Cargo agents:** A cargo agent has three primary responsibilities: provide quotations to potential clients, complete shipping and customs documentation, and arrange for parcel transportation.
  - **Local Agent:** He has the primary responsibility to complete shipping and logistics documentation, clearance procedures and arrange for vehicle/cargo transportation.
  - **Freight forwarder**: A freight forwarder, also known as a non-vessel operating common carrier (NVOCC), is a person or company that organizes shipments for individuals or corporations to provide goods from the manufacturer or producer to a market, customer or final point of distribution.
  - **Haulier:** An entity responsible for the main transport of goods.
  - **Charterer:** Chartering is an activity within the shipping industry. A charterer may own cargo and employ a shipbroker to find a ship to deliver the cargo for a certain price, called freight rate or may be a party without a cargo who takes a vessel on charter for a specified period from the owner and then trades the ship to carry cargoes at a profit above the hire rate.
  - **Transport manager:** A transport manager is a company or a person responsible for the execution, direction, and coordination of all transportation matters within a company or organization.
  - **Ship-owners:** A ship-owner is the owner of a merchant vessel (commercial ship).
  - **3PL/4PL Contractors:** 3PL and 4PL stand for “third party” and “fourth party” logistics. A 3PL is a firm that provides service to its customers of outsourced (or "third party") logistics services for part, or all of their supply chain management functions. A fourth party logistics provider has no own transport assets or warehouse capacity. It has an evocative and integration function within a supply chain, to increase its efficiency.

- **Trade facilitators:** They represent associations of carriers, cargo managers, shipping companies, traders, etc.; aimed at providing to the logistics community a wide range of services such as consultancy, documentary management, training, information, fee reductions, etc.

- **Transaction facilitators:**
  - **Shipping agent / Cargo broker:** They are the designated persons or agencies responsible for handling shipments and cargo at ports and harbors worldwide on behalf of shipping companies. In some parts of the world, these agents are referred to as port agents or cargo brokers.
  - **Consignees:** They are parties (usually buyers) named by the consignor (usually a seller) in transportation documents as the parties to whose order of consignment will be delivered at the port of destination.
  - **Shipbrokers:** Ship broking is a financial service, which forms part of the global shipping industry. Shipbrokers are specialists intermediaries/negotiators (i.e. brokers) between ship owners and charterers who use ships to transport cargo, or between buyers and sellers of ships.
  - **Customs brokers:** It is a profession that involves the "clearing" of goods through customs barriers for importers and exporters (usually businesses).
  - **IT Providers:** They represent companies or agencies contracted by or belonging to a Port Management Company or Port Authority entrusted to provide IT solutions for the management of port operations, documents, services, etc.
  - **Financial Holdings (Banks):** Port Authorities require to be in close relation with banks and financing entities to charge fees for their services, manage economical transactions among different parties and for their staff or make huge investments for technology, physical infrastructures, etc.
  - **Insurance companies:** The provision of critical services in critical infrastructures such as ports is not exempt of risks of any type. Therefore, Port Authorities count on appropriate insurances, to face accidents, thefts and even attacks or cyber-attacks.
  - **Marine Underwriter:** A Marine Underwriter is a financial actor, usually contracted by the Insurance Company, who provides insurance coverage both for the vessel and the freight that

  are transported evaluating the risks of insuring and setting premium pricing for the Insurance Company.
  - **Authorized Economic Operator (AEO):** An entity that complies with supply chain security standards (e.g. from World Customs Organization WCO)

- **Infrastructure providers:**
  - **Services contractors:** Ports, depending on their nature, count on many types of services contractors such as mooring, pilotage towage, management of ship-generated waste/garbage.
  - **Maintenance:** Ports are structures with many facilities and installations which require appropriate maintenance including electrical lines, data lines, IT and infrastructure, etc.
  - **Installation: It** includes the provision of any type of installation within the port area, such as gas, electricity, water, safety and security, telecommunication, etc.
  - **Land-side infrastructure contractors:** Providers of cranes, tractors, vehicles, in container and bulk terminals, etc.
  - **Marine infrastructure contractors:** Providers of auxiliary boats, tugs, bunkering platforms, etc.
  - **Security contractors:** Private security companies providing staff, vehicles, scanners, etc. for the port area security.

7.3 Actors

In this section we provide a list of actors that are actively involved in the use cases described in the sections that follow.

7.3.1 Primary

- **Port Facility Security Officer** (PFSO): A person responsible for the security of the port facility.
- **Ship Security Officers** (SSO): A person responsible for the security of the ship.
- **Port Authority**: A port is a maritime commercial facility where vessels can dock to load and discharge passengers and cargo.
- **Vessels**: A vessel, ship or boat that can transport passengers and cargo across the water. Here, all vessels are assumed to be equipped with digital communication systems, such as WiFi, 3G/4G/5G, VDES, SATCOM, etc.
- **Vessel Traffic Service** (VTS): shore-side systems (typically the coastal administration) which range from the provision of simple information messages to ships, such as position of other traffic or meterological hazard warnings, to extensive management of traffic within a port or waterway[4]
- **PKI service provider**: A Public Key Infrastructure (PKI) service provider is an entity that offers services related to the set up, operation and and management of public key cryptography.
- **Supervisory Control and Data Acquisition (SCADA)/EMS Operators:** Operators of SCADA/EMS systems related with the port and vessel operations.
- **ICT Administrators**: People responsible for the administration of ICT systems involved in the maritime sector.
- **Cybersecurity experts**: These may involve internal Port Authority cybersecurity experts, or external experts collaborating with a Port Authority.

7.3.2 Secondary

We also provide a list of secondary actors, involving both people and maritime specific systems, that according to the specific environment, might be related to the use cases.

[4] http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VesselTrafficServices.aspx

- Advanced Object Detection System (AOS)
- Automatic Identification System (AIS)
- Business Information and Tracking (BIT)
- Car Carriers
- Common Communication Network (CCN)
- Container Status System (CSS)
- Cranes (Gantry, Cargo etc.)
- Dynamic positioning system (DP)
- Electronic Chart Display and Information Systems (ECDIS)
- Excise Movement and Control System (EMCS)
- Freight Forwarder System
- Gate Operating System (GOS)
- IT Consultants and experts
- Lift-on-Lift-off vessels (LoLo)
- Onboard Safety Systems
- Port Community System (PCS)
- Port Management Information System (PMIS)
- Programmable Logic Controllers (PLC)
- Radio Communication System
- Radio Frequency Identification (RFID) tags
- Remote Terminal Units (RTUs)
- Roll–on/Roll–off vessels (RoRo)
- Sensors (e.g. Navigational Sensors)
- Ship Information System (SIS)
- Telecommunication operator
- Terminal Operating System (TOS)
- Vessel Traffic Management System (VTMS)
- Visitor Information Service
- Warehouse management system

7.3.3 Use Cases Numbers

For the above identified stakeholders and actors, the following table shows the use cases' numbers that each actor is associated with.

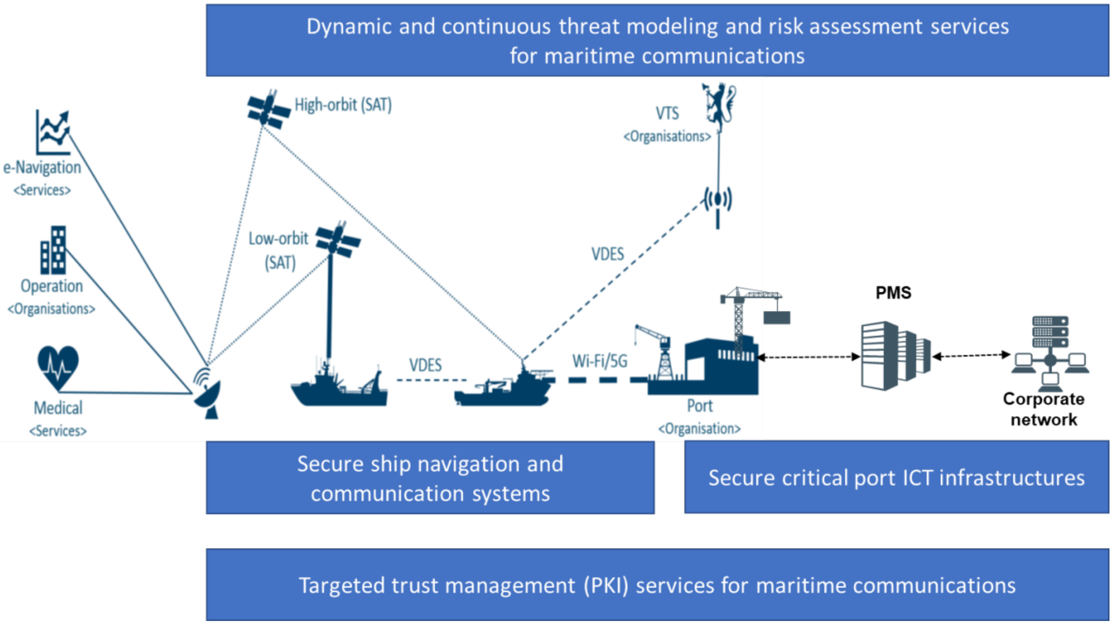
Use Cases	Stakeholders Involved	Actors Involved
MT-UC1	Port Authorities, Ship-owner, Cruise Operators, Public Administrations, Customs Authorities, Importer, Industry, Insurance Company	Port Facility Security Officer (PFSO), Ship Security Officers (SSO), ICT administrators, SCADA/EMS Operators, Cyber Security experts
MT-UC2	Port Authorities, Ship-owner	System Administrator, Security Analyst
MT-UC3	Port Authorities, Ship-owner, Cruise Operators, Public Administrations (ministries, Customs Authorities)	VTS, Vessel, Port
MT-UC4	The International Maritime Organization (IMO), Flag States, Port Authorities, Ship-owners, Cruise Operators, Public Administrations (ministries, Customs Authorities)	Vessel Traffic Services (VTS), Vessels, Ports, Public Key Infrastructure (PKI) service providers

Table 32: Maritime Transport - Mapping of actors to use cases

7.4 Functional Requirements

7.4.1 Overview of functionalities

To secure this complex, dynamic and continuously evolving ecosystem, there is a need to manage security threats and risks, to harden the security of the systems involved, and to secure the communications between the various maritime systems through the design and development of a targeted trust infrastructure that may support the underlying services of authentication, authorization, data confidentiality and integrity and service availability. Figure 18 presents an overview of the security services that will be examined in this demonstrator.



Dynamic and continuous threat modeling and risk assessment services for maritime communications

Secure ship navigation and communication systems

Secure critical port ICT infrastructures

Targeted trust management (PKI) services for maritime communications

Figure 18: Maritime Transport - Maritime transport environment and the security services demonstrated in T5.5

Future maritime communication will cover a diverse set of interactions, including information exchanges between ships, ships and organisations (such as ports, Vessel Traffic Services, and Shipping Operation centre), and ships and services (such as e-Navigation and Medical Aid Providers). The maritime transport demo will focus on identifying cybersecurity threats for the maritime environment, both at the ship side and the port side and will demonstrate the design and development of novel and targeted security services for identification, assessment and mitigation of such threats. In particular, the scope of this demo includes:

- Design threat modeling and risk assessment services for the identification and analysis of cyber and combined cyber-physical threats, both at the ship and the port side.
- Analyze security vulnerabilities of ship navigation and communication systems for ship-to-ship and ship-to-port communication to harden the security of their software components and to increase their resilience against related cyberattacks.
- Design and validate PKI for maritime communication to provide resilience against novel targeted threats.
- Use TM & RA tools to assess PKI tradeoffs (design choices, costs, security level, etc).

7.4.2 Use Cases List

The following use case have been identified and are analyzed below:

- <u>**MT-UC1 - Threat modeling and risk analysis for maritime transport services**</u>: this UC describes the functionalities related with the threat modeling and risk assessment services.

- **MT-UC2 - Maritime system software hardening**: it describes the process of software hardening for critical maritime systems.
- **MT-UC3 - Secure maritime communications** : it describes various maritime communications that require security services such as confidentiality, integrity and authentication.
- **MT-UC4 - Trust infrastructure for secure maritime communication**: it describe the functionalities related with the design of a trust infrastructure, required to support system and communication security for the maritime sector.

7.4.3 MT-UC1 – Threat Modeling and Risk Analysis for Maritime Transport Services

The interconnectivity of modern vessels and port infrastructures creates new opportunities for the maritime transport sector, but at the same time substantially increases their attack surface. Examples of relevant cyber security threats involve, remote hacking against port and vessel ICT systems, interception and manipulation of ship-to-ship and port-to-ship communication systems (e.g. AIS, ECDIS) and nearby attacks against IoT technologies, (e.g. ship navigational sensors or RFID tags used in port supply chain management). At the sane time, the list of the relevant threat agents is very dynamic and it covers a wide range of adversaries with different capabilities, access level and motivation, such as state adversaries, cyber terrorists or economic adversaries.

This use case will focus on the design and development of a targeted and dynamic threat modeling and risk assessment service for the critical maritime transport services, which can be analysed in further use cases as depicted in Figure 19. The service will be capable of identifying and assessing novel threats such as cascading threats, or threats that may be triggered by the underlying connectivity and dependencies of the critical maritime systems. A threat modeling and risk assessment service should enable the involved actors to collaboratively and securely exchange threat and risk related information, to define the scope of the assessment, to model their continuously evolving threat landscape, to assess their relevant cybersecurity threat, vulnerability, impact and risk, and to take informed decisions related with risk mitigation.

7.4.3.1 Use Case Diagram

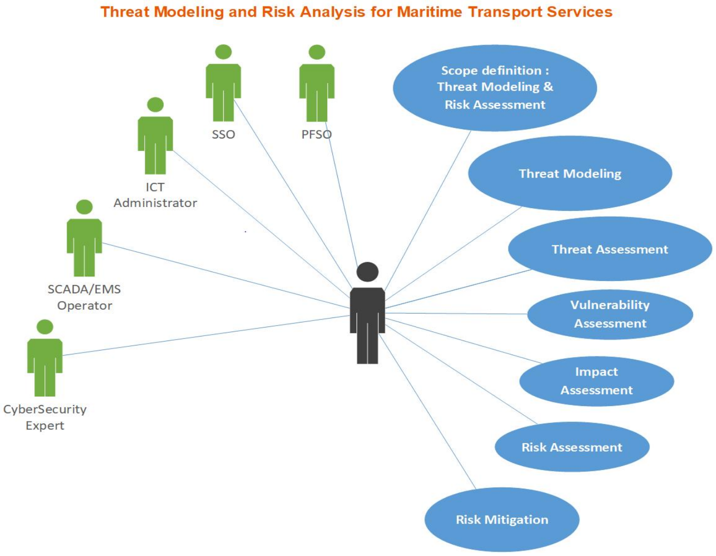


Figure 19: Maritime Transport - Threat modeling and risk analysis for maritime transport services

7.4.4 MT-UC2 - Maritime System Software Hardening

Modern vessels include various software controlled and connected systems that are critical for proper vessel operation. The vessel crew accesses internet at ports or via satellite internet as a connected part, bringing risk to vessel software systems. Software implementing these tasks can be written in safe or unsafe systems. When programs are developed in safe systems, they still execute using unsafe systems. These unsafe systems contain machine code that runs with no runtime support and therefore it is vulnerable to memory errors and corruption. With software hardening, exploitation by corrupting memory becomes harder. Even if code contains bugs, then hardening can make these bugs non-exploitable. Hardening can be applied to source code (when software can be recompiled) or directly to binaries. Protecting native code is critical, since, for example, any cryptographic operation can be bypassed if the program realizing the cryptographic algorithms can be compromised.
Moreover, hardening can be applied to the underlying OS, running in vessels or the port infrastructure, by sys admins, and to any application that includes unsafe components, as depicted in the use case diagram contained in Figure 19. In the latter case, hardening is applied by security analysts either by LLVM instrumentation, when source is available, or binary instrumentation.

