



Cyber Security for Europe

D5.3 – Validation of Demonstration Case Phase 1

Document Identification	
Due date	31 January 2021
Submission date	29 January 2021
Revision	1.1 (30 April 2021)

Related WP	WP5	Dissemination Level	PU
Lead Participant	NEC	Lead Authors	Alessandro Sforzin (NEC), Rahul Bobba (NEC)
Contributing Beneficiaries	ABI, AIT, ATOS, BBVA, C3P, CAIXA, CYBER, DAWEX, DTU, DUT, ENG, i-BP, ISGS, NEC, POSTE, SIE, SINTEF, TDL, UCY, UMA, UMU, UPRC	Related Deliverables	D5.1, D5.2

Abstract: This document presents deliverable “D5.3 – Validation Demonstration case Phase 1”. This deliverable describes in detail the validation strategy for each use case based on either technical test cases or a technology based analysis. The test cases cover the description, workflow and achieved results. The technology based analysis cover the validation of the requirements and functionalities from the technology and implementation architecture. The use cases were introduced in deliverable *D5.1 Requirements Analysis of Demonstration case Phase 1* [1]. In deliverable *D5.2 Specification and set-up Demonstration case Phase 1* an overview of the demonstrators’ set-up was provided along with a specification containing a rigorous analysis of its components. As part of the validation strategy, the validation summary and lessons learned for future work are also covered. The information is complemented with diagrams giving a formal, graphic presentation of all use cases core functionalities.

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. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.



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 is a research-based consortium with 44 participants covering 21 EU Member States and Associated Countries. CyberSec4Europe's main objective is to pilot the consolidation and future projection of the cybersecurity capabilities required to secure and maintain European democracy and the integrity of the Digital Single Market. The project focuses on seven selected sectors: open banking, supply chain, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange, and smart cities.

The seven demonstration cases – one for each of the seven selected sectors – are CyberSec4Europe's answer to the aforementioned challenges. They are the embodiment of the project's will to lead Europe's cybersecurity research and innovation 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. A demonstrator is a prototype of a cybersecurity solution, product, or service secure by design. In addition to being developed with an eye on security and privacy, the demonstrators will also be compliant with important EU regulations, such as PSD2 and GDPR.

Work Package 5 (WP5) oversees the demonstrators' design and development. The use cases identified for CyberSec4Europe provide the common research, development and innovation concepts to be developed by design and research activity (WP3), ensuring their integration in to the demonstration cases in each of the project phases. Since the inception of the project 18 months ago, two deliverables - D5.1 and D5.2 have been released. D5.1 focused on identifying their requirements and describing their importance in the context of the selected sectors, D5.2 focuses on formalising the use cases' workflows and their interactions defining the shape of the demonstrators.

This document presents deliverable D5.3 with the formal title *Validation Demonstration case Phase 1*. For each demonstrator use case a validation strategy is outlined along the expected objectives and goals. To start with the use case is described along with the aspects of the use case that will be validated. This is followed by a detailed description of the test case, the workflow and the results. As part of the validation approach, the quality indicators and requirements coverage is also described. The quality indicators cover the effectiveness and efficacy of the solution. A technology based analysis is presented which includes the validation of requirements and functionalities that can be inferred from the implementation architecture. For each use case a validation summary then follows including the validation outcome of the test cases. Each use case ends with a description of the lessons learned and outlines future work.

WP5 identifies the requirements and provides the blueprints of the demonstrator cases. They also help WP3 and WP4 define their research roadmaps. WP5 ultimately leverages the assets in WP3 to design the demonstrators' functionalities. The use cases identified for CyberSec4Europe provide the common research, development and innovation concepts to be developed by design and research activity (WP3), ensuring their integration in to the demonstration cases in each of the project phases.

Document information

Contributors

Name	Partner
Gabriele Gamberi	ABI
Marco Crabu	ABI
Roberto Tordi	ABI
Mario Trinchera	ABI
Stephan Krenn	AIT
Valerio Cini	AIT
Susana González Zarzosa	ATOS
Juan Carlos Perez Baun	ATOS
Miryam Villegas Jimenez	ATOS
Vanesa Gil Laredo	BBVA
João Resende	C3P
Rolando Martins	C3P
Ramon Martín de Pozuelo	CAIXA
Liina Kamm	CYBER
Jérémy Decis	DAWEX
Stéphane Vaquer	DAWEX
Alberto Lluch	DTU
Marco Angelini	ENG
Vincenzo Napolitano	ENG
Vincenzo Savarino	ENG
Erwan Dano	i-BP
Médéric Collas	i-BP
Laura Colombini	ISGS
Alessandro Sforzin	NEC
Rahul Bobba	NEC
Massimiliano Aschi	POSTE
Prabhakaran Kasinathan	SIE
Ricarda Weber	SIE

Martin Wimmer	SIE
Karin Bernsmed	SINTEF
Per Håkon Meland	SINTEF
David Goodman	TDL
Jolien Ubacht	TUD
Elias Athanasopoulos	UCY
Cristina Alcaraz	UMA
Rodrigo Roman	UMA
Antonio Skarmeta	UMU
Christos Grigoriadis	UPRC
Panayiotis Kotzanikolaou	UPRC
Spyros Papastergiou	UPRC
Eleni Maria Kalogeraki	UPRC
Christos Douligeris	UPRC

Reviewers

Name	Partner
Ahad Niknia	GUF
Jozef Vyskoc	VAF

History

Version	Date	Authors	Comment
0.1	2020-07-15	NEC	Added Table of Contents
0.2	2020-12-15	NEC	Added Abstract, Executive Summary and Introduction
0.3	2020-12-22	NEC	Added List of Figures, Tables and Conclusions
0.4	2021-01-15	NEC	Addressed reviewer feedback and included the updates from all the partners
0.5	2021-01-18	NEC	Included T5.1 Open Banking input
0.6	2021-01-19	NEC	Included additional updates from partners
0.7	2021-01-20	NEC	Included List of Acronyms and List of Contributors
0.8	2021-01-25	NEC	Included final updates on demonstrator cases
0.81	2021-01-28	NEC	Corrected the date format in History
1.0	2021-01-28	GUF	Final check, improvements and preparation for submission
1.1	2021-03-08	NEC	Added content in T5.7 section.

Table of Contents

1	Introduction.....	1
1.1	Structure of the Document.....	1
2	Open Banking.....	2
2.1	Use Case OB-UC2 – OBSIDIAN	2
2.1.1	Actors	2
2.1.2	Test Case.....	3
2.1.3	Technology Based Analysis.....	7
2.1.4	Quality Indicators.....	14
2.1.5	Requirements Coverage	17
2.2	Use Case OB-UC4 Open Banking API Architecture Platform (OBACHT)	18
2.2.1	Open Banking Architecture.....	19
3.2.1	Actors	21
2.2.2	Test Case: Account Access APIs	21
2.2.3	Technology Based Analysis.....	24
2.2.4	Requirements Coverage	28
2.3	Validation Summary.....	28
2.4	Lessons Learned and Future Work.....	29
2.4.1	OB-UC2 OBSIDIAN	29
2.4.2	OB-UC4 OBACHT.....	32
3	Supply Chain Security Assurance	33
3.1	Use Case SCH-UC1 Supply Chain for Retail	34
3.1.1	Actors	34
3.1.2	Test Cases.....	34
3.1.3	Technology Based Analysis.....	34
3.1.4	Quality Indicators.....	40
3.1.5	Requirements Coverage	40
3.2	Use Case SCH-UC2 Compliance and Accountability in distributed Manufacturing.....	42
3.2.1	Actors	45
3.2.2	Test Cases.....	45
3.2.3	Technology Based Analysis.....	49
3.2.4	Quality Indicators.....	51
3.2.5	Requirements Coverage	51
3.3	Validation Summary.....	55

3.4	Lessons Learned and Future Work.....	56
4	Privacy-Preserving Identity Management.....	58
4.1	Use Case IDM-UC1 – Registration.....	59
4.1.1	Actors	59
4.1.2	Test Cases.....	59
4.1.3	Technology based Analysis.....	60
4.1.4	Quality Indicators.....	60
4.1.5	Requirements Coverage	60
4.2	Use Case IDM-UC2 – Issuance	62
4.2.1	Actors	62
4.2.2	Test Cases.....	62
4.2.3	Technology Based Analysis.....	62
4.2.4	Quality Indicators.....	64
4.2.5	Requirements Coverage	64
4.3	Use Case IDM-UC3 – Presentation	66
4.3.1	Actors	67
4.3.2	Test Case.....	67
4.3.3	Technology Based Analysis.....	68
4.3.4	Quality Indicators.....	69
4.3.5	Requirements Coverage	74
4.4	Validation Summary.....	77
4.5	Lessons Learned and Future Work.....	77
5	Incident Reporting in the Financial Sector.....	78
5.1	Use Case IR-UC1: Data Collection, Enrichment and Classification.....	78
5.1.1	Actors	78
5.1.2	Test Case 1-UC1: Incident Data Collection.....	78
5.1.3	Test Case 2-UC1: Data Enrichment.....	84
5.1.4	Test Case 3-UC1: Event Classification.....	85
5.1.5	Technology Based Analysis.....	87
5.1.6	Quality Indicators.....	93
5.1.7	Requirements Coverage	96
5.2	Use Case IR-UC2: Managerial Judgement.....	110
5.2.1	Actors	111
5.2.2	Test Case 1 UC2: Managerial Judgement.....	111
5.2.3	Technology Based Analysis.....	112
5.2.4	Quality Indicators.....	113

5.2.5	Requirements Coverage	114
5.3	Use Case IR-UC3: Data Conversion and reporting preparation	125
5.3.1	Actors	126
5.3.2	Test Case 1-UC3: Data conversion and reporting preparation to ECB	126
5.3.3	Test Case 2-UC3: Data conversion and reporting preparation for PSD2	127
5.3.4	Technology Based Analysis.....	128
5.3.5	Quality Indicators.....	130
5.3.6	Requirements Coverage	131
5.4	Validation Summary.....	139
5.5	Lessons Learned and Future Work.....	140
6	Maritime Transport.....	142
6.1	Use Case MT-UC1: Threat Modelling and Risk Analysis for Maritime Transport Service	142
6.1.1	Actors	143
6.1.2	Test Case MT-TC1.....	143
6.1.3	Technology Based Analysis.....	151
6.1.4	Quality Indicators.....	154
6.1.5	Requirements Coverage	157
6.1.6	Comments/Considerations	159
6.2	Use Case MT-UC2 – System Hardening.....	159
6.2.1	Actors	160
6.2.2	Test Case MT-TC2.....	160
6.2.3	Technology Based Analysis.....	163
6.2.4	Quality Indicators.....	163
6.2.5	Requirements Coverage	164
6.2.6	Comments/Considerations	164
6.3	Use Case MT-UC3 – Secure Maritime Communications.....	164
6.3.1	Actors	164
6.3.2	Technology Based Analysis.....	165
6.3.3	Quality Indicators.....	166
6.3.4	Requirements Coverage	166
6.3.5	Comments/Considerations	168
6.4	Use Case MT-UC4 - Trust infrastructure for secure maritime communication	168
6.4.1	Actors	168
6.4.2	Test Case MT-TC4.....	168
6.4.3	Technology Based Analysis.....	168