7.4.4.1 Use Case Diagram

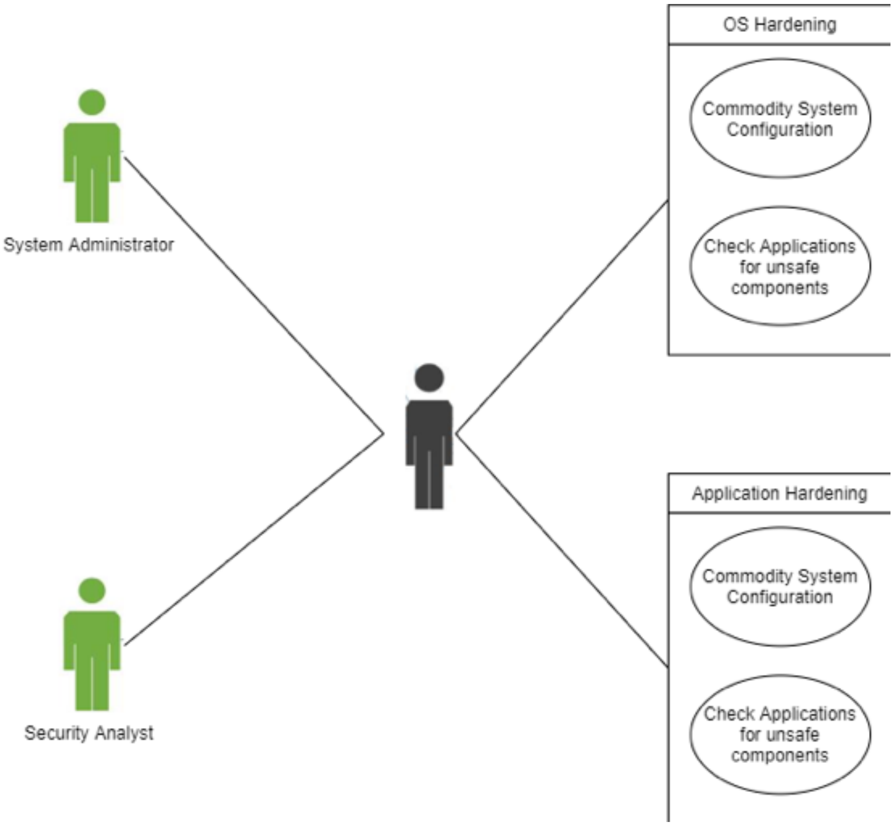

OS Hardening
Commodity System Configuration
Check Applications for unsafe components
System Administrator
Application Hardening
Commodity System Configuration
Check Applications for unsafe components
Security Analyst

Figure 20: Maritime Transport - Maritime system software hardening

7.4.5 MT-UC3 – Trusted and Secure Maritime Communications

Various type of information is exchanged in this use case. Namely:

- VDES frequencies (to be used for VTS information services)
- AIS information: Maritime Mobile Service Identity (MMSI), time, ship position, speed, rate of turn, length, course etc.

- Vessel voyage information: Route plans and mandatory ship reports
- Maritime Single Window reporting information: Ship certificates, single window reports (notifications, declarations, certifications, requests and service orders), log books, passengers' lists and crew lists.
- Port to vessel information: Weather reports, passenger or cargo manifestos, etc

The information is exchanged/transmitted between different maritime stakeholders and actors using all kinds of systems. Authenticity, integrity, availability, in some cases confidentiality, non-repudiation, resilience and privacy of the communication must be assured. To cover those requirements multiple communication systems are suggested below and depicted in Figure 21.

- VTS to Vessels broadcasting:
    - *General VTS to vessels communication.* In general, the communications should be visible to all vessels nearby.
    - *Transmission of VDES bulletin board.* A bulletin board will announce available channels and modulations through a regularly transmitted broadcast message from the VDES base stations and satellites.
    - *Transmission of DGPS corrections.*
    - *Transmission of reports and manifestos*. VTS transmits weather reports and passenger or cargo manifestos to the vessels.
- Vessel to Vessel communication:
    - *General vessel to vessel communication.* In general, the communications should be visible to all vessels nearby.
    - *AIS broadcasting:* Every vessel broadcasts to all nearby vessels information from the Automatic Identification System (AIS), which is used (among other things) to avoid collisions at sea.
- Vessel to VTS:
    - *Transmission of vessel voyage information:* Vessels transmit their route plans and mandatory SRS (Ship Reporting System) reports to VTS
- Vessel to Port:
    - *Maritime Single Window reporting:* The Maritime Single Window environment is an initiative to digitalise and harmonise ship reporting to EU countries. Digital reports are sent from the vessel to the Port through a National Single Window (NSW).

7.4.5.1 Use Case Diagram

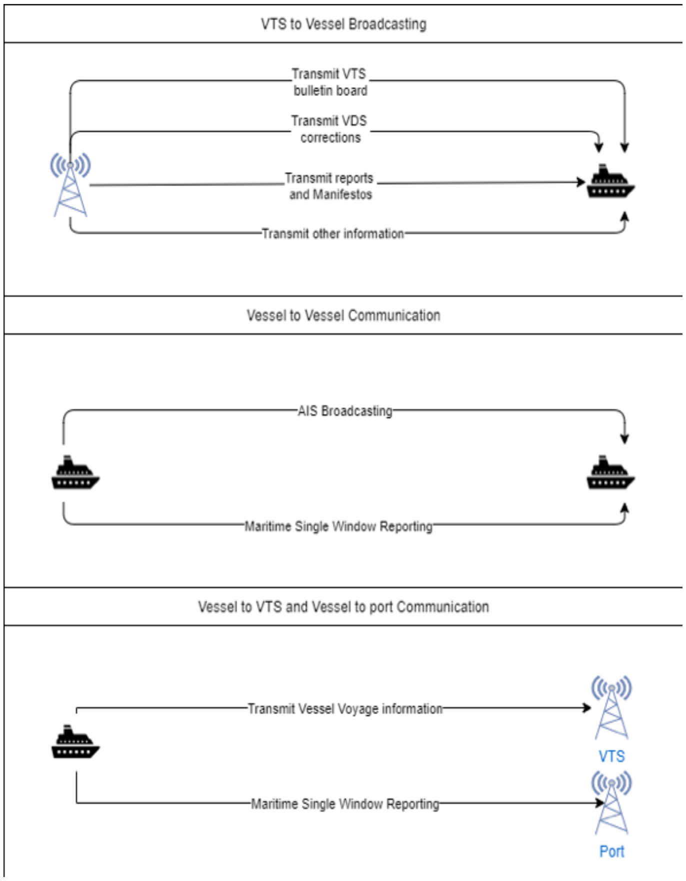

VTS to Vessel Broadcasting
Transmit VTS bulletin board
Transmit VDS corrections
Transmit reports and Manifestos
Transmit other information
Vessel to Vessel Communication
AIS Broadcasting
Maritime Single Window Reporting
Vessel to VTS and Vessel to port Communication
Transmit Vessel Voyage information
Maritime Single Window Reporting
VTS
Port

Figure 21: Maritime Transport - Trusted and secure maritime communications

7.4.6 **MT- UC4 – Trust Infrastructure for Secure Maritime Communication**

The information exchanged in this use case will belong to one or more of the following four categories:

- Message payloads
- Certificate Signing Request (CSR), which is used to issue certificates to new actors in the PKI.
- Certificate, which provides the binding between an actor and the actor's cryptographic key.
- Certificate Revocation List (CRL), which is used to revoke the certificate(s) from one or more actors in the PKI.

The information will be exchanged between different maritime actors at sea and on shore, using any of the existing or future communication systems (WiFi, VDES, SATCOM, etc). Setting up and operating a trust infrastructure, as the one depicted in Figure 22, will enable these actors to authenticate themselves and securely exchange information. This use case demonstrates establishment of a Public Key Infrastructure (PKI) service, as a means to facilitate:

- Enrolment of new actors in the circle of trust.
- Issuing of cryptographic credentials that will allow the actors to communicate securely.
- Checking the status of the cryptographic credentials.
- Exclusion of misbehaving or "expired" actors from the circle of trust.

7.4.6.1 Use Case Diagram

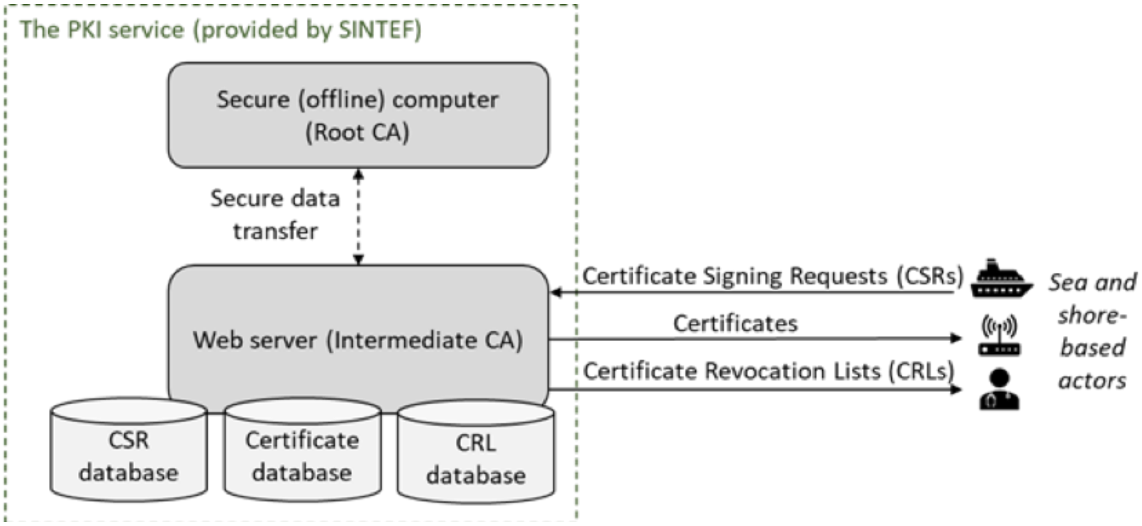

The PKI service (provided by SINTEF)
Secure (offline) computer (Root CA)
Secure data transfer
Web server (Intermediate CA)
CSR database
Certificate database
CRL database
Certificate Signing Requests (CSRs)
Certificates
Certificate Revocation Lists (CRLs)
Sea and shore-based actors

Figure 22: Maritime Transport - Trust infrastructure for secure maritime communication. The diagram shows the issuing of cryptographic credentials and enrolment of new actors

7.5 Security and Privacy Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-SP01	AE	There must be a reliable authentication mechanism to uniquely identify the persons accessing the maritime information systems (e.g. the NSW).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP02	AC	Critical information, such as security information (e.g. threat and risk assessment information) or maritime related critical information should only be available to authorized entities.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP03	AE	Access control should be implemented for vessel software systems. (e.g. limiting access to only certain systems for each user).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP04	AC	Segregation of networks between critical vessel software systems and common use systems. (e.g. between crew internet access and ship control systems).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	Low	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-SP05	AE	It must be possible to validate authenticity of the originator as well as of the destination of the transmitted data (e.g. VTS information, vessel voyage information, bulletin board data, AIS data).	MT-UC3, MT-UC4	High	Yes
MT-SP06	AC	It should be possible to establish a mutual authentication between two parties.	MT-UC3, MT-UC4	High	Yes
MT-SP07	AE	It must be possible to authenticate new actors that want to enroll into the PKI service.	MT-UC4	High	Yes
MT-SP08	AC	It must be possible to revoke users and to exclude actors.	MT-UC4	High	Yes
MT-SP09	AE	It must be possible to ensure confidentiality of the communications and of stored or processed critical information.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP10	AC	Integrity protection for all command and control systems and other critical systems (e.g. critical sensors).	MT-UC2	High	Yes
MT-SP11	AE	Integrity protection for the software, such that only updates from trusted sources get applied.	MT-UC2	High	Yes
MT-SP12	AC	There must be integrity protection of the information exchanged (e.g. VTS information, vessel voyage information, bulletin board data, AIS data), so that the maritime stakeholders/actors (vessels, VTS etc.) can verify the content.	MT-UC3	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-SP13	AE	The maritime information systems (e.g. NSW) shall give the possibility to verify the history, location, or application of the information by means of documented recorded identification: user identification, timestamp, action performed.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	Medium	Yes
MT-SP14	AC	It must be possible to verify the integrity of the active and revoked certificates (CRL).	MT-UC4	High	Yes
MT-SP15	AE	The availability of critical maritime systems must be assured.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP16	AC	The vessel must be able to transmit data (e.g. AIS information) without significant delays according to the required timing intervals (depending on speed).	MT-UC3 MT-UC4	High	Yes
MT-SP17	AE	There must be mechanisms to ensure the non-repudiation and traceability of actions performed by all persons generating, modifying or accessing the maritime information systems and data, such as the National Single Window (NSW[5]).	MT-UC3, MT-UC4	High	Yes
MT-SP19	AC	The processing or transmission of privacy-sensitive data must be compliant with protection of data regulation, i.e. General Data Protection Regulation (GDPR), Directive (EU) 2016/680, Data quality principles Regulation (EU) 2016/679, ENISA Privacy and Data Protection by Design).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes

[5] https://ec.europa.eu/transport/sites/transport/files/modes/maritime/doc/2015-06-11-nswguidelines-final.pdf

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-SP20	AE	All critical maritime systems should follow the resilience-by-design principle.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	Medium	Yes
MT-SP21	AC	The maritime stakeholders and actors (vessel and VTS etc.) must be able to detect malicious activity or states of operation that initiate need for fallback modes.	MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-SP22	AE	The PKI must be operational without online access for longer periods of time (weeks).	MT-UC4	High	Yes
MT-SP23	AC	The vessel must be able to receive and interpret older versions of the maritime information systems such as Automatic Identification Systems (AIS).	MT-UC2, MT-UC3	High	Yes

Table 33: Maritime Transport - Security and privacy requirements

7.6 Non-Functional Requirements

7.6.1 Look and Feel Requirements

No look and feel requirements have been identified at this point.

7.6.2 Usability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-U01	Usab	Entities that are not familiar with cybersecurity (non-experts) should be able to provide security-related inputs.	MT-UC1 MT-UC4	Medium	No
MT-U02	Usab	There must be ease of applying frequent software security updates to most vessels.	MT-UC2	High	Yes

Table 34: Maritime Transport – Usability requirements

7.6.3 Operational Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-OP01	Usab	There should be a collaborative approach that assists the maritime stakeholder in analyzing and assessing the security processes and possible threats associated with the ICT systems.	MT-UC1	High	Yes
MT-OP02	SDLC	There should be new algorithms and techniques for capturing, analyzing and modelling the multi-order dependencies within the maritime supply chains.	MT-UC1	Medium	Yes
MT-OP03	SDLC	There should be new techniques for predicting and representing combined attacks/threats paths and patterns and measuring their effectiveness and applicability.	MT-UC1	Medium	Yes
MT-OP04	Perfo	The PKI must be able to scale (with respect to number of certificates) for a number of users which is relevant for maritime sector.	MT-UC4	High	Yes
MT-OP05	IdM	The PKI solution must be suitable for the maritime communication infrastructure in the sense that its bandwidth often is severely limited.	MT-UC4	High	Yes
MT-OP06	Func	The PKI must be language-independent in order to be applicable in an international environment, regardless of country of origin of the participating actors.	MT-UC4	High	Yes

Table 35: Maritime Transport - Operational requirements

7.6.4 Maintainability and Portability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-MP01	SDLC	The PKI should be possible to operate by an internationally recognised trusted third party, such as IMO.	MT-UC4	High	Yes
MT-MP02	SDLC	The PKI should be applicable on top of any vessel communication systems (WiFi, VDES, SATCOM, etc).	MT-UC4	High	Yes
MT-MP03	Config	The PKI should enable migration to future cryptographic algorithms without excessive costs or efforts.	MT-UC4	High	Yes

Table 36: Maritime Transport - Maintainability and portability requirements

7.6.5 Social and Political Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-SPL01	SDLC	Compliance with the NATO Alliance Maritime Strategy.	MT-UC1, MT-UC2, MT-UC3, MT-UC4	Medium	No

Table 37: Maritime Transport - Social and political requirements

7.6.6 Legal and Regulatory Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-LR01	SDLC	Compliance with existing security standards (such as ISO27001, 27005, ISPS, ISO2800, ISO28001) associated with the protection of the maritime supply chain, mandated by law and regulation for the protection of critical infrastructures (NIS Directive, Directive 2002/21/EC, Directive (EU) 2016/1148).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MT-LR02	SDLC	Compliance with the international maritime security law and regulation (such as the SOLAS Convention, the ISPS Code).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes
MT-LR03	SDLC	Compliance with regulations on EU Critical Infrastructure (Council Directive 2008/114/EC of 8 December 2008, SEC(2008)2701: the Critical Infrastructure Warning Information Network (CIWIN).	MT-UC1, MT-UC2, MT-UC3, MT-UC4	High	Yes

Table 38: Maritime Transport - Legal and regulatory requirements

7.7 Mandated Constraints

This section gives an overview on relevant national and international standards that specify a number of rules, obligations and requirements which should be taken into consideration.

- **Information security Standards**
  - ISO / IEC 27001 - "Information security management systems - Requirements" is the normative document to which an organization that wishes to be certified must refer.
  - ISO / IEC 27002 - "Information technology - Security techniques - Code of practice for information security management" provides guidance not prescriptive to protect the information assets of a company
  - ISO / IEC 27003 - "Information technology - Security techniques - Information security management system implementation guidance provides guidelines to define a project for the implementation of a management system of information security in accordance with ISO 27001
  - ISO / IEC 27004 - "Information technology - Security techniques - Information security management - Measurement" provides the procedures and examples of construction for defining and measuring the effectiveness of the Management System for Information Security adopted by the organization and related controls of Annex A.
  - ISO / IEC 27005 - "Information technology - Security techniques - Information security risk management" provides guidance on how and steps to be taken for a correct assessment of the business risk, particularly the risk inherent in information security. This standard, in the 2011 version, has been aligned with ISO / IEC 31000 "Risk management - Principles and guidelines".
  - The ISO 28000:2007 "Specification for security management systems for the supply chain", defines the requirements for the implementation of safety management along the supply chain.
- **Maritime Security Standards**
  - International Ships and Port Facilities Security Code (ISPS)
  - International Safety Management Code
  - EC Regulation No 725/2004 on enhancing ship and port facility security
  - EC Directive 2005/65 on enhancing port security
  - MSC 96-4-1 - The Guidelines on cybersecurity on board ships
  - IMO-PKI guidance_Rev 2015
  - MSC 96-4-2 - Guidelines for Cyber risk Management
  - MSC 96-4-5 - Measures aimed at improving cybersecurity on ships
  - IEC: 2016 MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS - Cyber Risk Management Guideline

7.8 Relevant Facts and Assumptions

7.8.1 Facts

No relevant facts affecting the system have been identified at this point.