6.4.4	Quality Indicators.....	171
6.4.5	Requirements Coverage	171
	Comments/Considerations	172
6.5	Validation Summary.....	172
6.6	Lessons Learned and Future Work.....	173
7	Medical Data Exchange	174
7.1	Use Case MD-UC2	174
7.1.1	Actors	175
7.1.2	Test Case MD-UC2-TC-001	175
7.1.3	Test Case MD-UC2-TC-002	176
7.1.4	Test Case MD-UC2-TC-003	177
7.1.5	Test Case MD-UC2-TC-004	178
7.1.6	Test Case MD-UC2-TC-005	179
7.1.7	Test Case MD-UC2-TC-006	180
7.1.8	Quality Indicators.....	181
7.1.9	Requirements Coverage	182
7.2	Validation Summary.....	187
7.3	Lessons Learned and Future Work.....	188
8	Smart Cities	190
8.1	Use Case SMC-UC2.....	190
8.1.1	Actors	191
8.1.2	Test Case SMC-UC2-TC01	191
8.1.3	Technology Based Analysis.....	193
8.1.4	Quality Indicators.....	194
8.1.5	Requirements Coverage	201
8.2	Use Case SMC-UC3.....	205
8.2.1	Actors	206
8.2.2	Test Case SMC-UC03-TC01	206
8.2.3	Technology Based Analysis.....	208
8.2.4	Quality Indicators.....	208
8.2.5	Requirements Coverage	211
8.3	Use Case SMC-UC4.....	214
8.3.1	Actors	215
8.3.2	Test Case SMC-UC04-TC01	215
8.3.3	Technology Based Analysis.....	219
8.3.4	Quality Indicators.....	220

8.3.5	Requirements Coverage	223
8.4	Use Case SMC-UC5	225
8.4.1	Actors	226
8.4.2	Test Case SMC-UC5-TC01	226
8.4.3	Technology Based Analysis.....	227
8.4.4	Quality Indicators.....	229
8.4.5	Requirements Coverage	233
8.5	Use Case SMC-UC6.....	235
8.5.1	Actors	236
8.5.2	Test Case SMC-UC6-TC01	236
8.5.3	Technology Based Analysis.....	237
8.5.4	Quality Indicators.....	239
8.5.5	Requirements Coverage	244
8.6	Validation Summary.....	247
8.7	Lessons Learned and Future Work.....	248
9	Conclusions	250
10	References	251

List of Figures

Figure 1: OBSIDIAN architecture	4
Figure 2: Sharing data anonymously.....	4
Figure 3: Sharing protocol - sending a demand	5
Figure 4 Sharing protocol - contacting several partners with a single request	5
Figure 5: Sharing protocol - establishing a network response	6
Figure 6: OBSIDIAN decision processing.....	6
Figure 7 OBSIDIAN network architecture overview	8
Figure 8 OBSIDIAN client functional architecture	8
Figure 9: OBSIDIAN server functional architecture	9
Figure 10 IBAN declaration.....	9
Figure 11: File format descriptor	10
Figure 12: IBAN request.....	11
Figure 13: The OBSIDIAN dashboard	12
Figure 14: The OBSIDIAN dashboard: data import (1)	12
Figure 15: The OBSIDIAN dashboard: data import (2)	13
Figure 16: The OBSIDIAN dashboard: IBAN validation.....	13
Figure 17: The OBSIDIAN dashboard: IBAN pseudonymisation	13
Figure 18: Participant checking an IBAN anonymously	14
Figure 19: Result of another IBAN check.....	14
Figure 20: Poste Italiane breakdown of revenues (2020).....	20
Figure 21: OAuth 2.0 Account Access Flow	24
Figure 22: General Open Banking Architecture	24
Figure 23: Poste Italiane's Open Banking Architecture	25
Figure 24: An OBA with and without an intermediary.....	26
Figure 25: PSD2 Gateway Operative Model	27
Figure 26: The positioning of Poste Italiane's architecture with respect to the high level OBA	28
Figure 27: MISP architecture	29
Figure 28: Workflow management features.....	42
Figure 29: An excerpt of SCH-UC2 plant construction compliance approval	43
Figure 30: SCH-UC2 use case workflow.....	44
Figure 31: Test results of SCH-UC2-TC1 Authentication.....	46
Figure 32: DNS query	47
Figure 33: Wireshark packet capture	47

Figure 34: Opening the wf-gui application.....	47
Figure 35: User interface tests.....	48
Figure 36: High-level components of the privacy-preserving identity management demonstrator.....	59
Figure 37: Issuance	63
Figure 38: User authentication towards the mobile app using a PIN.....	64
Figure 39: Verification.....	67
Figure 40: Users need to approve which attributes are revealed to a relying party.....	68
Figure 41: The key of the issuer is displayed at the bottom of the screen.....	68
Figure 42:: IR-UC1 - Scenario 1 (Cyber incident caused by ransomware due to phishing email).....	80
Figure 43:: IR-UC1 – scenario 2: Cyber incident caused by DDoS attack on the e-banking website.....	81
Figure 44: IR-UC1 Scenario 3 (Cyber incident caused by DDoS attack on the e-banking website)	82
Figure 45: IR-UC1 – Scenario 4 (Manual shut-down of bank website for investigation after slowdown) .	83
Figure 46: Example of TheHive incident template for the IR-UC1.....	88
Figure 47: Specific information for Mandatory Incident Reporting in TheHive template for IR-UC1	89
Figure 48: Additional information for Mandatory Incident Reporting in TheHive template for IR-UC1 ..	89
Figure 49: Observables added for data enrichment in IR-UC1.....	90
Figure 50: Report generated by the Incident Reporting Event Classifier in IR-UC1	91
Figure 51: Managerial judgement form (IR-UC2).....	113
Figure 52: Green-light managerial judgement (IR-UC2).....	113
Figure 53: Templates menu in IR-UC3.....	128
Figure 54: ECB Template (IR-UC3).....	129
Figure 55: PSD2 template (IR-UC3).....	130
Figure 56: Results of Integration Testing.....	147
Figure 57: Risk assessment performance results	148
Figure 58. Layout of the PKI enrollment.....	169
Figure 59. User interface for creating and submitting a Certificate Signing Request.....	169
Figure 60. User interface for approving Certificate Signing Requests.....	170
Figure 61. Generated certificate in PEM format.....	170
Figure 62: Test case SMC-UC02-TC01 summary.....	192
Figure 63 - Consent Management E2E process	206
Figure 64 - Test case SMC-UC03-TC01 summary.....	207
Figure 65 - Overview of the Porto Data Hub with integration and components	217
Figure 66 - Overview of the Porto Data Hub workflow	218

Figure 67 - Test case SMC-UC05-TC01 summary.....	226
Figure 68 - Test case SMC-UC06-TC01 summary.....	236

List of Tables

Table 1: OBSIDIAN participants.....	2
Table 2: OB-UC02 validation requirements' coverage.	18
Table 3 – Poste Italiane: key consolidated financial targets (2017 – 2022).....	21
Table 4: MISP transaction processes	30
Table 5: MISP pros and cons	30
Table 6: Blockchain pros and cons	30
Table 7: Banking secrecy in Europe	32
Table 8: Supply Chain Security Assurance - SCH-UC1 Requirement Coverage.....	42
Table 9: Supply Chain Security Assurance – SCH-UC2 validation requirements' coverage.	55
Table 10: Supply Chain Security Assurance demonstrator's use cases validation summary.....	56
Table 11: IDM-UC1 Validation requirements' coverage.....	61
Table 12: IDM-UC2 Validation requirements' coverage.....	66
Table 13: IDM-UC3 Validation requirements' coverage.....	76
Table 14: Privacy-preserving identity management demonstrator's use cases validation summary.	77
Table 15: Incident Reporting – IR-UC1 Validation Requirements' Coverage.	110
Table 16: Incident Reporting – IR-UC2 Validation Requirements' Coverage	125
Table 17: Incident Reporting – IR-UC1 Validation Requirements' Coverage	139
Table 18: Incident Reporting demonstrator's use cases validation summary.	139
Table 19: Summary of the results of Unit Testing.....	145
Table 20: Summary of the .java classes included in the Integration Testing	147
Table 21: Results of the discovery procedure	151
Table 22: Security Domains	152
Table 23: Stakeholder Questionnaire	156
Table 24: Maritime Transport –MT-UC1 Validation requirements' coverage.....	159
Table 25: Results of Computational Overhead imposed by VTPin.	161
Table 26: Memory Overhead Summary for VTPin.....	162
Table 27: Overhead for tested Servers	163
Table 28: Requirements' coverage for MT-UC2.	164

Table 29: Requirements Coverage for MT-UC3	167
Table 30: Requirements Coverage for MT-UC4	172
Table 31: Maritime Transport demonstrator's use cases validation summary	173
Table 32: Medical Data Exchange – MD-UC2 Validation requirements' coverage	187
Table 33: Medical Data Exchange demonstrator's use cases validation summary	188
Table 34: Smart Cities - SMC-UC02 Validation requirements' coverage	205
Table 35: Smart Cities - SMC-UC03 Validation requirements' coverage	214
Table 36: Smart Cities - SMC-UC04 Validation requirements' coverage plan	225
Table 37: Smart Cities - SMC-UC05 Validation requirements' coverage	235
Table 38: Smart Cities - SMC-UC06 Validation requirements' coverage	247
Table 39: Smart Cities demonstrator's use cases validation summary	248

List of Acronyms

ABC	Attribute Based Credential
AGPL	Affero General Public License
AIRE	Atos Incident Reporting Engine
API	Applicationn Programming Interface
ASPSP	Account Servicing Payment Service Provider
BFT	Byzantine Fault Tolerance
BPMN	Business Process Model and Notation
CA	Certificate Authority
CAGR	Compound Annual Growth Rate
CAPEC	Common Attack Pattern Enumeration and Classification
CAPEX	Capital Expenditure
CERT	Computer Emergency Response Team
CFT	Crash Fault Tolerant
CISO	Chief Information Security Officer
CRI	Credential Revocation Information
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVE	Common Vulnerabilities and Exposures
DANS	Data ANonymization Service
DDoS	Distributed Denial of Service
DEP	Data Exchange Platform
DLT	Distributed Ledger Technology
DNS	Domain Name Service
EBA	European Banking Authority
ECB	European Central Bank
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECTS	European Credit Transfer System
eID	Electronic Identity
eIDAS	Electronic Identification Authentication and trust Services

EPC	Engineering, Procurement and Construction (The purchaser)
ESB	Enterprise Service Bus
EU	European Union
FI	Financial Institution
FMFC	French Monetary and Financial Code
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation
GE	Generic Enabler
GUI	Graphical User Interface
HE	Homomorphic Encryption
HLF	Hyperledger Fabric
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IALA	International Association of Marine Aids to Navigation and Lighthouse
IBAN	International Bank Account Number
ICT	Information and communications technology
ICLT	Incident Classification Team
IDP	Identity Provider
ISPS	International Ship and Port facility Security
ID	Identity
IMO	International Maritime Organization
IMT	Incident Management Team
IP	Internet Protocol
IR-Ucx	Incident Reporting Use Case x
IRT	Incident Reporting Team
IT	Information Technology
IOC	Indicator Of Compromise
JDK	Java Development Kit
JSON	JavaScript Object Notation
JWT	Json web token