7.8.2 Assumptions

An assumption related with UC2 is that software components are implemented in unsafe programming systems (e.g., C/C++ binaries).

7.9 Related WP3 and WP4 Tasks

Several partners involved in the demonstrator presented in this task are also actively involved in tasks of WP3 and WP4. In this part we provide a short discussion of how work presented in this demonstrator is related to tasks of WP3 and WP4.

In particular, WP3 defines all common research. related to development of technologies that are leveraged in the various demonstrators of WP5. Here are some tasks of WP3 that provide techniques that are useful for the maritime demonstrator.

- **T3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies** (partners involved: CYBER, UPRC, UCY). This task defines the technology behind several security and privacy enablers. Among these enablers, several apply on the maritime demonstrator and, specifically, these are (a) identity-management and authentication over multiple non-federated providers, (b) trusted execution on IoT devices, and (c) integrity-preserving storage for processing of critical data with long-term protection requirements. The maritime demonstrator leverages technologies from all these domains. For instance, identity management over multiple non-federated providers is critical, since several different components, of different origin, are involved in the demonstrator. Additionally, the demonstrator includes several IoT devices, and, finally, communication with the vessel may involve the exchange of critical information.
- **T3.3: SDL – Software Development Lifecycle** (partners involved: CYBER, SINTEF, UCY). This task explores the development lifecycle of software, from the early stages up to deployment, from a security and privacy point of view. The task focuses on secure-by-design and proactive methodologies for software development. In the maritime demonstrator, contrary to other domains and demonstrators, software can be considered legacy (hard to rewrite from scratch using new secure-by-design techniques). Nevertheless, in the maritime demonstrator, we explore the ability of unsafe software to defend against attacks by using software-hardening techniques.
- **T3.5: Adaptive Security (**(partners involved: UPRC)**:** Task 3.5 is related with research in risk assessment and threat modelling. In the maritime transport demo, open research challenges involve the study and modelling of cascading threats, as well as of risk methods that emphasize on the system survivability and the resilience of systems under attack.
- **T3.8: Conformity, Validation and Certification** (partners involved: CYBER (lead)). This task analyses technologies, system designs and implementations to determine whether the combination of cybersecurity technologies in use achieve the desired security goals, allowing to compare different systems. The task will design a security framework capable of formally defining cyber-physical attack incidents, detecting an intrusion at different levels (physical or cyber), provide a resiliency policy and generate a forensics analysis.

Furthermore, WP4 aims at creating a common roadmap that represents the joint effort of all the various demonstrators of the project. To this aspect, T4.1 engages all vertical stakeholders (end users and industrial participants) so as to collect their requirements. With this, T4.1 establishes a feedback loop with the requirements of the maritime demonstrator. Moreover, all research challenges related to T5.8 are documented in the roadmap for maritime transport, which is documented in T4.8.

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3		✓	✓		✓			✓		
WP4	✓							✓		

Table 39: Maritime Transport - Relationship with WP3 and WP4 tasks

8 Medical Data Exchange

In this section are described the requirements for the CyberSec4Europe demonstration case titled Medical Data Exchange. Firstly, a high-level overview of the demonstration case and its goals is provided, followed by a description of the actors involved. Then is provided a more detailed functional requirements using use cases, followed by a description of non-functional requirements. Finally, relevant constraints and assumption to be considered while implementing this demonstration case are reported.

8.1 Goals

The main objectives of the Medical Data Exchange demonstrator are:

- Integrate and validate the research outcomes on the cyber-security and sensitive and personal data protection for medical data sharing in a realistic environment (DAWEX Data Exchange platform) by:
  a) Enhancing the multi-lateral trust among stakeholders generating and consuming data in the medical business sector;
  b) Improving data marketplace platform trustworthiness;
  c) Generating new business opportunities.

These objectives are aligned with the following project objectives outlined in WP5 and WP3:

- **[Obj. 5.2]** To identify use cases as demonstration cases with a high impact that sufficiently supports or if possible, enhances the intentions of EU regulations and directives, such as GDPR, eIDAS and PSD2.
- **[Obj. 3.2]** Innovative research in the main topic fields of cybersecurity providing and supplying of European products and solutions adapted to different sectors' needs, as well as with a sufficient level of trust among market players.

The challenges this demonstrator will address in the health domain context when sharing sensitive data are described as follow:

- **Security and data protection aspects to ensure trust between parties**. The data exchange marketplaces have to ensure trust between all parties involved in the data ecosystem, by guaranteeing their identities, and providing them legal functionalities as well as protecting citizen's rights;
- **Guarantee the right data management from different sources** (smart wearables, hospitals, laboratories, insurance companies, pharmaceutical companies, etc.). The marketplace must assure that all data are properly protected by using privacy preserving techniques;
- **Compliance with EU laws and regulations.** Both EU companies and non-EU companies must be compliant to GDPR;
- **Improve the identity and access management.** Increasing security when both data providers and data consumers access the marketplace.

Considering the general objectives of the project, the Medical Data Exchange demonstrator participates addressing basically the following technical and the innovation objectives:

- **Technical Objective 1:** To create a research and development programme with a common research and innovation roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing;
- **Technical Objective 3:** To provide services to the community including the support of certification authorities with testing and validation labs equipped with state-of-the-art technology and expertise;

- **Innovation Objective 1**: To facilitate leadership in cybersecurity by developing novel cybersecurity solutions, products, and services for critical challenges that significantly increase the cybersecurity resilience of the European Digital Single Market;
- **Innovation Objective 2**: To reduce fragmentation by using synergies between experts from various cybersecurity domains and by building bridges between researchers and industrial communities.

8.2 Stakeholders

In the context of the health domain and, particularly, when sharing data is performed, several stakeholders are involved. We see them as stakeholders within the health data ecosystem, each with their own roles, objectives and responsibilities. Two main categories of stakeholders can be distinguished:

- General health domain stakeholders
- Specific health data sharing stakeholders

General health domain stakeholders are playing a basic role in the heath domain:

- **Policymakers**: Are those participants such as health authorities, legal and regulatory bodies, which are in charge of creating laws and regulations related to (personal) data protection and monitoring regulatory compliance when data sharing is performed. Their objective is providing the legal context to protect data subject rights.
- **Data Subjects**: The subject who owns both its personal data and its sensitive health data, and it consents to share the latter with third parties for unselfish goals or for a rewarding benefit. Examples are patients or persons that wear devices acting as data sources which generate the corresponding health data (e.g., wearables).

Specific health data sharing stakeholders are involved in the process of sharing sensitive health data of the data subjects:

- **Data providers**: Stakeholders who gather both personal data and sensitive health data from data subjects through different data sources:
    - Participants in Health EU projects;
    - Hospitals;
    - Pharmaceutical companies;
    - Health tech companies;
    - In some cases, the data subject itself can act as a data provider.
- **Data aggregators**: These stakeholders are enabled to aggregate health data and perform data analytics. Data aggregators offer protected data to data consumers through the data exchange marketplace. The retrieved and provided data must not harm the data subject's privacy. Towards this end, different privacy-preserving techniques, such as anonymization or pseudonymization, could be employed. Additionally, sensitive health data must be properly protected by using a crypto scheme, with the aim of avoiding leaks of these data subject's sensitive data. According to it, some examples of data aggregators are the following:
    - Health tech companies;
    - Municipalities;
    - Health data hubs
    - Health consortiums;
    - Health EU projects.
- **Data consumers**: Comprise a wide number of participants which use the protected data provided via the data exchange marketplace for their studies, while the data subject's privacy is still preserved:
    - Public and private research organizations;
    - Health authorities;
    - Hospitals;

  - Pharmaceutical companies;
  - Health EU projects
- **Data Exchange Marketplaces providers:** the marketplace owner is in charge of connecting the data providers with the data consumers for sharing sensitive health data, assuring at any moment the data subject's privacy across the marketplace. Services for compliance with current regulations and for assuring the data subject's rights are also provided. Additionally, the data consumers are able to upload and share processed data to marketplace.

8.3 Actors

In this section, we provide a list of actors with brief descriptions. Actors are all the entities that interact with the Medical Data Exchange marketplace. They can be of two types: (i) Primary actors, which are actors that have goals which this demonstration case needs to fulfil; and (ii) Secondary actors, which do not have specific goals associated with this demonstration case but are needed for the execution of its use cases.

8.3.1 Primary

Actors who provides the data to be shared and those who consume such data have a main role in the envisaged use cases:

- **Health tech companies**: they provide data subject's health data, aggregates health data from users' wearables;
- **Pharmaceutical companies**: they can provide medical data and act as consumer as well;
- **Hospitals**: they provide sensitive health data from patients;
- **Research organizations and laboratories**: they consume data for research purposes;
- **French Health data hub**: gathering anonymized data from private players and consumes data for study purposes;
- **Municipalities**: that gather data collected from different public institutions;
- **French health consortium** is a private initiative made up by several companies and supported by the French government, gathering both private and public institutions.
- **MyHealthMyData EU project**[6]: they provide synthetic data and also consumes aggregated data.

8.3.2 Secondary

Actors who do not participate during the data sharing, but they are needed to fulfil this process.
Health data exchange marketplace and **privacy preserving tools system** that will be applied are necessary for completing the described use case scenarios.

- **Wearable provider**: provides devices for retrieving health data subject's data;
- **Infrastructure providers**: provides infrastructure for connecting data providers with data consumers and monetize the data exchange for all the stakeholders involved.

8.3.3 Use Cases Numbers

Table 40 associates the actors involved for each use case in the Medical Data Exchange demonstrator.

[6] http://www.myhealthmydata.eu/

ACTORS	MD-UC1	MD-UC2	MD-UC3
Hospitals	X	X	X
Pharmaceutical companies	X	X	X
Health tech companies	X	X	X
Data subject	X	X	X
Municipalities	X	X	X
French consortium	X	X	X
Dawex GDM EU project	X	X	X
Public and private research organizations	X	X	X
Health authorities	X	X	X
Pharmaceutical companies	X	X	X
Insurance companies	X	X	X
French Health data hub	X	X	X
Wearable provider	X	X	
Health data exchange marketplace provider	X	X	X

Table 40: Medical Data Exchange - Mapping of actors to use cases

8.4 Functional Requirements

In this section, we provide a brief description of these demonstration case functionalities, along with a list of use cases implementing them.

8.4.1 Overview of functionalities

With the goal of allowing the exchange of sensitive medical and health data through the Dawex data exchange marketplace, different challenges related to security and privacy of such data need to be addressed. Particularly, health data must be protected in order to avoid leaks of sensitive information and ensure data integrity between the stakeholders. Furthermore, and according to the EU laws and regulations (e.g., GDPR), data subjects' privacy must be guaranteed, assuring a correct management of their data. Additionally, identity management at the exchange marketplace need to be improved, with the aim of properly validating the stakeholders' identities. According to it, we propose a generic use case, which is shown in Figure 23.

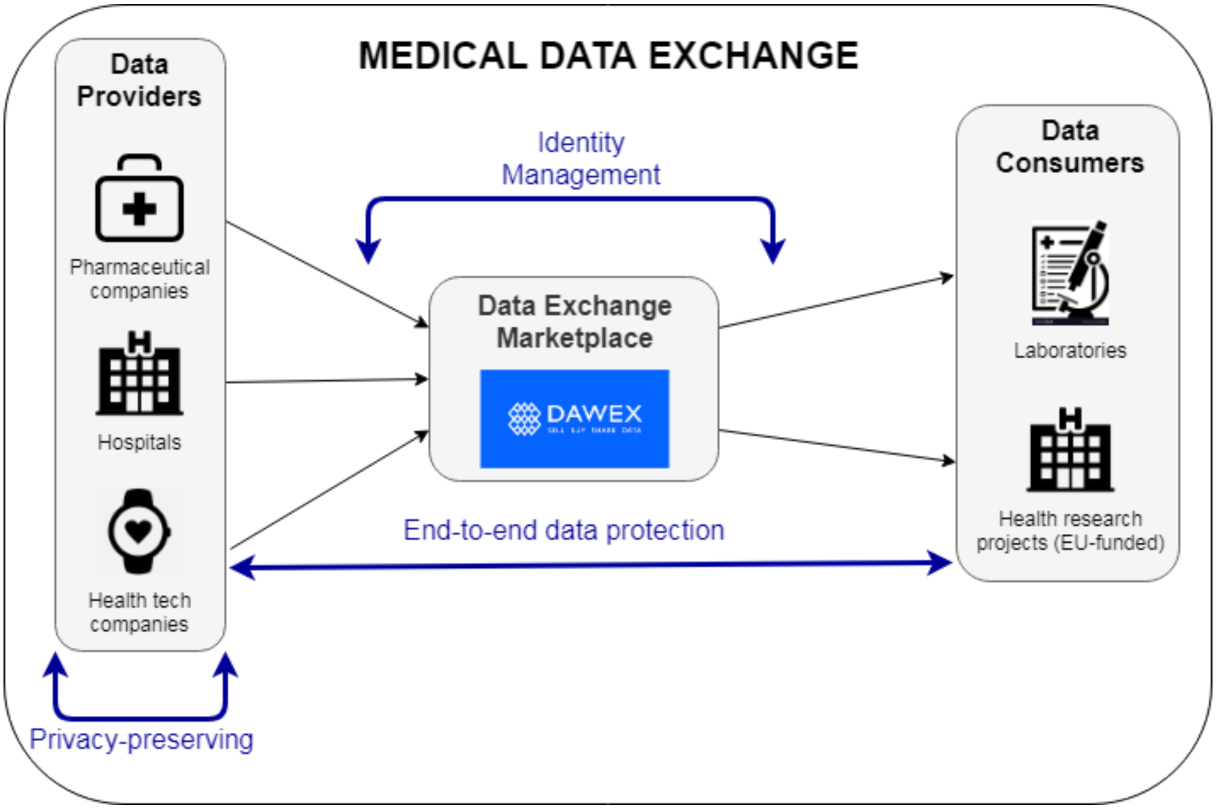


Figure 23: Medical Data Exchange - Generic Use Case

This generic use case allows the exchange of sensitive health data through the Dawex data exchange marketplace between different stakeholders, also addressing the security and privacy challenges previously pointed out. Specifically, we integrate the most relevant and innovative tools and methods in cybersecurity in order to ensure confidentiality and integrity of shared health data (e.g., by using functional encryption, homomorphic encryption or multi party computation), as well as to preserve privacy of involved subjects sharing such health data (e.g., by employing data anonymization or pseudonymization techniques). Similarly, we also propose the use of strong authentication mechanisms and emerging decentralized technologies (e.g., eIDAS or Blockchain) to improve the stakeholders' identity management at the data exchange marketplace. Regarding the stakeholders, we consider pharmaceutical companies, hospitals and health tech companies on the data provider side, among others. On the data consumer side, laboratories and Dawex GDM EU project[7] are involved. Furthermore, data are mapped into a common data model using standard biomedical terminologies at the metadata level, so that their scope, volume and relevant characteristics can be easily viewed and evaluated by data consumers (i.e., data buyers) through the Dawex exchange marketplace. To facilitate this process, data visualisation tools will be integrated, thereby facilitating user experience.

8.4.2 Use Cases List

Based on the indicated generic use case, the envisaged UCs for the Medical Data Exchange are the following

- **MD-UC1 - Sharing Sensitive Health Data through an API**: Protected sensitive health data are shared by using an API that is made available through the data exchange marketplace;
- **MD-UC2 - Sharing Sensitive Health Data through Files**: Protected sensitive health data are shared by using files that are stored and made available through the data exchange marketplace;

[7] https://cordis.europa.eu/project/rcn/218537/factsheet/en

- **MD-UC3 – Enhancing the security of on-boarding and accessing the Dawex exchange marketplace**: Security for on-boarding and accessing process to the data exchange marketplace is enhanced through strong authentication by using the eIDAS network and blockchain technology.