KPI	Key Performance Indicator
LDAP	Local Directory Access Protocol
LPA	Local Public Administration
MISP	Malware Information Sharing Platform
ML	Machine Learning
MMSI	Maritime Mobile Service Identity
MSW	Maritime Single Window
MPC	Multiple Party Computation
MSP	Membership Service Provider
N/A	Not Available
NATO	The North Atlantic Treaty Organization
NFC	Near-Field-Communication
NIS	Network and Information Security
OBA	Open Banking Architecture
OBACHT	Open Banking API Architecture
OBSIDIAN	Open Banking Sensitive Data Sharing Network for Europe
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
PEM	Privacy-enhanced Mail
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPA	Piraeus Port Authority
PSD2	Payment Services Directive 2
PSU	Payment Services User
PT	Pen tester
REST	Representational State Transfer
ROE	Return On Equity
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SCA	Strong Customer Authentication
SCM	Software Configuration Management
SCS	Supply Chain Service

SDK	Software Development Kit
SGX	Software Guard Extensions
SHA-2	Secure Hash Algorithm 2
SIEM	Security Incident and Event Management
SSL	Secure Socker Layer
SSO	Single Sign On
SQL	Structured Query Language
TEE	Trusted Execution Environment
TCP	Transmission Control Protocol
TCx	Test Case x
TLS	Transport Layer Security
TPP	Third Party Provider
TPS	Transactions Per Second
TTP	Trusted Third Party
UI	User Interface
URL	Uniform Resource Locator
UX	User Experience
VAS	Value-Added Services
VDES	VHF data exchange system
VHF	Very High Frequency
VTs	Vessel traffic service
ZKP	Zero Knowledge Proof

1 Introduction

This Deliverable D5.3 titled *Validation of Demonstration Case Phase 1* is the result of the combined work from research centers, industry members and partners in WP5. A total of seven demonstration cases have been identified based on an initial set of requirements. These requirements played a key role in identifying the technological and research roadmaps of the project.

The demonstration cases form the core of the project emerging from the collaborative efforts between multiple Work Packages (3, 4, and 5). One of the project's goals is for the demonstration cases to adopt in their lifecycle the technological components created by WP3. The road to reach these goals is structured as a double cycle of research and development. The first cycle gives an initial definition of the research challenges and roadmaps that will drive the second iteration of the project. The second cycle will further refine the research goals of the project to exhaustively address cybersecurity challenges, and make them relevant beyond the scope of the project.

This document is a follow up of the Deliverables D5.1 and D5.2 and here we focus on the validation objective, strategy and summarize the results. For each demonstrator use case we follow a structure where the validation approach is outlined including a description of what aspects will be validated and how they will be validated. The validation approach can be done either via a test case approach or using a technology based analysis or in some use case both approaches seem relevant as is illustrated in the use cases in this document. The test case approach follows a scientific and software engineering methodology including a description, workflow and documenting the test results. The technology based validation approach follows an analytical approach inferred from the technology implementation.

D5.3 is the next logical step in CyberSec4Europe's roadmap. D5.3 also marks the end of the first cycle and in the lessons learned section of each use case we take this opportunity to highlight the aspects that could not be included in this cycle and will be addressed in the next cycle.

1.1 Structure of the Document

The document is structured into 9 sections with the sections 2 to 7 presenting the demonstrator cases followed by the conclusion in the last section

- Section 2 presents the validation of the *Open Banking* demonstrator case in CyberSec4Europe WP5
- Section 3 presents the validation of the *Supply Chain Security Assurance* demonstrator case in CyberSec4Europe WP5
- Section 4 presents the validation of the *Privacy-preserving Identity Management* demonstrator case in CyberSec4Europe WP5
- Section 5 presents the validation of the *Incident Reporting in the Financial Sector* demonstrator case in CyberSec4Europe WP5
- Section 6 presents the validation of the *Maritime Transport* demonstrator case in CyberSec4Europe WP5
- Section 7 presents the validation of the *Medical Data Exchange* demonstrator case in CyberSec4Europe WP5
- Section 8 presents the validation demonstration of the *Smart Cities* demonstrator case in CyberSec4Europe WP5
- Section 9 provides the conclusion

2 Open Banking

This first phase demonstrator is focused on scenarios in the two use cases:

- OB-UC2 OBSIDIAN (Open Banking Sensitive Data Sharing Network for Europe)
- OB-UC4 OBACHT (Open Banking API Architecture)

It had been hoped to include the use case OB-UC1 Sharing of Identity Verification and Fraudulent Activity, which was initially outlined in D5.1 and then considerably modified in D5.2 featuring scenarios that include, inter alia, the infrastructure developed for OB-UC2 OBSIDIAN. It is now anticipated that further development of OB-UC1, stymied in part as a result of COVID-19 restrictions that inhibited in-depth partner collaboration during the latter half of 2020, will take place during the second phase of T5.1.

2.1 Use Case OB-UC2 – OBSIDIAN

The primary objective of this use case is to demonstrate how fraud-related information can be shared between participating banks and/or other financial institutions, while remaining in conformity with the GDPR and banking secrecy regulations. To that end, the task has developed an implementation of a trust network aimed at providing financial institutions with a channel to share and exchange critical information about effective frauds, in near real time and in a privacy-preserving manner, leveraging the latest online open banking services.

The goal of this trust network is, by making such sharing possible, banks are able to improve their ability to detect and react in real time to cases of fraud. For example, when a bank detects a transfer fraud, it is then able to share the information about the IBAN implied in the transfer with other banks, which can take this information into account at the time to prevent the fraudster from using this IBAN to carry out other fraudulent transactions.

In order to validate the use case, we will be looking at the architecture and supporting technologies, compliance to the GDPR as well as the usability of the system in operation.

2.1.1 Actors

This use case has been carried out and validated out by the participants in the demonstrator i.e.,

Participant	Country	Role(s)	Validation
i-BP (Groupe BPCE)	France	Developer / Technology owner	Technical evaluation
ABI Lab	Italy	User/stakeholder/expert	
Trust in Digital Life	Belgium	User	Questionnaire
CaixaBank	Spain	User/stakeholder/expert	
Poste Italiane	Italy	User/stakeholder	

Table 1: OBSIDIAN participants

The validation of the quality indicators was performed by the technology owner, i-BP.