8.4.3 MD-UC1 - Sharing Sensitive Health Data through an API

In this use case (see Figure 24), the data provider gathers both personal data and sensitive health data from a specific data source, such as a user's wearable (step 1). Note that this provider must have previously acquired consent of the corresponding data owner in order to manage such data. Specifically, we consider data providers as legal persons (e.g., health tech companies, municipalities, French Heath Hub consortium) uploading health data as a report or medical tests. These data providers are able to aggregate health data coming from different sources and perform certain data analytics with them, so that they also play the data aggregator role. Therefore, they must also be in charge of preserving data subjects' privacy, as well as properly protecting shared health data. Moreover, with the aim of monetizing the stored health data, the data provider makes them available to interested buyers by providing related metadata on the data exchange marketplace catalogue (step 2). Then, a data consumer (e.g., a medical laboratory) that is enabled to browse the catalogue (step 3) looks for an appropriate set of data in which it is interested. In this sense, information about how to treat the data will be provided (depending on the kind of crypto techniques applied during browse data protection process). To make this browsing easier, data visualization tools (provided by Dawex) will be used, thus improving the user experience, as already mentioned. Subsequently, the data consumer contacts the data provider to agree the terms and conditions about the management of the further requested data. It should be pointed out that this step is made through specific contract services that the Dawex marketplace supplies. Then, the data consumer requests health data to the data provider (step 4), which uses a data protection service (step 5) enabled to preserve data subject's privacy by using data anonymization or pseudonymization techniques. Additionally, this service also allows to encrypt the requested health data by employing an encryption schema, such as functional encryption, homomorphic encryption and so on. Note that the data protection service may be provided by the marketplace or by a third party in different ways:

- As a jar file to be integrated in the data provider system;
- As a standalone REST service to be deployed on the data provider environment;
- As a marketplace service itself.

Finally, the data consumer retrieves the protected data through the marketplace (step 6) and then, it tries to decrypt the encrypted health data. At this point, if the decryption process is successful, and the consumer recovers the heath data, such actor could perform analytics over these just obtained data (step 7). Otherwise, it only be able to perform analysis with encrypted data (e.g., by using homomorphic encryption). It should be noted that, while the data consumer is able to carry out certain analysis with received health data for the original purpose, data subjects' privacy is preserved in any moment.

Moreover, it should be clarified that data protection on data sources (e.g., on user wearables) when they act as data providers is out of scope of this demonstrator. Then, the data provider should oversee:

- Obtaining consent of the data subject who is the owner of the shared health data in order to properly manage such data;
- Preserving data subject's privacy on the data provider system;
- Complying with the data owner rights.

8.4.3.1 Use Case Diagram

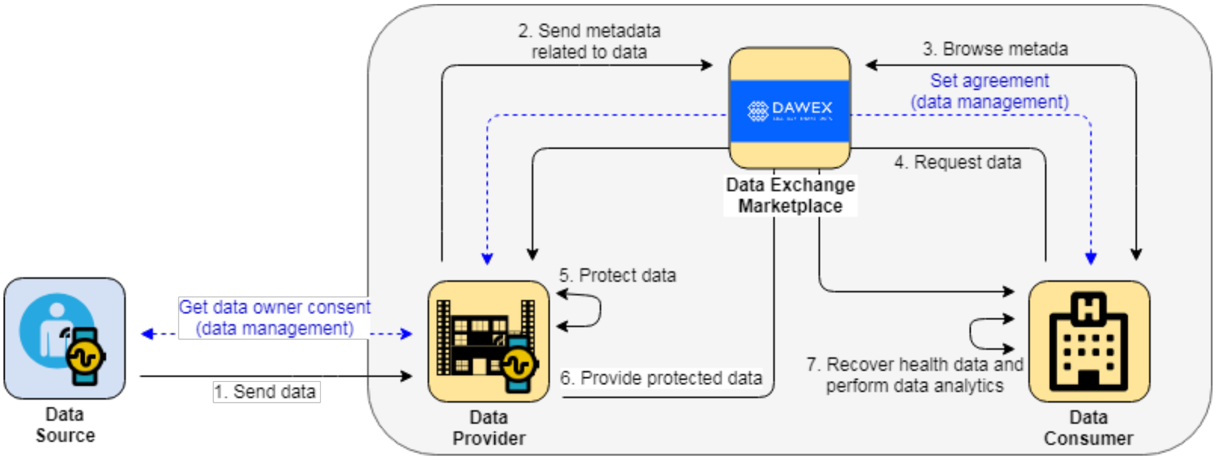

2. Send metadata related to data
3. Browse metada
Set agreement (data management)
4. Request data
DAWEX
Data Exchange Marketplace
5. Protect data
Get data owner consent (data management)
1. Send data
6. Provide protected data
7. Recover health data and perform data analytics
Data Source
Data Provider
Data Consumer

Figure 24: Medical Data Exchange - UC1 Overview

8.4.4 MD-UC2 - Sharing Sensitive Health Data through Files

This use case (see Figure 25) differs from the previous one, when health data are included and shared through files, which are in turn stored in the data exchange marketplace. Therefore, many of the interactions are similar. For this specific reason, those that are different, have been described. Specifically, when the provider receives data from a source (step 1), the former launches the data protection service over the received data before of generating a file and include them on it, so that unauthorized accesses to the health data are avoided and data subject's privacy is preserved (step 2). Note that, as previously stated, the data protection service may be provided in different ways. Once this file containing protected health data is generated, the data provider uploads it on the data exchange marketplace to be shared, also including a set of related metadata. Then, when the data consumer set the agreement with the data provider, the former requests the file. It should be pointed out that, unlike in the previous use case, this request is performed to the marketplace (not to the data provider) since it is in charge of storing and providing files containing protecting health data to interested consumers (steps 5 and 6).Finally, the data consumer tries to decrypt the health data from the just received file and, if it succeeds, the consumer will be able to perform analytics over such data (step 7), while data subject's privacy is still preserved thanks to the previous data protection service.

8.4.4.1 Use Case Diagram

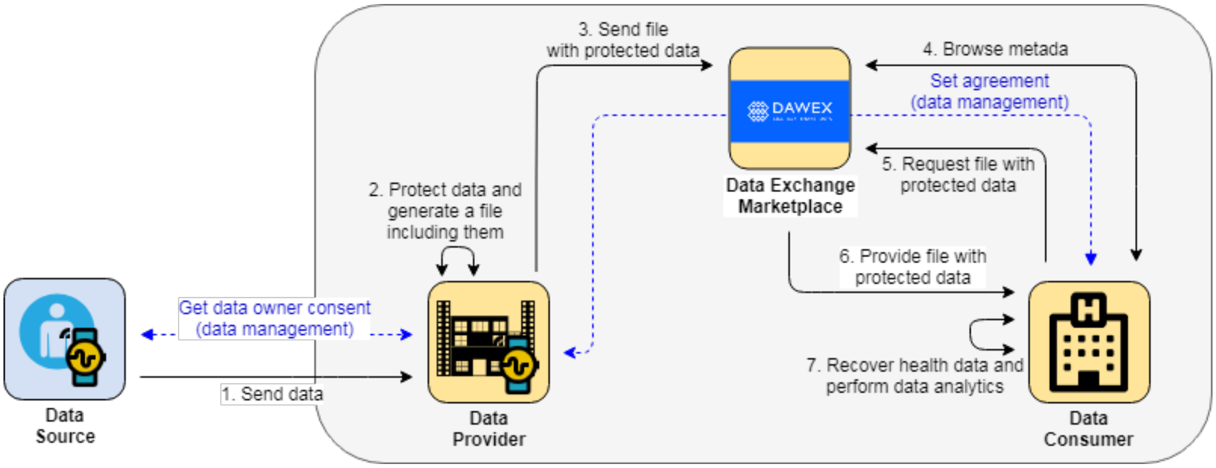

3. Send file with protected data
4. Browse metada
Set agreement (data management)
DAWEX
Data Exchange Marketplace
5. Request file with protected data
2. Protect data and generate a file including them
6. Provide file with protected data
Get data owner consent (data management)
1. Send data
7. Recover health data and perform data analytics
Data Source
Data Provider
Data Consumer

Figure 25: Medical Data Exchange - UC2 Overview

8.4.5 MD-UC3 – Enhancing the security of on-boarding and accessing the Dawex platform

The different stakeholders trying to use the Dawex marketplace need to be registered in advance. For onboarding purposes, based on the country eIDAS node availability for private sector, the Dawex data exchange platform will integrate a connection to eIDAS network for using an electronic identity issued by an EU country developing an eID scheme, under the eIDAS notification process. Currently, eIDAS network is able to authenticate natural person and is envisaged legal person would also be authenticated during the project development. This enables to improve the current online onboarding protocol on the Dawex platform, in terms or trustworthiness and assurance, thus easing both the enrolment and access processes to the platform users. This way, the user's identity is validated by a trusted party, such as an Identity Provider from an EU country, which is issuing the eID (e.g., eID card). Once the user is registered on the Dawex platform, its identity can be derived to SSI blockchain. Specifically, after the user's authentication, the platform service generates a verifiable credential, which can be stored on the user's portable SSI Wallet (e.g., in a mobile phone). By registering this credential in a blockchain ledger, the user is permanently able to provide those certifications, without depending on the availability of the initial IdP for later verifications. Figure 26 depicts the previously described scenario.

8.4.5.1 Use Case Diagram

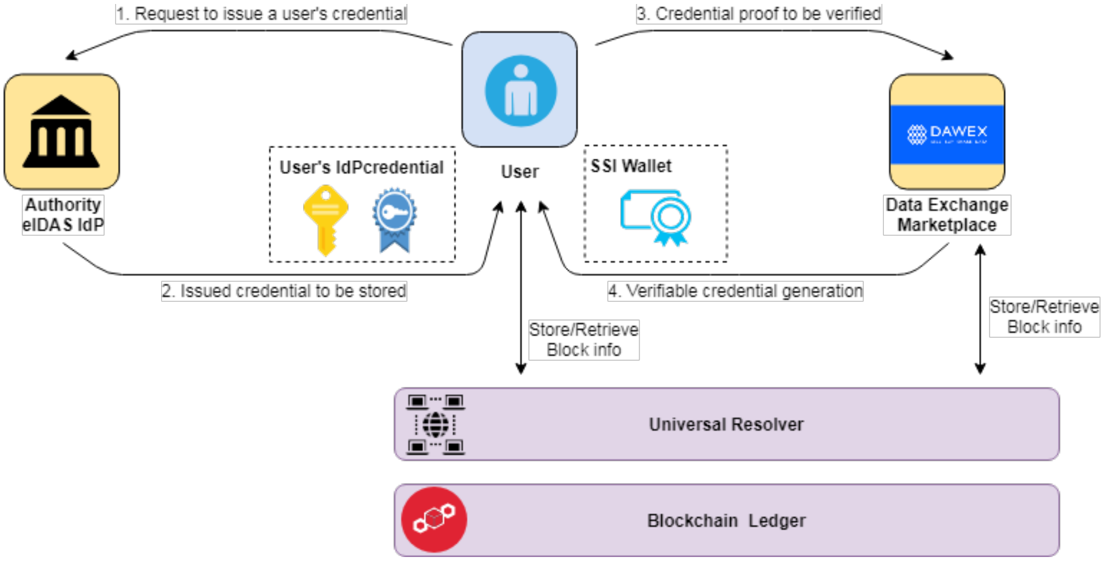

1. Request to issue a user's credential
3. Credential proof to be verified
User
Authority eIDAS IdP
User's IdPcredential
SSI Wallet
DAWEX
Data Exchange Marketplace
2. Issued credential to be stored
4. Verifiable credential generation
Store/Retrieve Block info
Store/Retrieve Block info
Universal Resolver
Blockchain Ledger

Figure 26: Medical Data Exchange - UC3 Overview

8.5 Security and Privacy Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-SP01	DPriv	When personal and sensitive data are shared, data providers must preserve the data subjects' privacy by using privacy-preserving techniques	MD-UC1 MD-UC2	High	Yes
MD-SP02	Anon	When personal and sensitive data are shared, data providers must preserve the data subjects' privacy by using anonymization tools	MD-UC1 MD-UC2	High	Yes
MD-SP03	Conf	Communications between data providers and data consumers through the platform to exchange health data must be protected by security associations, in order to avoid leaks of sensitive information	MD-UC1 MD-UC2	High	Yes
MD-SP04	DInt	Communications between data providers and data consumers through the platform to exchange health data must be protected by security associations, preserving data integrity	MD-UC1 MD-UC2	High	Yes
MD-SP05	Conf	Data subject's health data must be protected at any time by using an encryption scheme that allows to ensure their confidentiality	MD-UC1 MD-UC2	High	Yes
MD-SP06	DInt	Data subject's health data must be protected at any time by using an encryption scheme that allows to ensure their integrity	MD-UC1 MD-UC2	High	Yes
MD-SP07	AuthnE	The enrolment and the access processes to the data exchange marketplace should provide a strong authentication mechanism to ensure only those legitimate stakeholders are allowed to perform such processes	MD-UC1 MD-UC2 MD-UC3	Medium	Yes

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-SP08	Func	The marketplace must provide sharing contracts between data providers and data consumers	MD-UC1 MD-UC2	High	Yes
MD-SP09	Acc	Mechanisms for tracking data access must be provided by the marketplace (e.g., by using blockchain technology).	MD-UC3	High	Yes
MD-SP10	IdM	Decentralized identity verification should be provided by the marketplace, in order to facilitate the user access to the marketplace	MD-UC3	Medium	No
MD-SP11	IdM	eIDAS authentication should be integrated for authentication purposes for accessing the marketplace	MD-UC3	Medium	No
MD-SP12	IdM	Definition and limit the perimeter for the use of the Self Sovereign Identity based on blockchain regarding the Dawex roadmap must be provided	MD-UC3	High	Yes

Table 41: Medical Data Exchange - Security and Privacy requirements

8.6 Non-Functional Requirements

The following non-functional requirements are detected to be applied to this demonstrator.

8.6.1 Look and Feel Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-LF01	Avail	A schema for metadata must be defined and provided by Dawex marketplace. The schema must use a well-known standard (such as XSD).	MD-UC1 MD-UC2	High	Yes
MD-LF02	Avail	Metadata must be provided to the Dawex marketplace either using the marketplace interface configuration or using a supported format type such as csv, xml, json or shapefile	MD-UC1 MD-UC2	High	Yes

Table 42: Medical Data Exchange - Look and Feel requirements

8.6.2 Usability Requirements

No usability requirements have been identified at this point.

8.6.3 Operational Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-OP01	GDPR	All the legal conditions for the exchange of sensitive health data must be provided by the marketplace	MD-UC1 MD-UC2	High	Yes
MD-OP02	Avail	Definition of the taxonomy related to medical data must be provided	MD-UC1 MD-UC2	High	Yes

Table 43: Medical Data Exchange - Operational requirements

8.6.4 Maintainability and Portability Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-MP01	Usab	Marketplace should consider the final user feedback for updating the platform.	MD-UC1 MD-UC2 MD-UC3	Medium	No

Table 44: Medical Data Exchange - Maintainability and portability requirements

8.6.5 Social, Economic, and Political Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-SPL01	Anon, Unlink	Data subjects' personal data must be protected at any moment avoiding third parties can learn from the data	MD-UC1 MD-UC2	High	Yes
MD-SPL02	DPriv	Data providers must be able to provide data from multiple sources in an adequate form to data consumers for analytics.	MD-UC1 MD-UC2	High	Yes
MD-SPL03	Transp	The data exchange marketplace should allow shared data monetization. The data owner can be remunerated when its health data are used.	MD-UC1 MD-UC2 MD-UC3	Medium	No

Table 45: Medical Data Exchange - Social and political requirements

8.6.6 Legal and Regulatory Requirements

ID	REQUIREMENT	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
MD-LR01	GDPR	The data subjects' privacy must be preserved at any time. Towards this end, data providers and data consumers must fulfil the GDPR regulation and accomplish the data subjects' rights.	MD-UC1 MD-UC2	High	Yes
MD-LR02	GDPR	The marketplace must provide sharing smart contracts between data providers and data consumers	MD-UC1 MD-UC2	High	Yes

Table 46: Medical Data Exchange - Legal and Regulatory requirements

8.7 Mandated Constraints

No mandated constraints have been identified at this point.

8.8 Relevant Facts and Assumptions

8.8.1 Facts

No relevant facts affecting the system have been identified at this point.

8.8.2 Assumptions

No assumptions about the system have been identified at this point.

8.9 Related WP3 and WP4 Tasks

Some of the partners participating in this demonstrator are also engaged in tasks of WP3 and WP4. This section gives an overview of the relation between this demonstrator and tasks of WP3 and WP4. Figure 27 depicts the connection between this demonstrator with the envisaged roadmap described in T4.9, and the assets provided by T3.2 of WP3, the Medical Data Exchange demonstrator leverages.

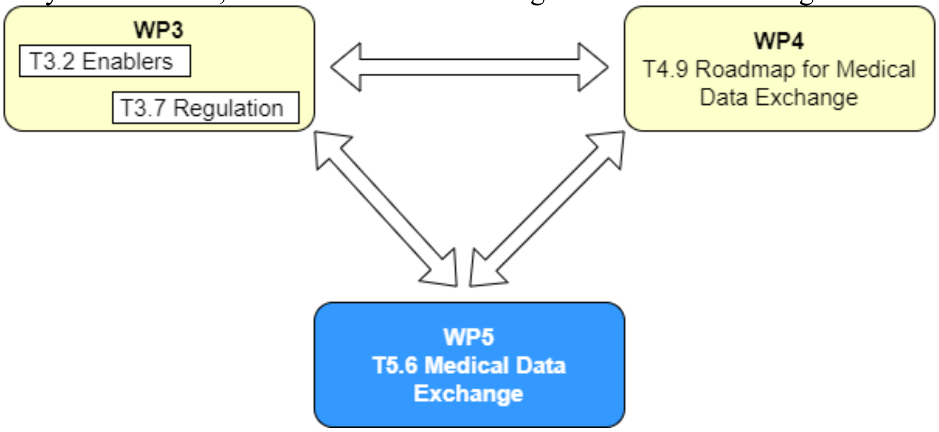

WP3
T3.2 Enablers
T3.7 Regulation
WP4
T4.9 Roadmap for Medical Data Exchange
WP5
T5.6 Medical Data Exchange

Figure 27: Medical Data Exchange - Interactions with WP3 and WP4 tasks

The Medical Data Exchange demonstrator has a close link and dependencies with following WP3 tasks:

- **Task 3.2 Research and Integration on Cybersecurity Enablers and underlying Technologies**: This task identifies the horizontal cross sectoral security and privacy enablers, like blockchain, identity management, PET and the advance over state of art, providing privacy preserving enablers, that will be used in T5.6 demonstrator. Namely the assets provided by this task involved in the Medical Data Exchange demonstrator are (a) anonymization service (DANS) and authentication service (SPeIDI). The health demonstrator leverages these provided technologies for preserving data owner privacy and for increasing security when users get access to the exchange platform.
- **Task 3.7 Regulatory Sources for citizen-friendly Goals:** This task will be focus on best practices for innovative and GDPR compliant user experience, and on the investigation of the compliance for identity technologies interoperability (e.g. eIDAS, GDPR, ePrivacy). These technologies play a main role in health demonstrator as personal and sensitive data subject's data are shared.

Additionally, WP4 aims to create a common roadmap that represents the joint effort of all the various demonstrators of the project. Regarding the health demonstrator the following tasks are involved:

- **Task 4.1**: This task collects requirements from demonstrator T5.6 and receives feedback from this task for the roadmap.
- **Task 4.3**: This task provides the steps to follow by task 4.9 related to this demonstrator, for providing a roadmap.
- **Task 4.9**: This task documents in the roadmap for health demonstrator all research challenges related to T5.6 based on the methodology explained in Task 4.3.

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3		✓					✓			
WP4	✓		✓						✓	

Table 47: Medical Data Exchange - Relationship with WP3 and WP4 tasks

9 Smart Cities

In this section, we describe the requirements for the CyberSec4Europe demonstration case titled "Smart Cities". We first provide a high-level overview of the demonstration case and its goals, highlighting the relationship with the project objectives, followed by a description of the actors involved. We then provide more detailed functional requirements using use cases, followed by a description of non-functional requirements. Of course, a specific section will focus on cyber security requirements. Finally, we report relevant constraints and assumption to be considered while implementing this demonstration case.

9.1 Goals

A fundamental point for creation of smart cities is the generation, analysis and sharing of large quantities of data. Smart city technologies capture data about people and places to all forms of privacy and day by day they drastically expand the volume, range and granularity of the data being collected and processed. However, this 'smart city' process puts individual privacy at risk, thus reducing individual trust.
Taking into account this aspect the demonstration cases linked to Murcia, Porto and Genova contexts will move around personal data exchange among citizens and other city stakeholders, mainly the Municipalities, as key player in the delivery of public services and citizens' data management. In this frame the CS4E Smart Cities demonstration cases will focus on two main aspects:

- Setup and operate a consent-based infrastructure to support city sensor networks, urban data platforms and and other data exchange infrastructures in cities & communities and enable secure personal data exchange that can be reused in public services and complies to European GDPR regulations;
- Setup an Open Innovation cycle that will drive city stakeholders from cyber security risks and needs assessment to the identification of the related solutions (i.e. cyber security services).

Both of these aspects are strictly related with the project's objectives [Obj.5.2] and specifically to the aspect related to the GDPR regulation to enable a novel ecosystem capable to foster business models based on personal data exchange and usage in Smart City and Public Services while properly managing the related cybersecurity risks and regulations compliance in order to increase user confidence concerning personal data exchange and usage and to pave the way for a cyber security competence centre on Smart City.

Finally the Smart Cities demonstration cases will also contribute to other Work Package's objectives, most significantly to:

- [Obj. 3.3] Reach an interdisciplinary cybersecurity know-how for developing next-generation digital technologies to support innovative products and services;
- [Obj. 4.2] To reduce fragmentation of cybersecurity research in Europe by providing an alignment of research activating and linking them to industrial demonstration cases;
- [Obj. 6.2] A professional, continuing education framework for employers to train and assess the cyber-security capability of their workforce.

The Smart City demonstration cases are rooted in the ambition that Local Public Administrations (LPA) should be able to adopt a set of tools to protect themselves from cyber-risks, in privacy and security, especially in order to detect and prevent such attacks over two main levels: at individual level (e.g. citizens, civil servants), and organizational level (e.g. PAs, third parties).

Starting with a co-creative process of user needs assessment, an Open Innovation environment will involve city stakeholders to identify potential solutions/best practices already included, o to include as new. in existing marketplace of cybersecurity services (e.g. OASC Catalogue) to be used by municipalities. This marketplace will offer in particular solutions that enable personal data sharing among different services and third party actors with different processing purposes in compliance with the GDPR.

Needs assessment applied in demostrations cases will be applied at individual and organizational level with a set of tools:

- At individual level:
    - a *Social Driven Vulnerability Assessment*, that simulates one of the most dangerous attack strategy, so-called Social Engineering, performed by attackers against individuals (both employees and citizens) in order to convince them to reveal personal and sensitive information of themselves and their employer;
    - an assessment tool for individuals to measure their capability to indentify phishing emails. Moreover, we aim at introducing an entire training platform that will support organizations (not only LPAs) to manage and assign specific training plans to individuals (both citizens and employees), in order to improve cyber-threats awareness and knowledge how to defend themselves from an "on-going threat reality".
- At organizational level: a Risk Assessment Tool whose aim is to help risk managers, CEOs and LPAs to have a detailed report based on discovered vulnerabilities and estimated economic impacts. The outcome of this tool is not only to provide a predictive analysis of the possible attacks and impacts that an organization may suffer from a cyber attack, but also to give a detailed plan of mitigation actions (such as awareness raising, training, security colture, security technology policies) to implement in order to minimize risks.

The Smart Cities demonstrator cases will be implemented starting from the requirements, described in the next sections and provided by CS4E partner cities Genoa, Murcia and Porto in order to implement the above-mentioned processes around personal data exchange among citizens, public administrations (PAs) and other city stakeholders.

9.2 Stakeholders

This section is devoted to the identification of the main stakeholders that are the entities that will be affected by, or who have an interest (economic, technical, political, societal, legal, etc.) in the Smart Cities demonstration case. We consider three main categories of stakeholders:

- **Local Public Administrations**: It includes all public or semi-public entities involved (administrative, public employee and other staff..) in digital transformation, smart cities processes and public service provision;
- **Service Suppliers**: Public and/or private organizations providing any type of smart city services-These services are generally processing different types of data (personal or not);
- **Platform Providers**: Public and/or private entities working with the providers of city data and services, and managing the content, defining policies and regulations of the platform.

9.3 Actors

In this section a list of actors including brief descriptions is provided. Actors are all entities interacting with one or more use cases identified for the CS4E Smart Cities demonstration case. There are two types of actors: (1) Primary actors, who are actors that have specific goals which this demonstration case needs to fulfil; and (2) secondary actors, who don't have specific goals associated with this demonstration case, but are needed for the execution of its use cases.
The two types of actors are described in more detail in the next section.

9.3.1 **Primary**

Actors who participate during the data sharing or cyber security assessment and solution elicitation and have a main role in the envisaged use cases:

- **Citizens**: operates as data subjects or end users of personalized data sharing services provided by Smart Cities service providers;
- **Service Providers**: They provide Smart Cities personalized services base on data sharing data. According to the type of services they are Data Consumers or Data Providers and hence operate both as Data Processors and Controllers according to the definition provided by GDPR Regulation;
- **City Data Publisher**: Publishes open and proprietary data into the platform. Manages and maintain resources in the platform accordingly to its terms and conditions;
- **CISO – CIO – CEO**: *Chief Information Security Officer; Chief Information Officer; Chief Executive Officer* whose aim is to support to identify and evaluate cyber-vulnerabilities and related risks and identify the most suitable solution to adopt.

9.3.2 Secondary

Actors who do not participate during the data sharing or cyber security assessment and solution elicitation but they are needed to fulfil these processes:

- **DPO – Data Protection Officer**: In the processes of the individual use cases, the DPO can access comprehensive records of all data processing activities conducted by each service provider (acting as Data Controller/Processor), including the purposes of all processing activities, which must be made public on request DPO could participate to interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information;
- **Employees**: For SMC-UC5 and SMC-UC6, to assess vulnerabilities, the solutions should evaluate even human-related vulnerabilities, such as human behaviour of employees and citizens;
- **Pen-tester**: Is a technical expert, who will be delegated by managers (or CISO) to conduct the Social Driven Vulnerability Assessment (SDVA);
- **Risk Manager**: in case of large-enterprises, Risk Management is often related to a specific profile whose aim is to identify, prioritize and evaluate risks followed by economic consequences.

9.3.3 Use Cases Numbers

Actor	SMC-UC1	SMC-UC2	SMC-UC3	SMC-UC4	SMC-UC5	SMC-UC6	SMC-UC7
Employees	X	X	X	X	X	X	X
Citizens	X	X	X	X			
Service Providers	X	X	X	X			
City Data Publisher	X	X	X	X			
CISO – CIO – CEO					X	X	X
DPO	X	X	X	X			X
Risk Manager					X	X	X
Pen-tester					X	X	

Table 48: Smart Cities - Mapping of actors to use cases

9.4 Functional Requirements

In this section we provide a brief description of the demonstration cases functionalities, along with a list of use cases implementing them.

9.4.1 Overview of functionalities

The Smart Cities Demonstration cases will support the following main functionalities.

9.4.1.1 Urban Data Platform functionalities

The urban platform provides city data in both human and machine (e.g. sensors, actuators, systems) readable and understandable formats to support interoperability between data sources and data consumers(Figure 28). The urban platform enables users to consume and publish data in a secure and privacy protected manner. User's experience is enhanced by the provision of value-added services. To this end services provide the functions for updating, maintaining and accessing services as well as tracking their usage by users in a lawful manner, assuring security and privacy.
Below the list of main functionalities:

- The platform (p/f) must provide open API so that new services exploiting the data can be built;
- The p/f must be able to accommodate multiple data sources and origins;
- Data shall be annotated, as example in the form of Linked Data (LD);
- A standard query language endpoint (like SPARQL) must be made available in order to search and retrieve data;
- It must be possible to federate multiple instances of the p/f without compromising security;
- Data annotation must include quality properties (availability, accuracy,…);
- It must be decided at run-time where (i.e. cloud level, edge) analytics are executed and then deploy functionalities accordingly;
- The p/f must support Personal Data Sharing in which personal data is accessed and used by third party companies to provide services to the city.

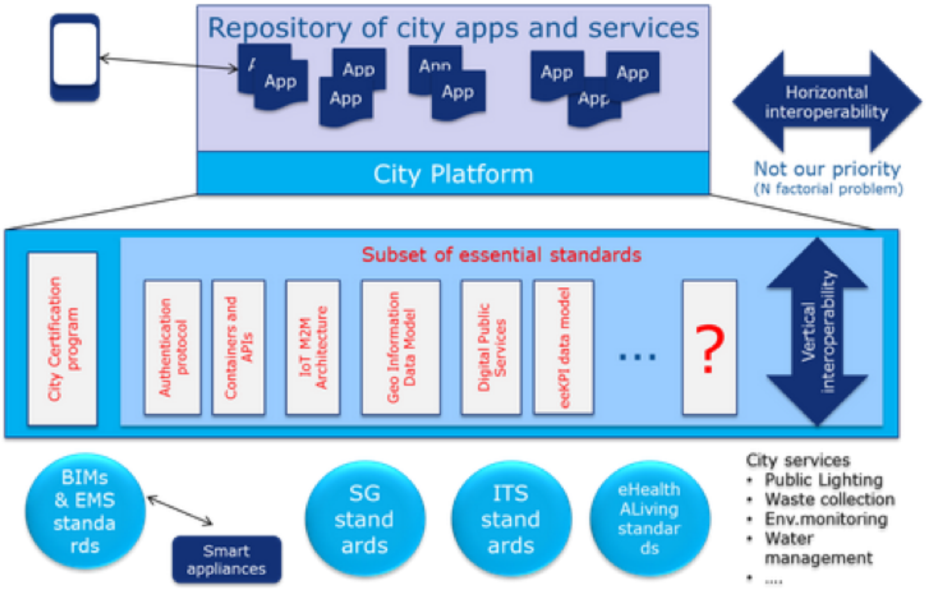


Figure 28: Smart Cities - Urban data platform

9.4.1.2 Empower the citizens to their data

The demonstration case has to support Urban Data platform for a "user-centred" personal data management (Figure 29):

- The p/f must provide mechanism to enforce privacy and data protection;
- End-users must be able to decide their own access policies as far as their personal data is concerned;.

- End-users must be able to check easily, for example with visualization tools, who has access to their data;
- The access policies must be context dependent, allowing to bypass restrictions in case of natural disaster, or emergency for instance;
- Right to be forgotten must be guaranteed (i.e. ability to erase unwarranted or wrong data) when legally possible;
- The p/f shall not make the raw data available without prior pre-processing.

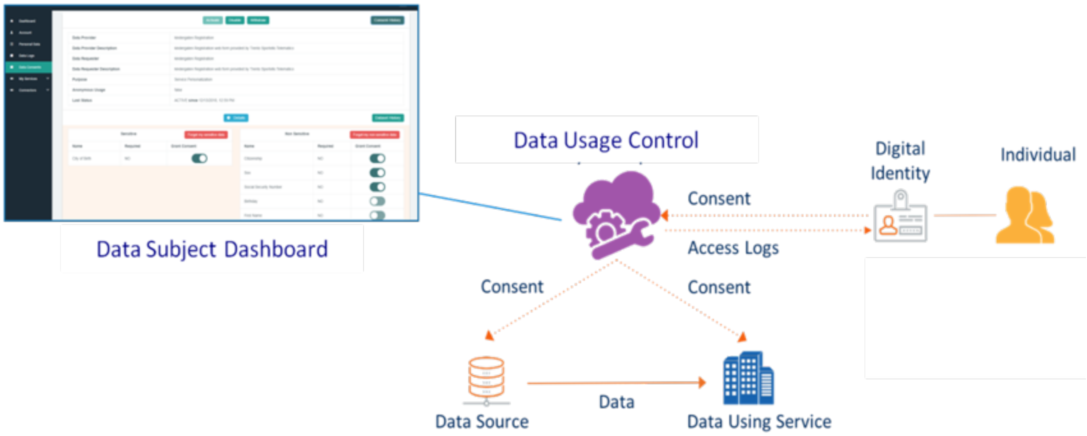


Figure 29: Smart Cities - Data usage dontrol dashboard for personal data

9.4.1.3 Operationalization of a decentralized sensor data infrastructure

Demonstration case has to support the operationalization of a sensor data infrastructure for allowing multiple stallholders to interoperate without a centralized ownership (Figure 30), while enforcing privacy and security required by GDPR:

- To provide a decentralized identity management;
- To support different stakeholders with different levels of access to the data;
- Break-the-glass built-in mechanism for accessing sensitive data while recording evince of the operation, e.g., law enforcement requesting raw video footage, without digital masks, as a crime scene evince;
- Ensuring data confidentiality to be enforced at the computational level in order to minimize data leakage;
- Ensuring secure communications between the sensors and the backend (i.e - the platform)..