2.1.2 Test Case

2.1.2.1 Description

The objective of this use case is to address the increase in banking fraud¹ and digital banking cybersecurity challenges² by creating a European network for sharing fraud information between open banking players. The role of the proposed network is to enable national and cross-border cooperation between banks to prevent fraud by immediately sharing fraud information (like, for example, an IBAN implied in a transfer fraud) within a secure, trusted network once a fraudulent attack occurs whilst protecting the data in transit. The role of the network is to share fraud information within the network and establish user experience trust levels; and, in so doing, provide network access to data and money laundering information and share terrorist financing information in the network.

The core requirements of the demonstrator are:

- Bank anonymity
- Regulatory compliance
- Sharing information without transferring underlying data ownership
- Real-time sharing
- Privacy by design

2.1.2.2 Test case workflow

There are four key stages to this use case:

- (1) Each bank owns a list of fraudulent IBANs associated with frauds and fraud attempts, stored in a local database. In France, at least, each major bank has already built such a list.
- (2) Each IBAN is pseudonymised (through hashing and encryption techniques) before being committed into a dedicated OBSIDIAN database
- (3) The OBSIDIAN server broadcasts IBAN check requests and federates responses: **it doesn't store any business data**
- (4) The OBSIDIAN client is responsible for guaranteeing the local pseudonymised IBAN database is connected to the network

See also Figure 1 for the use case initial set up.

¹ An increase of 36% in payment fraud (in terms of amount) in 2018 in France, the accelerated development of online scams, the lack of effective means to fight against fraud operating modes where the customer is manipulated or the customer is the fraudster

² For example: instant payments, the rise in the opening of online accounts, the market supremacy of non-European ICT companies in delivering transaction scoring services which are fully cloudified

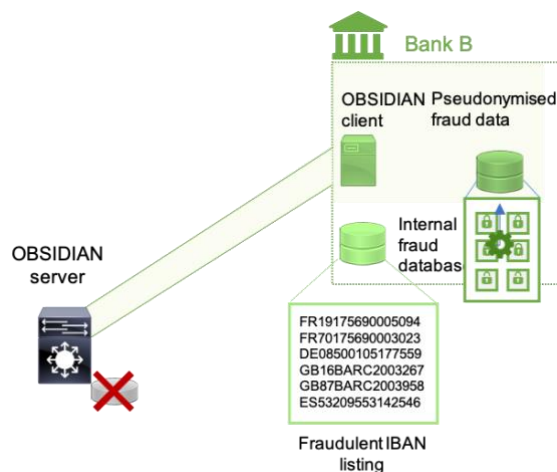


Figure 1: OBSIDIAN architecture

By centralising information exchange flows, the OBSIDIAN server makes it possible for banks to exchange information pseudonymously – see Figure 2. Additional technologies have been studied to improve the anonymity of the data and the banks; for example, by fragmenting TCP packets on the network and making them transit through several intermediate servers.

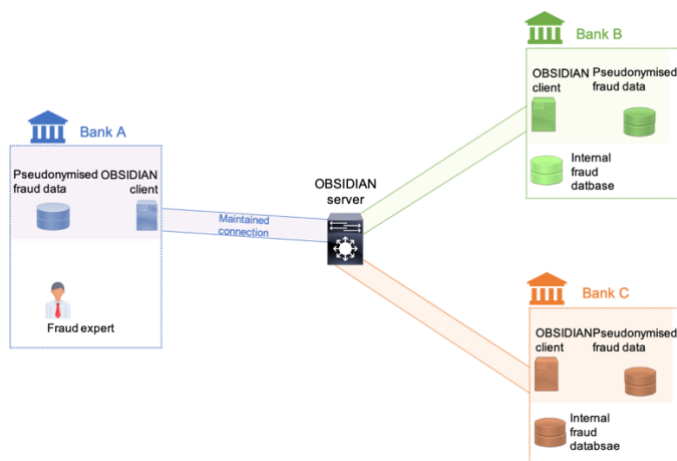


Figure 2: Sharing data anonymously

When a fraud manager (or a system) of a participating bank detects a suspicious transaction and wants to check the beneficiary's IBAN, she will use the OBSIDIAN client to protect it (through pseudonymisation and encryption) and then send a check request to the OBSIDIAN network – see Figure 3.

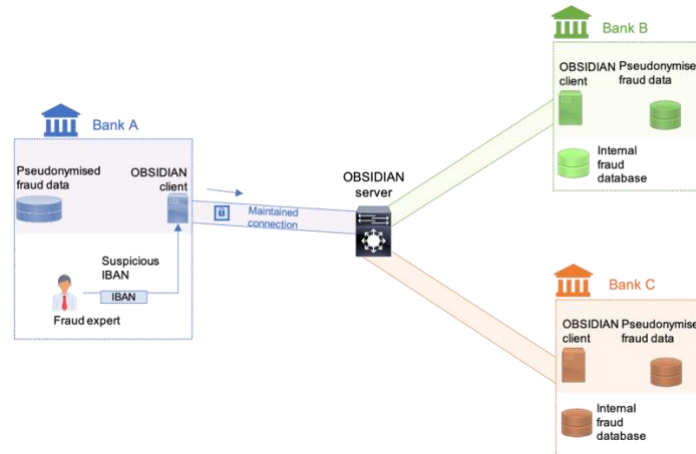


Figure 3: Sharing protocol - sending a demand

The OBSIDIAN server broadcasts Bank A's requests to the other network participants (Banks B and C), without storing any of data itself, except for some statistics measuring network KPIs – see Figure 4. The receiving banks – B and C – don't know the origin of the request (Bank A) but they trust it. This trust is guaranteed through network governance principles, strong authentication mechanisms used in the OBSIDIAN clients (for requests originated by humans) and API authorisation mechanisms (for requests originated by bank systems).