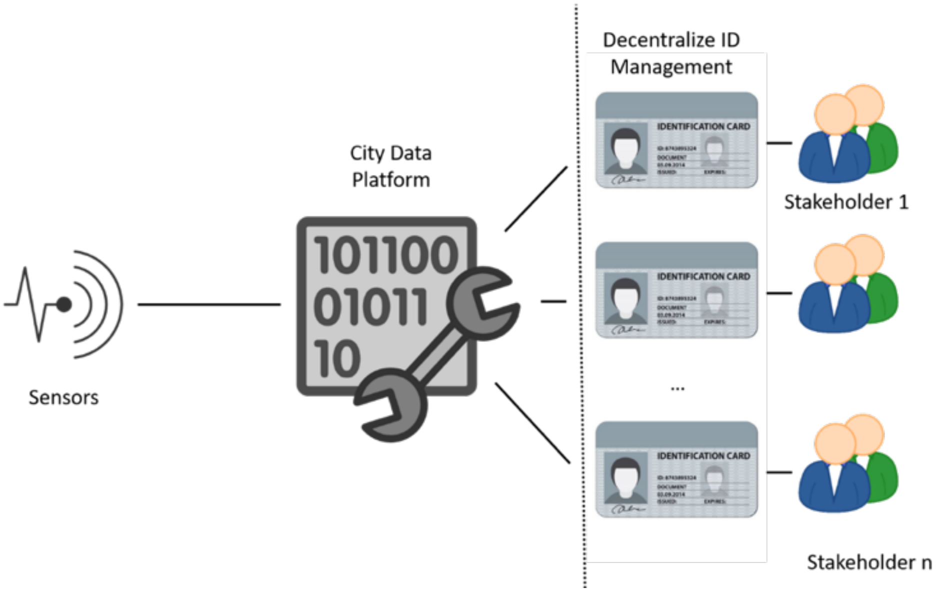


Figure 30: Smart Cities - Decentralized sensor data infrastructure

9.4.1.4 Protect Smart Cities assets from cyber risks

To protect Smart Cities from cyber risks, the suggested demonstration case provides two assessments for different aims (Figure 31):

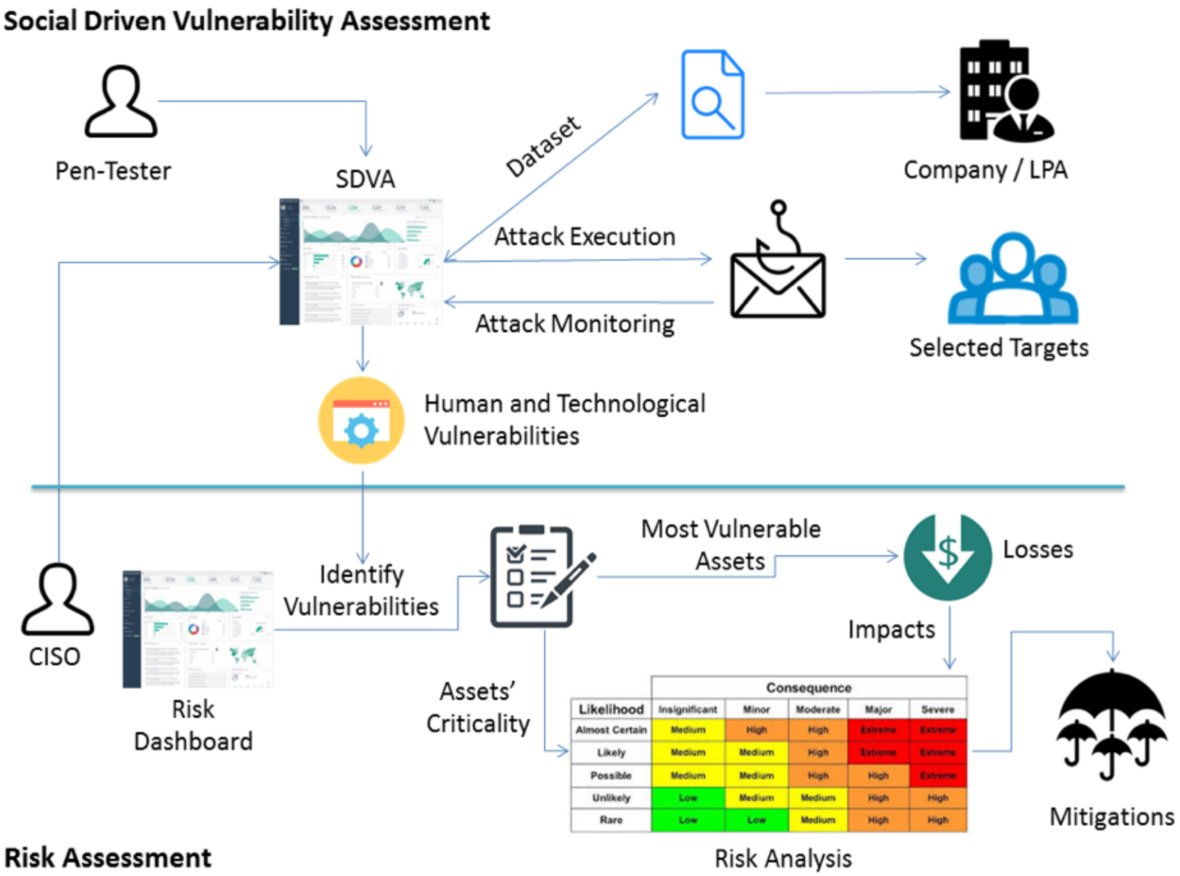
1. A *Social Driven Vulnerability Assessment(SDVA)*: the aim is to allow CISO to conduct a social engineering campaign in order to assess employees' reactions on such specific kind of attacks (Phishing for example) and report discovered vulnerabilities, both human and technology based;
2. A *Risk Assessment*: The aim is to support LPA to assess evidence-based risk profiles for smart cities in order to identify major cybersecurity risks for their services and managed assets. LPA managers will be also supported by the solution to make decisions related to cyber-security investments on hard and soft mitigations in order to minimize exploitable vulnerabilities.

Below the list of major functionalities for the *Social Driven Vulnerability Assessment* (SDVA)(1):

- To define the pen-test approach (if black box or white box);
- Gather information on LPA's digital shadow, likewise public information available on internet, their web technologies and employee contacts email addresses;
- To prepare a sample (better call hook for the attack) for the social engineering attack;
- To launch and monitor the social engineering attack of the campaign;
- To report targets 'reactiveness and, in case of successful attack, to report all the information about technological vulnerabilities discovered and their severity and impact on the organization.

Below the list of major functionalities for the *Risk Assessment* (2):

- Understanding Smart City cyber posture, in terms of major interested threat agents, their motivations and their skills used to attack the LPAs;
- Evaluate LPA cyber vulnerabilities thought a Cyber Maturity Model;
- Identify vulnerable assets and their relationships in case of attacks;
- Estimation of the consequences from a Qualitative and/or Quantitative analysis;
- Discover cyber risks and their possibility to be mitigated.



	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Medium	Medium	High	High	Extreme
Unlikely	Low	Medium	Medium	High	High
Rare	Low	Low	Medium	High	High

Figure 31: Smart Cities - Social driven vulnerability and risk assessment processes

9.4.1.5 Cyber security solution elicitation and market place

The demonstration case has to support all city stakeholders in the elicitation adoption of cyber security solutions and best practices to assure security and privacy in city services used by citizen. To this end the demonstration case has to support the following functionalities:

- To suggest or report cyber security needs and issues (e.g. to the municipalities);
- Launch challenges in order to find possible solutions to solve those needs;
- Propose, by following a collaborative approach, new ideas as possible solutions;
- Evaluate and select the best ideas in order to be refined and implemented in a collaborative way, according to a definite evaluation and selection mechanism;
- Provide more details (refinement) about the selected ideas;
- To support the publication of new solutions/services directly in a City Marketplace or identify already available solutions that match the selected ideas (e.g. OASC Catalogue).

The Figure 32 below summarizes the process.

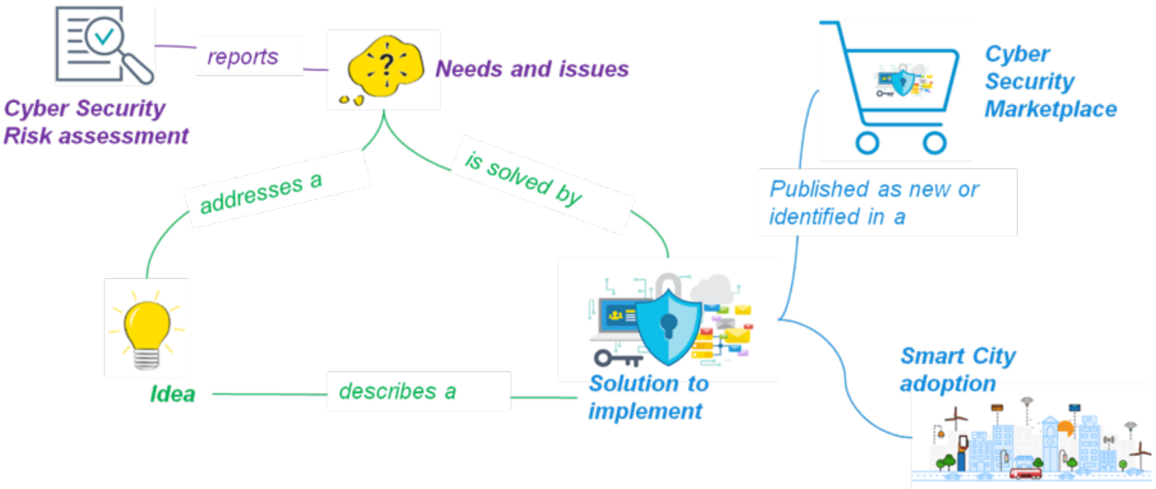


Figure 32: Smart Cities - Process of cybersecurity solution elicitation

The above main functionalities could be mapped in the following use cases.

9.4.2 Use Cases List

- **SMC-UC1 - Register Data Consumer and Manage Services**: Users, as data publishers or consumers, can register in the platform and personalize value-added services, and request approval to consume city data via GUI or APIs.
- **SMC-UC2 - Discover and Consume City Data**: Registered and authorized users can discover and consume city data via GUI or APIs in a lawful manner.
- **SMC-UC3 – Personal Data Sharing**: Personal data is accessed and used by third party companies through third party consenting process.
- **SMC-UC4 - Sensor Data Sharing and Processing**: The sensor data is produced by different stakeholders and its processing can be performed by varying entities.
- **SMC-UC5 – Social Driven Vulnerability assessment:** Assess Social Engineering exposure by simulating phishing attacks on Service Provider's targets-groups .
- **SMC-UC6 – Cyber Risk Assessment:** evaluate the Service Provider's cyber maturity level and estimate probability and impacts of cyber attacks .
- **SMC-UC7 - Cyber Security Needs and Solution Elicitation and Selection**: City stakeholder can identify cyber security threats/risks and related potential solutions/best practices, already available or to publish in a city market place.

The above use cases are mapped with the following functional requirements:

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-F01	IdM	Allow users to register to use services and consume proprietary city data and open data (optional)	SMC-UC1	Medium	No
SMC-F02	Func	Provide service providers mechanisms to define the terms and conditions of platform services data usage	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4	Medium	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-F03	Func	Allow users to format data in any supported data formats	SMC-UC2, SMC-UC3, SMC-UC4	Medium	Yes
SMC-F04	Func	The query request may require data to be sourced from different storage locations	SMC-UC2, SMC-UC3, SMC-UC4	Medium	Yes
SMC-F05	Func	Allow query requests against all metadata used to manage the repository.	SMC-UC2, SMC-UC3, SMC-UC4	Medium	No
SMC-F06	SLog	Keeps an audit trail of all actions. All data must be traceable at any given moment, by owner. It must be possible to identify in a human-readable report: (i) all data concerning an individual, and (ii) the identity of the owner of any piece of data stored within the system	SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC6	High	Yes
SMC-F07	NoS	User can track personal data processing and subscribe for process events notification	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-F08	Func	Removing or adding of new stakeholders have to conform to a majority	SMC-UC4	Medium	No
SMC-F09	SDLC	CISO must conduct a legal and ethical compliant social engineering campaign on his/her LPA	SMC-UC5	High	Yes
SMC-F10	SDLC	The risk assessment must indicate Human, IT, and Physical LPA cyber-vulnerabilities.	SMC-UC6	High	Yes
SMC-F11	SDLC	To support a co-creation approach for discovery and problems detection and idea/solution evaluation and selection process	SMC-UC7	High	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-F12	Func	To support the discovery and publication of new/already available service solutions following a "marketplace" approach.	SMC-UC7	Medium	No

Table 49: Smart Cities - Functional Requirements

9.4.3 SMC-UC1 – Register Data Consumer and Manage Services

User can register in the platform and request approval to consume city data via GUI or APIs. They provide valid registration details (to be defined) and wait for the platform to confirm their registration. Users must accept the terms and conditions for platform usage and define how their personal data can be used by the Platform Owner and value added-services. Users can manage and alter their registration information at any time.

This use case can be further divided into a number subordinate use cases listed in Table 50.

USE CASE	BASIC STIMULUS AND RESPONSES
SMC-UC1.1 - Register Consumer	1. The platform prompts the user for a username and password or register new account. 2. The user selects registration options. 3. The platform prompts user for data consumer registration information (e.g. username, password) and privacy policies 4. The user enters the information requested. 5. Platform verifies information and creates new account. • If non-valid information, platform shows error message and returns to step 1. 6. Platform acknowledges registration has been successful. 7. End of registration.
SMC-UC1.2 - User manages services	1. Platform provides user with an interface for services management. 2. User chooses to edit or delete services: • If edit, user revises service information (access-control, commercial models, parameters) and deployment; • If delete, user selects services to be removed / disabled. 4. User confirms action. 5. Platform quickly process user's request. 6. Platform confirms execution of request: • If valid request, platform acknowledges request has been processed successfully. • If non-valid request, platform returns to step 1. 7. End of services management.
SMC-UC1.3 - User tracks services usage	1. Platform provides user with an interface for services management 2. User chooses to visualise usage information of a service 3. Platform quickly process user's request for data usage information 4. Platform provides user with statistical information about services usage and data users anonymised information 5. End of data services tracking.

Table 50: Smart Cities – SMC-UC1 subordinate use cases

9.4.3.1 Use Case Diagram

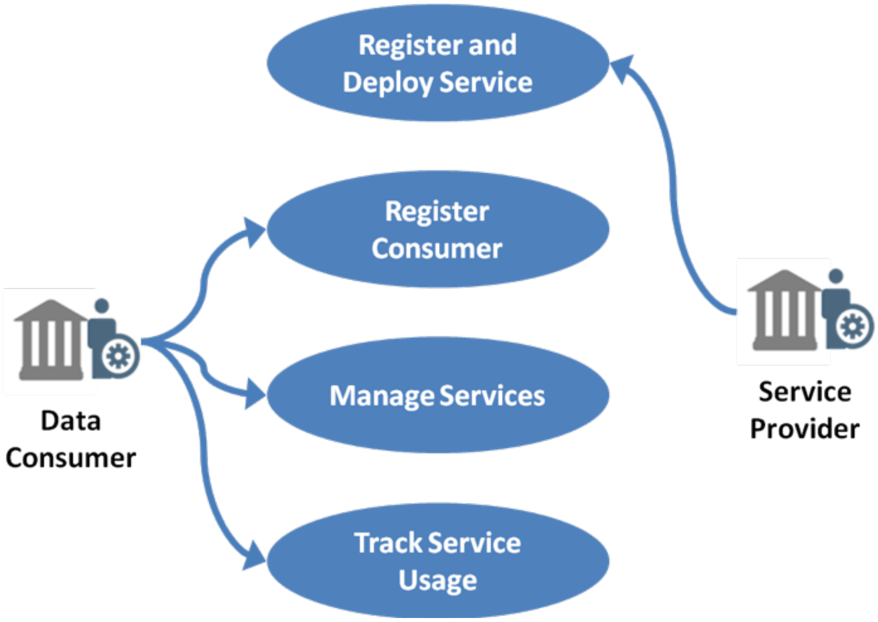


Figure 33: Smart Cities - SMC-UC1 use case diagram

9.4.4 SMC-UC2 - Discover and Consume City Data

Users are registered in the platform and have received approval to consume city data via GUI or APIs. Users have accepted the terms and conditions of platform usage and define how their personal data can be used by the Platform Owner, including their usage for data profiling tools for service enhancing and personalization. Users, at any time, can manage and alter their registration information. The use case and involved actors are summarised in Figure 34.

This use case can be further divided into a number subordinate use cases that Table 51 lists.

USE CASES	BASIC STIMULUS AND RESPONSES
SMC-UC2.1 - Discover city data via data query end-points	1. Users access specialised data query end-points (e.g. SPARQL) 2. Users provides information for pre-defined parameters for search 3. Users request data search 4. Platform quickly process users request for data • All queries are verified against access rights restrictions • If restriction applies users are redirected to log in interfaces • Users provide credentials and log on the system 5. Users are provided with query results on the end-point if access is allowed • If access is not allowed, platform issues an error message to the user.
SMC-UC2.2 - Discover city data via GUI	1. Users search city data via GUI 2. Users inputs search parameters (e.g. key words, categories, formats, publishers) 3. Users request data search 4. Platform quickly process users request for data • All queries are verified against access rights restrictions • If restriction applies users are redirected to log in interfaces

USE CASES	BASIC STIMULUS AND RESPONSES
	• Users provide credentials and log on the system 5. Users are provided with query results on an interface • If access is not allowed platform issues an error message to the user
SMC-UC2.3 - Customise City Data	1. Users request data to be formatted in a particular format supported by the platform. 2. Platform quickly process users request for data formatting. 3. Mechanism for data conversion is called and process data. 4. Users are provided with data formatted as requested.
SMC-UC2.4 - Consume City Data via GUI	1. Users / Machines select data to be downloaded. 2. Users / Machines are redirected to authentication mechanism in case of registration is needed for the particular dataset: ○ If authentication is successful, users are provided with requested data streams. 3. Users are provided with requested data via APIs.
SMC-UC2.5 - Consume City Data via APIs	1. Users / Machines makes data request on the platforms API 2. Users / Machines are redirected to authentication mechanism in case of registration is needed for the particular dataset • If authentication is successful, users are provided with requested data streams 3. Users are provided with requested data via APIs

Table 51: Smart Cities – SMC-UC2 subordinate use cases

9.4.4.1 Use Case Diagram

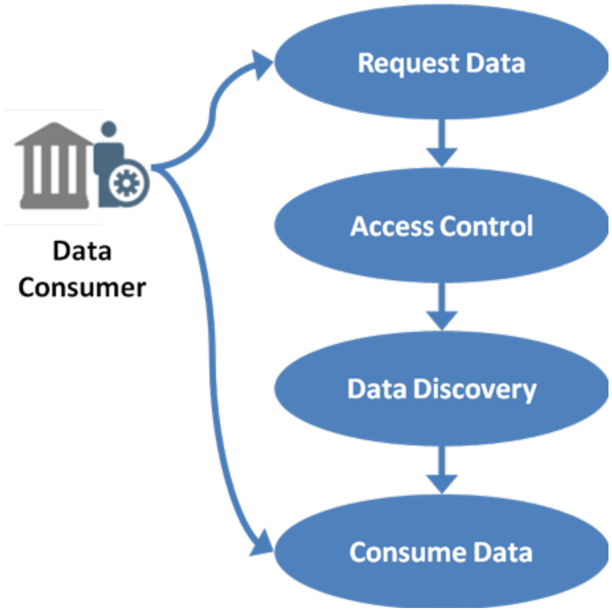


Figure 34: Smart Cities - SMC-UC2 use case diagram

9.4.5 **SMC-UC3 - Personal Data Sharing**

A municipality manages a large number of information regarding citizens and the territory.

Citizens data concern:

- Identifying data (e.g. Name, Birth date);
- Tax information;
- Specific information related to the use of social and commercial services (e.g. kindergartens, primary school, social services etc.).

Territory information are related to:

- Topography and street names;
- Road conditions;
- Facilities and infrastructure;
- Emergency systems (e.g. fire hydrants);
- Public works.

The municipality's goal is to maintain data security and governance by sharing part of its data with third party actors (companies, other public entities etc.). Data sharing processes, and in particular citizens' personal data sharing has to be supported by privacy and security enhancement tools. It is important to introduce tools for a lawful data sharing processes, with the ability to grant and withdraw consent to sharing data from a service (Data Source) to be processed in another service (third party). Consent authorizes Data Sources to provide data to Data Consumers and authorizes Data Requester to process that data. Consent has to refer to a Data Usage Policy that can be linked to consent formalization. Consent needs to be given in a clear manner so that the data controller can demostrate that a valid consent has been given. Consent record should demonstrate:

- Who consented.
- When they consented.
- What was consented.
- How data was consented.
- Wheather a consent withdrawal occurred.
- Who consented on the individual's behalf (in case of minors)..

Consent is free given by data subject and the process consists of five steps:

1. Data source and third party data consumer as Data Controler&Processor have to define and describe data processing and related policies.
2. Information about the service is presented to the data subject including what information the data consumer would like to have and for what purpose.The data subject then defines data processing rules and constraints, which must meet the third party minimum requirements for the consent to be actionable.
3. Consent Record (receipt) is stored in data subject client (dashboard or wallet).
4. Consent Record (receipt) is delivered to the involved services and any requested authorization data (e.g. token) is delivered to the services.
5. Citizens as data subject by means of a dashboard/wallet is enabled to manage and control "personal data" during the interactions in the data sharing process. By means of that dashboar, the data subject has a single point to verify which data are used, by whom, how and for which purpose. Furthermore the data subject receives notifications about data processing and can perform objections or consent withdrawal as well as make use of its right to be forgotten and data portability rights.

Figure 35 summarises how each involved actor interacts with the use case.

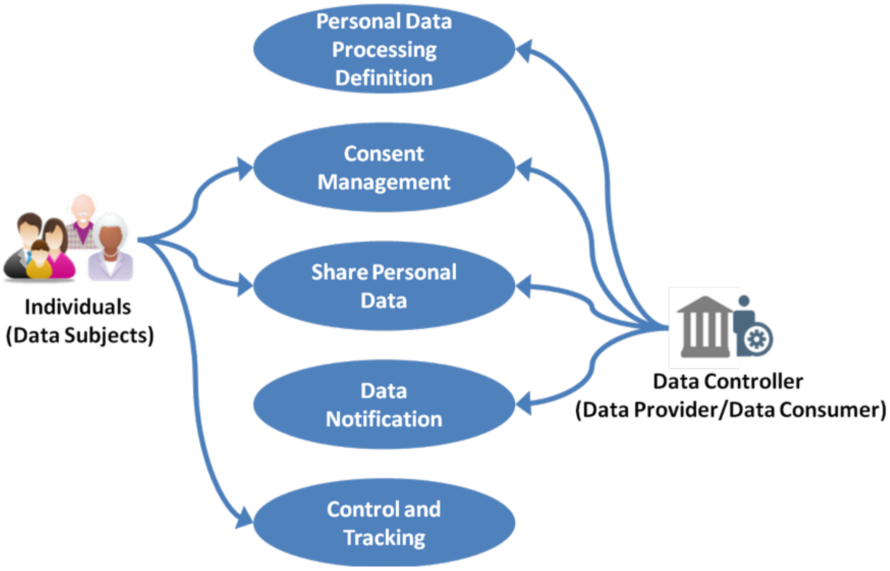

Personal Data Processing Definition
Consent Management
Share Personal Data
Data Notification
Control and Tracking
Individuals (Data Subjects)
Data Controller (Data Provider/Data Consumer)

Figure 35: Smart Cities - SMC-UC3 use case diagram

9.4.6 SMC-UC4 - Sensor Data sharing and operationalization

Cities must leverage the multiple sources of information regarding sensor data, i.e. Internet of Things (IoT) data. In this regards, different stakeholders can produce data, so the ownership of data is spread across these actors. Data Providers may also transform, process and enrich sensor data with additional data sources. The data processing must be compliant to the GDPR, hence the following functionalities must be taken into account (see Figure 36):

- Decentralized identity management
- Data tagging
- Audit trail for at all stages of the operation
- Break-the-glass mechanisms to ensure proper response in emergency scenarios
- Confidentiality while processing data
- Privacy preserving techniques for sensitive data

The municipality’s goal is to maintain data security and governance while allowing multiple stakeholders, such as private (companies) and public (law enforcement, etc) entities, to participate.
Specifically, GDPR complaint privacy policies and regulations need to be defined and enforced by Data Producers stakeholders when acquiring, storing, processing and providing data.

9.4.6.1 Use Case Diagram

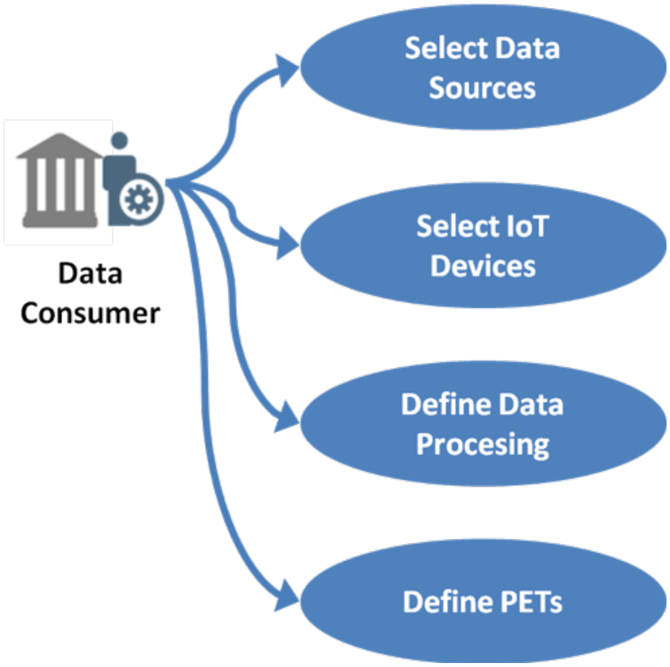


Figure 36: Smart Cities - SMC-UC4 use case diagram

9.4.7 SMC-UC5 - Assess Social Engineering exposure by simulating phishing attacks on Service Provider's targets-groups

Following privacy by design and security by design concepts, this use case has as main goal to describe the process that need to be implemented in order to allow CISO (or managers in case of LPA) to conduct an entire Social Driven Vulnerability Assessment on their employees in order to understand how vulnerable the organization is to social engineering attacks and assess the impact of such an attack on the organisation. In detail, individuals using such a solution will be able to understand what public information about their organization is available and accessible on the web and using this information, they can delegate pen-testers to simulate a real phishing attack and discover both human and technological vulnerabilities. Figure 37 summarises how each involved actor interacts with the use case.

This use case can be further divided into a number subordinate use cases that Table 52 lists.

USE CASE	BASIC STIMULUS AND RESPONSES
SMC-UC5.1 - SDVA set-up	1. CISO creates a new social driven vulnerabilities assessment (SDVA) 2. Machine provides to CISO a SDVA key access • Only CISO can access to sensible information 3. CISO configures the SDVA instance • Pen-tester information • SMTP server configuration • Upload list of targets 4. Automated anonymization of information
SMC-UC5.2 - Information gathering	1. Pen-tester receives access to SDVA instance 2. Pen-tester collects information about targets based on CISO' requirements • Web researches (eg. Wikileaks, pastebin, whois etc..) 3. Pen-tester tags collected information as sensitive or appropriate to use in order to not violate any defined policies by the CISO

USE CASE	BASIC STIMULUS AND RESPONSES
	4. Pen-tester/Machine creates datasets that may be used to create the hook of the attack
SMC-UC5.3 - Hook Preparation	1. Pen-tester creates the email to be used as hook • Subject and Sender • Content • Evocative images 2. Pen-tester creates fake websites as landing page • Adding scripts to collect and track targets activities
SMC-UC5.4 - Launch of the attack	1. Pen-tester selects the available hooks 2. Pen-tester configures the scope of the attack: • Collect credentials • Website visiting 3. Pen-tester sets the time schedule of the attack 4. Once the attack is launched, automated collection of all information about targets activities: • Number of email sent • Number of visits in the websites • Numbers of collected credentials • Technical information collected from targets' system 5. Pen-tester/Machine stop the attack
SMC-UC5.5 - SDVA Reports	1. Machine aggregates information about the attack 2. CISO access to statistical results • Overall activities • Clicks vs provided credentials • General statistics based on targets sample (eg.departments age range, etc..) 3. Based on collected technical information on targets' system, the machine provides information about all the common vulnerabilities discovered. 4. CISO accesses to final report and see severity scores 5. CISO is also able to download the entire report about the attack

Table 52: Smart Cities – SMC-UC5 subordinate use cases

9.4.7.1 Use Case Diagram

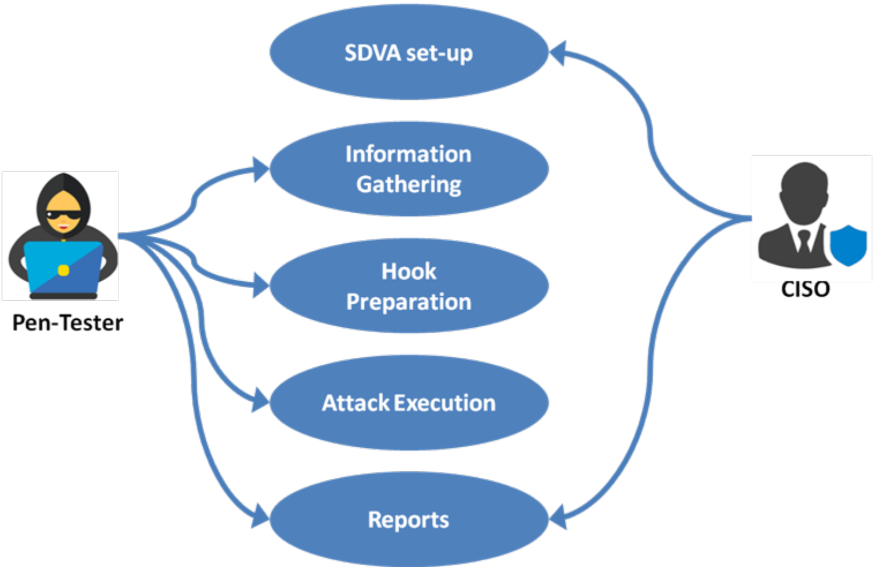


Figure 37: Smart Cities - SMC-UC5 use case diagram

9.4.8 SMC-UC6 - Cyber Risk Assessment, evaluate the Service Provider's cyber maturity level and estimate probability and impacts of cyber attacks

CISO must perform a risk assessment based on company's vulnerabilities and, once the most vulnerable assets are identified, is able to estimate from both qualitative and quantitative impact analysis the related consequences in case of cyber attacks. The general approach then is to support users to distinguish tolerable risk from non-tolerable ones and make decisions on the most effective best cyber-security mitigations strategy to implement. Figure 38 summarises how each involved actor interacts with the use case.

This use case can be further divided into a set of sub use cases that Table 53 lists.

USE CASE	BASIC STIMULUS AND RESPONSES
SMC-UC6.1 - Identify LPA Cyber-Posture	1. LPA manager accesses to the main menu of the solution 2. LPA manager selects the "asses vulnerabilities" stage and perform the self-assessment • Identification of Threat Agents and their motivations • Identification of Cyber-Vulnerabilities • Human related • IT related • Physical related 3. Machine provides overall scores about likelihood to be attacked and vulnerabilities found.
SMC-UC6.2 - Create Risk Assessment	1. LPA manager access to the stage "Risk Assessment" 2. LPA manager clicks on "create" 3. Machine creates the risk-model
SMC-UC6.3 - Asset Clustering	1. LPA accesses to the stage "asset clustering" 2. Machine provides the asset taxonomy (both tangible and intangible categories) 3. LPA manager select which are the assets that wants to involve in the risk assessment
SMC-UC6.4 - Identify consequences	1. LPA manager accesses to the stage "Consequences" 2. LPA manager selects the evaluation to be performed • Qualitative approach

USE CASE	BASIC STIMULUS AND RESPONSES
	• Quantitative approach If Qualitative: 3. Machine provides list of vulnerable assets 4. LPA manager select for each asset the rating impact scale. If Quantitative: 3. LPA manager provides economic value for the quantification of the losses on assets. 4. Machine calculate impacts on assets
SMC-UC6.5 - Evaluate Risks	1. LPA manager access to the risk management stage 2. Machine provide a graphical representation of the assets in a risk matrix defining criticality of the assets and estimated impacts 3. LPA manager prioritizes risk by setting risk criteria (tolerable vs no tolerable) 4. Machine updates the risk matrix 5. Machine provides list of possible controls actions to mitigate the risk

Table 53: Smart Cities - SMC-UC6 subordinate use cases

9.4.8.1 Use Case Diagram

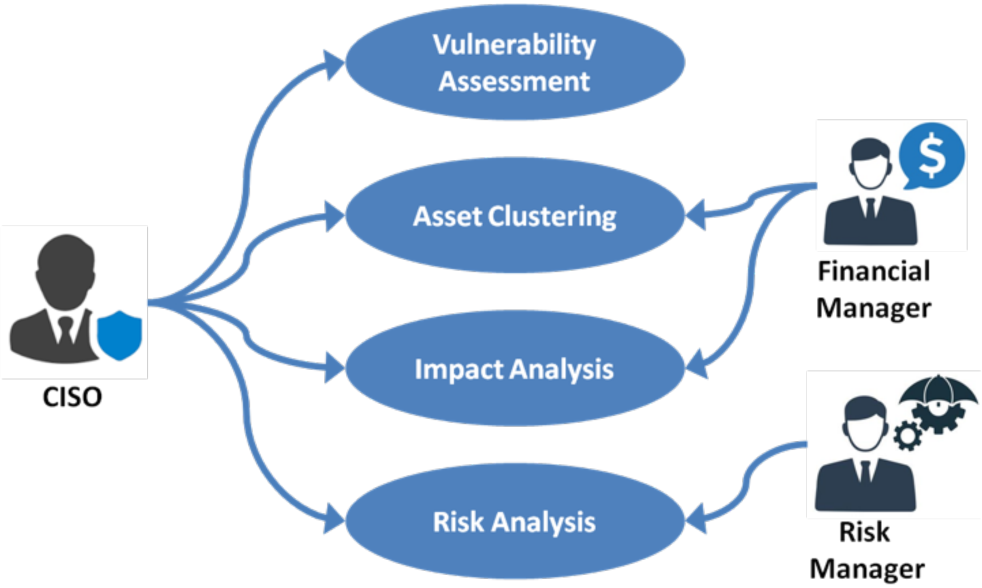


Figure 38: Smart Cities - SMC-UC6 use case diagram

9.4.9 SMC-UC7 - Cyber security needs and solution elicitation and selection

Following a security and privacy assessment, city stakeholders as authenticated user have access to functionalities to create a need, an idea or a challenge by providing the required information. Each stakeholder is involved in the process and is invited to cooperate with each other to identify problems and needs to be able to solve them. The co-operation environment supports participanting stakeholders in the management of cyber security needs and solutions elicitation lifecycle and related solutions selection and adoption. The main phases are:

- Discovery and Problem Detection;
- Idea generation;
- Idea Selection;
- Idea Refinement;

- Solution selection.