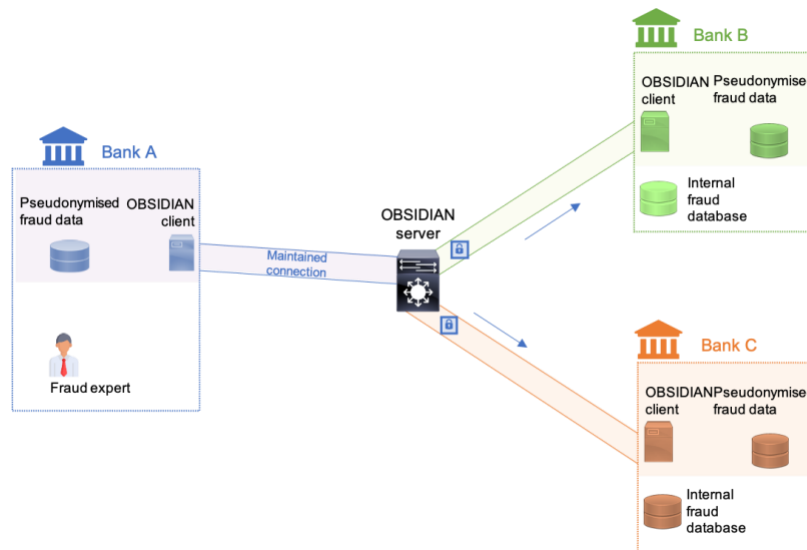


Figure 4 Sharing protocol - contacting several partners with a single request

The check demand recipients (i.e., Banks B and C) apply a second layer of encryption, selecting their own pseudonymised data which is protected in the same way Bank A pseudonymised the request (with different secret keys). Once done the banks send back the request with another encryption layer and their own pseudonymised data to the OBSIDIAN server which then relays these responses to Bank A. Throughout the transaction process, the data is never decrypted and in fact it cannot be as the keys remain secret. As such Bank A is unable to identify which banks answered its check demand – see Figure 5.

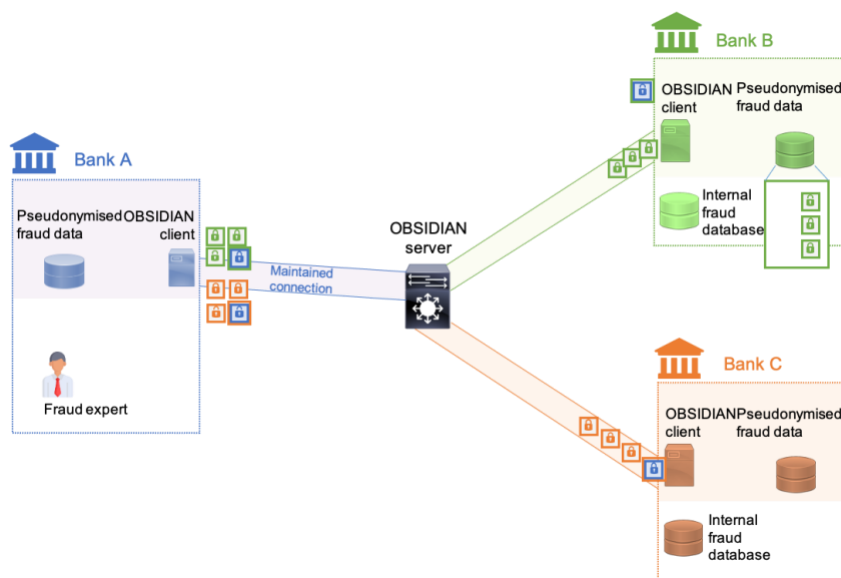


Figure 5: Sharing protocol - establishing a network response

Bank A adds a second layer of encryption to the response data it's received and is now in a position to compare the responders' data to the initial request, based on the commutative properties of the encryption algorithm. If a strict equality is found, Bank A knows that another bank has identified its suspicious IBAN as fraudulent and can then confidently take the right decision to protect its clients – see Figure 6.

It should be noted that the role of the OBSIDIAN network is only to support the data exchange, without interfering into any of the banks' internal decision processes.

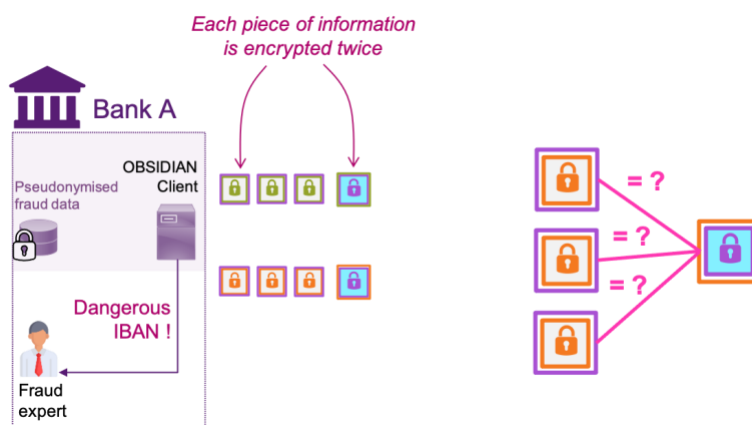


Figure 6: OBSIDIAN decision processing

2.1.2.3 Test results

The objectives of the test were validated through the following criteria:

- Protection of banking secrecy
 - Bank B and Bank C did not know the fraud request came from Bank A
 - Bank A could not identify the origin of the request responses
 - Bank B and Bank C did not know the result or outcome of the request