In the *Discovery and Problems detection phase*, the stakeholders involved (in particular municipality) share information in order to have a mutual understanding about needs, problems and services. Mutual knowledge is created. In the *Idea generation phase* the stakeholders co-define the implicit knowledge created in the previous phase and convert it to explicit and shared knowledge. The collaboration between the users is promoted in this phase, in order to co-create innovative ideas to solve the problems discovered in the previous stage. Inthe subsequent *Idea selection phase* the municipality, together with an expert team (appropriately appointed) evaluates all the proposed ideas based on a set of barrier and quantitative criteria and select a subset of ideas. The selected subset of ideas will pass to the next phase, the *Refinement phase.* After the refinement the stakeholders starts a process of development and collaborative design. The author and the collaborators of an idea cooperate with each other to implement the refined idea. To do this, the involved actors are also supported by a marketplace of cyber security services and best practices to be used for the solution implementation. The implemented solution can in turn be published in the marketplace for later discovery and adoption by other cities (see Figure 39).

9.4.9.1 Use Case Diagram

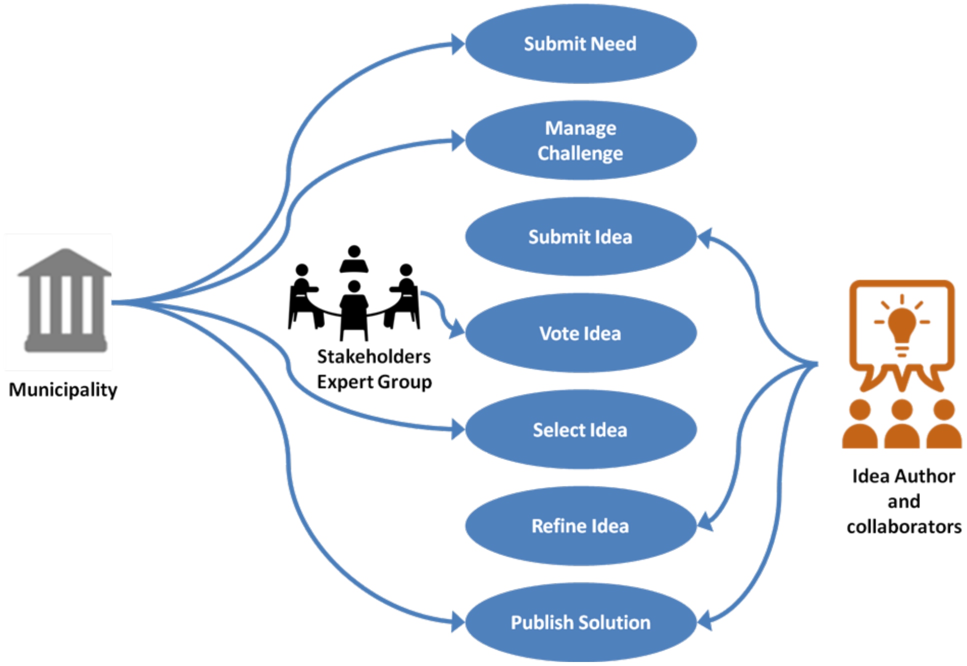


Figure 39: Smart Cities - SMC-UC7 use case diagram

9.5 Security and Privacy Requirements

This section resumes, for completeness, all the security and privacy requirements (functional and non functional). Solutions applied to demonstration case, described in the above use cases, should conform to security-by-design principles, privacy-by-design principles and EU Legal compliance.

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-SP01	AuthnE	Solution ensures that authentication is implemented	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP02	AC	Keep sensitive information secured and accessible only to authorized users	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP03	Acc	Solution ensures that accounting is implemented	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP04	Config	Solution ensures the required protection across multiple communication protocols. Security has to be at the same level for all types of connection and regardless of whether the app is connected to the device over the Internet or locally;	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP05	SDLC	Solution can be integrated with existing authentication mechanisms;	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	NO
SMC-SP06	Acc	Solution provides data provenance, so that it allows for auditing of data access and update on secured data;	SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC6	High	Yes
SMC-SP07	SDLC	Solution is easy to protect and isolate parts from vulnerabilities;	SMC-UC1, SMC-UC2, SMC-UC3,	Medium	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
			SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7		
SMC-SP08	Acc	Solution allows for monitoring access and changes;	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-SP09	Acc	Solution manages log records from its own components and from the underlying devices and systems in order to be able to track any breaches and to identify patterns and prevent problems that can pinpoint problems before they happened;	SMC-UC5, SMC-UC6	High	Yes
SMC-SP10	CE	Solution should support end-to-end encryption (protocol and message), automatic standard-based encryption from device to the application and encrypting data in transit between platform elements;	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP11	IdM	Solution should have a secure store for keys and be able to integrate with key stores.	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP12	SDLC	Solution must implement privacy rules as stated by the European Union, in particular the new GDPR, national law, ECHR[8] (Article 8), EU Charter[9] (Article 7 and 8), Public law, criminal law and civil law of the countries where use cases will be implemented (fundamental rights, communication secrecy, privacy laws;	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes

[8] European Convention on Human Rights - https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Convention_ENG.pdf

[9] EU Charter of Fundamental Rights - http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-SP13	GDPR	Solution has to be transparent about the "who, what, where, when, and why" for any data or information being collected and should allow people to keep personal data private or share for specific purposes, safeguarding data ownership and control;	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP14	GDPR	Any personal data "processed" in use case should require signed consent by the relevant parties covering its intended use;	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP15	GDPR	When a new request with the data arises, the platform has to be able to request a refit for purpose to the party;	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP16	AuthnM	Personal data has to be stored in a protected way (e.g. encryption, hashing);	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes
SMC-SP17	GDPR	Any systems used for the storage and processing of personal data within the project must demonstrate a good level of security readiness, which can be done by (a) inclusion of the system within the scope of an ISO 27001 certified Information Security Management System or (b) independent verification by a third-party audit.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP18	GDPR	Unused or unnecessary data that is collected must be deleted as early as possible	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP19	GDPR	Whenever functions within the platform could be performed without the use of personal data or with the use of anonymized data, this should be preferred;	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SP20	GDPR	Whenever personal information is visible to	SMC-UC1, SMC-UC2, SMC-UC3,	Medium	Yes

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
		others, this should clearly be indicated to users;	SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7		
SMC-SP21	Func	No automated decision should be done when processing personal data.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-SP22	GDPR	Demonstration case solutions should prevent the possibility of creating central surveillance on users or groups of users.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-SP23	SDLC	The establishment of technological practices for security and privacy should based on open architectures and standards	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-SP24	GDPR	User can manage personal data consents (opt-in, opt-out, withdrawal) for third party re-use	SMC-UC2, SMC-UC3, SMC-UC4	High	Yes

Table 54: Smart Cities - Security and privacy requirements

9.6 Non-Functional Requirements

The following non-functional requirements are detected to be applied to this demonstrator

9.6.1 Look and Feel Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-LF01	UI	The demonstration case must include a GUI that will allow the interaction with the end uses in data sharing processes or in cyber security risk assessment and solution elicitation.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-LF02	Func	The GUI interfaces must support at least two languages and provide an easy way to incorporate new ones.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes

Table 55: Smart Cities - Look and feel requirements

9.6.2 Usability Requirements

Solutions must be designed to be used by Non IT people with lack of information technology knowledge.

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-U01	Usab	Solutions should be designed to be used by individuals with lack of information technology knowledge.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	No

Table 56: Smart Cities - Usability requirements

9.6.3 Operational Requirements

ID	CATEGORY	DESCRIPTION	USE-CASES	PRIORITY	MANDATORY
SMC-OP01	Perfo	Solutions should be able to scale in term of data capacity, user capacity and components and services to be integrated.	SMC-UC2, SMC-UC3, SMC-UC4	Medium	Yes
SMC-OP02	Func	Solutions need to run on a distributed architecture and the components should be decoupled	SMC-UC2, SMC-UC3, SMC-UC4	Medium	Yes
SMC-OP03	Config	The architecture must be "pluggable" and components in the platform must be easily replaceable with minimum impact.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-OP04	SDLC	Solutions should not require service interruption to perform a risk assessment	SMC-UC5, SMC-UC6	Medium	Yes
SMC-OP05	SDLC	Solutions should be compatible to existing hard- and software architecture of the Smart Cities	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes

Table 57: Smart Cities - Operational requirements

9.6.4 Maintainability and Portability Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-MP01	GDPR	Open infrastructures to allow for seamless change of service providers without proprietary data lock-ins	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-MP02	GDPR	To grant the data owner easier ability to exercise their right to data portability	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes

SMC-MP03	SDLC	Data available in a machine readable open formats and accessible by means of secure and standardized APIs,	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	Medium	Yes
SMC-MP04	Func	Open up for reuse of data in different services and follow "once only" principle in public services.	SMC-UC2, SMC-UC3	Medium	Yes

Table 58: Smart Cities: Maintainability and portability requirements

9.6.5 Social and Political Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-SPL01	Fair	Solution cannot be used for political purposes.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-SPL02	SDLC	Solution should not affect the life of citizens and the ways in which the services of the municipality are used by the latter.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes

Table 59: Smart Cities - Social and political requirements

9.6.6 Legal and Regulatory Requirements

ID	CATEGORY	DESCRIPTION	USE CASES	PRIORITY	MANDATORY
SMC-LR01	SDLC	Compliance with the Agenzia per l'Italia Digitale - Agency for Digital Italy [AGiD] guidelines and the CAD (Codice per l'Amministrazione Digitale) regulation.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes
SMC-LR02	GDPR	Compliance with the GDPR and other linked regulations.	SMC-UC1, SMC-UC2, SMC-UC3, SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7	High	Yes

Table 60: Smart Cities - Legal and regulatory requirements

9.7 Mandated Constraints

No mandated contraints have been identified at this point.

9.8 Relevant Facts and Assumption

9.8.1 Facts

No relevant facts affecting the system have been identified at this point.

9.8.2 Assumptions

No assumptions about the system have been identified at this point.

9.9 Related WP3 and WP4 Tasks

Smart Cities demonstrator (Task 5.7) has a close link and dependencies with following WP3 and WP4 tasks:

- **Task 3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies** (partners involved: C3P, CNR, UMU). This task defines the technology for privacy and security enablers to deploy in the IoT edge. Among these enablers, several applications on the smartcities demonstrator, specifically are (a) identity management and authentication solutions over multiple non-federated providers, (b) security and privacy services to deploy a basic Edge Computing platform(c) Security & Privacy by Design approaches, decentralized evidence-based authorization and distributed access control using blockchain,(d) IoT Privacy-Preserving Middleware Platform. The smartcities demonstrators involves the use of technologies of all these levels. Particularly, those task involving the IoT environment and privacy and secure data storage, since the demonstrator includes IoT architectures, authentication and communication of private information**.**

- **Task 3.3 SDL – Software Development Lifecycle** (partners involved: C3P, CYBER, DTU, KAU). This task identifies research challenges, requirements and approaches in all stages of the lifecycle of software centred in secure-by-design and proactive methodologies. The enables for this task with put special focus in new components from T3.2. smartcities demonstrator integrates some of the enablers developed in T3.2 and thus requires the enablers from 3.3. Especially those that involves evaluation and audit of privacy methods and services..
- **Task 3.4 Security Intelligence** (partners involved: ATOS, C3P, CNR, KUL, UMU). This task the state of the art for reliability, safety and privacy guarantees of security intelligence techniques based on artificial intelligence, machine learning and data analytics. In the smartcities demonstrator, security intelligence is a transversal area, thus the demonstrator leverage of the enabler proposed in T3.4 due offers the mechanism to protect the use case while detecting, preventing, and mitigating the effects of security threats..
- **Task 3.6 Usable Security (Human-centred Cybersecurity)** (partners involved: UCD, KUL, VTT,). This task formulates and develops recommendations and guidelines on how to provide usable requirements in security designs. Besides, it specifies a framework to test these requirements, centred in biometric-based and multimodal user authentication mechanism. Among the enablers identified several applications on the smartcities demonstrator, especially, (a) to provide users with awareness mechanisms to support visualisation of the system status and security risks (b) to enable effective and usable security controls (c) to help users with automation and AI on their security and privacy decisions.
- **Task 4.1 Vertical stakeholders engagement and consultation** (partners involved: FORTH, KAU, UMA, UPS-IRIT). This task gathers the prerequisites of all interested parties of the Smart City demonstrator. This process will allow us to start analyzing the requirements of WP5 from a global point of view, ensuring that we do not neglect any interest in this field. We already took this way with the outcome of their first deliverable D4.1 “Requirements Analysis from Vertical Stake-holders”.
- **Task 4.2 Legal and regulatory requirements** (partners involved: FORTH, POLITO, UM). This task provides legal and regulatory requirements, these need to be taken into account in T5.7. Especially the identification of the unique European Legal and Regulatory Requirements (such as the GDPR, the NIS directive and the ePrivacy Regulation, PSD2 and eIDAS) will be deeply analysed to collect any useful advises for our demonstrator.
- **Task 4.6 Roadmap for industrial challenge 5.3 (Privacy-preserving Identity Management)** (partners involved: UMU, AIT, UCY, UM, UPRC, VTT). This task presents the roadmap while identifying the requirements needed and the defying the main research challenges focused in Privacy Preserving Identity Management. The smartcities demonstrator involves a great number of diverse identities and services that need con coexists in a secure and private environment. Thus among all the challenges identified in Task4.6, this demonstrator consider some challenges to be present within it as, (a) unlinkability and minimal disclosure (b) privacy preservation in the blockchain. This tools and techniques provides a secure and private ecosystem while using cryptographic tools focused on attributes and partial, anonymous credential systems, and blockchain. The synergies of Task4.6 and the smartcities demonstrator will impact the solution on data sharing and data management in the urban platform.
- **Task 4.10 Roadmap for industrial challenge 5.7 Smart cities** (partners involved: ENG, UMU, C3P, CNR, ENG, GEN, OASC, POLITO). This task provides the roadmap for the smart cities demonstrator and, of course, it is strongly related to the T5.7. Indeed, in this task, the challenges, methodologies and tools will be analysed and starting from them, the demonstrator plan will be created. Any future releases of T4.10 deliverables will be the guide for T5.7 activities.

WORK PACKAGE	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
WP3		✓	✓	✓		✓				
WP4	✓	✓				✓				✓

Table 61: Smart Cities - Relationship with WP3 and WP4 tasks

10 Conclusions

This document presenteds deliverable “D5.1 – Requirements Analysis of Demonstration Cases Phase 1”.

For all demonstration case it identified relevant stakeholders and actors that have direct and specific interests into, or interact with, their ecosystem.

Furthermore, it described a a set of use cases and their requirements. Non-functional requirements have been organized in specific categories, namely Look and Feel, Usability, Operational, Maintainability and Portability, Social and Political, and Legal and Regulatory. This systematic categorization allows for the definition of relevant requirements, thus providing a clear view of what cybersecurity challenges CyberSec4Europe needs, and aims, to overcome. Security and privacy requirements are treated separately from the above categories to highlight the importance of addressing the cybersecurity issues pinned down in the selected sectors.

Finally, the document shows the relationship of each demonstration case with the tasks of WP3 – “Blueprint Design and Common Research” and WP4 – “Research and Development Roadmap”, in order to facilitate, promote, and strengthen the collaboration between the three core work packages.

11 Bibliography

[Lop17]	J. Lopez, C. Alcaraz, J. Rodriguez, R. Roman, and J. E. Rubio, "Protecting Industry 4.0 against Advanced Persistent Threats", European CIIP Newsletter, vol. 11, issue 26, no. 1, European CIIP Newsletter, pp. 27-29, 2017.
[Che17]	Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., and Yin, B, Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges. IEEE Access, 6, 6505–6519, 2017. https://doi.org/10.1109/ACCESS.2017.2783682
[Lu17]	Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1–10, 2017. https://doi.org/10.1016/j.jii.2017.04.005
[Alc19]	C. Alcaraz, "Secure Interconnection of IT-OT Networks in Industry 4.0", Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies, no. Advanced Sciences and Technologies for Security Applications book series (ASTSA), Springer International Publishing, pp. 201-217, 2019.
[Tup18]	Tuptuk, N., & Hailes, S. Security of smart manufacturing systems. Journal of Manufacturing Systems, 47(November 2017), 93–106, 2018. https://doi.org/10.1016/j.jmsy.2018.04.007
[NIS17]	NIST, Cybersecurity Framework Manufacturing Profile, NISTIR 8183, September 2017.
[NIS-C]	NIST and CISCO, Best Practices in Cyber Supply Chain Risk Management, Cisco® Managing Supply Chain Risks End-to-En, U.S. Resilience Project.
[NIS18]	NIST, NIST Cybersecurity Framework, NIST release Version 1.1, 2018.
[EU16]	European Union, Machinery Directive 2006/42/EC, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF, 17th May 2016, last access in 2019.