- In the exchange, no one knew who exchanged information with whom
- GDPR compliance
 - The OBSIDIAN server did not store any fraud data
 - IBANs were always pseudonymised when exchanged
 - Banks could take back their data whenever necessary (GDPR right to erasure compliant)
- Usability
 - No complicated mathematics: technology easily understood by IT experts
 - Simple integration: one client connected to one server only
- EU-wide availability
 - Applicable to the countries with the most restrictive secrecy laws
 - Can easily be expanded into a European network

2.1.3 Technology Based Analysis

2.1.3.1 Architecture

The underlying principle of the trust network is that it is based on secure multi-party computation (MPC) and consists of:

- centralised architecture for exchange flows
- decentralised data storage
- data protection based on hash and encryption mechanism

This is achieved through a central network server that communicates securely to numerous network clients deployed at each node in the network – the participating financial institutions. Key to the trustworthiness of the network is that no sensitive data is stored on the central network server – all fraud-related data is stored locally at each network node, independent of the network server and all the other nodes in the network – see Figure 7.

Fraud data – in this use case, IBANs – is encrypted with Elliptic Curve Diffie Hellman (ECDH) used to generate a shared key each time data is transferred between the network clients and the server. The implementation deployed uses Elliptic Curve Cryptography (ECC) implemented in JavaScript to offer a very simple OBSIDIAN client consisting of a web app usable for any fraud manager/banking expert without requiring her to install any software on her workstation.

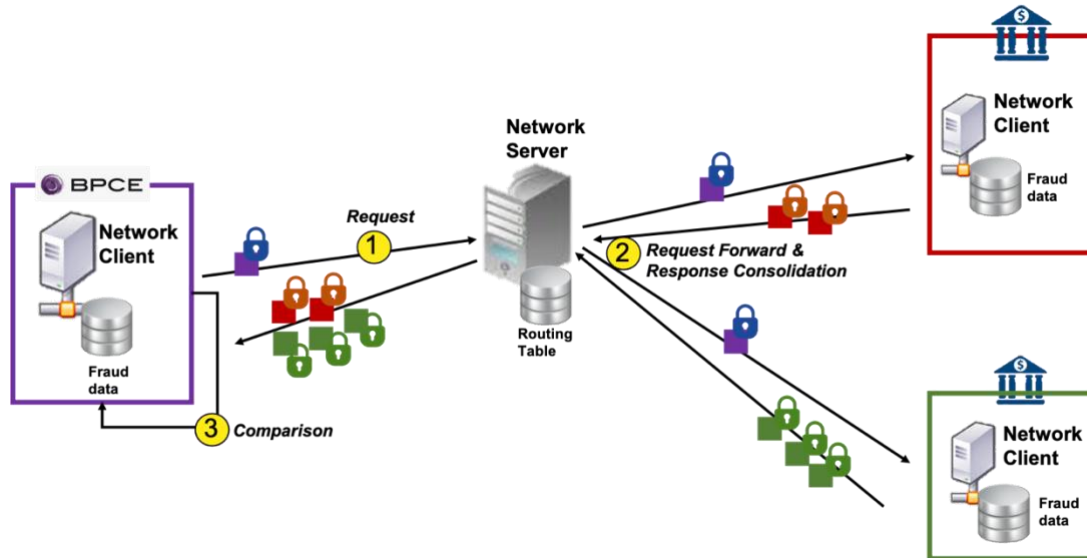


Figure 7 OBSIDIAN network architecture overview

2.1.3.2 Network Client

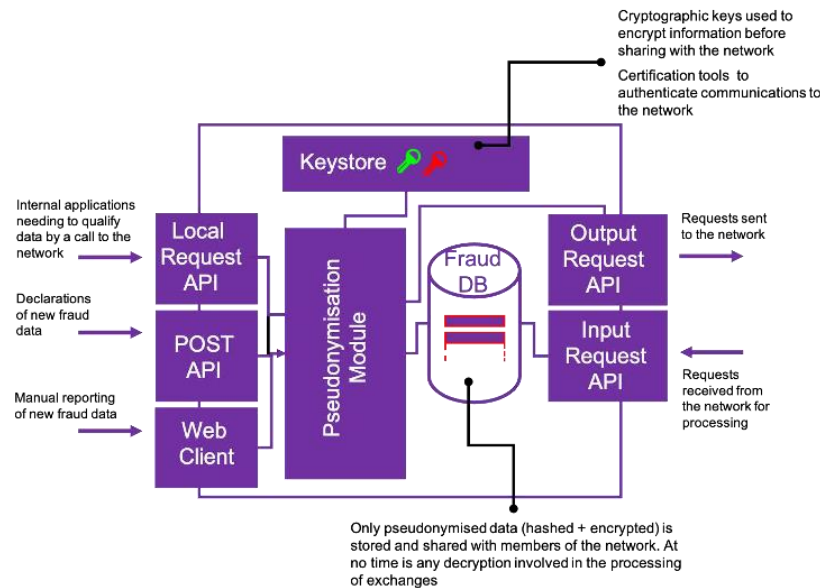


Figure 8 OBSIDIAN client functional architecture

The functional architecture of the network client is described in Figure 8, and consists of:

- A local database, containing fraud data, hashed and encrypted through the pseudonymisation module using cryptographic keys kept in the local keystore
- A suite of input and output APIs to manage:
 - incoming and outgoing requests to and from the network
 - requests and declarations from the organisation itself

2.1.3.3 Network Server

The network server has three key functions :

- The validation of incoming requests
- The orchestration of incoming and outgoing calls
- The monitoring and management of the overall operation of the network

It consists of :

- A local database, containing a routing table with the URLs of the network participants and logging information
- An orchestration ‘cockpit’ to manage the validation, monitoring of incoming onboarding and fraud requests from network participants
- Modules to dispatch fraud requests across the network

See also Figure 9.

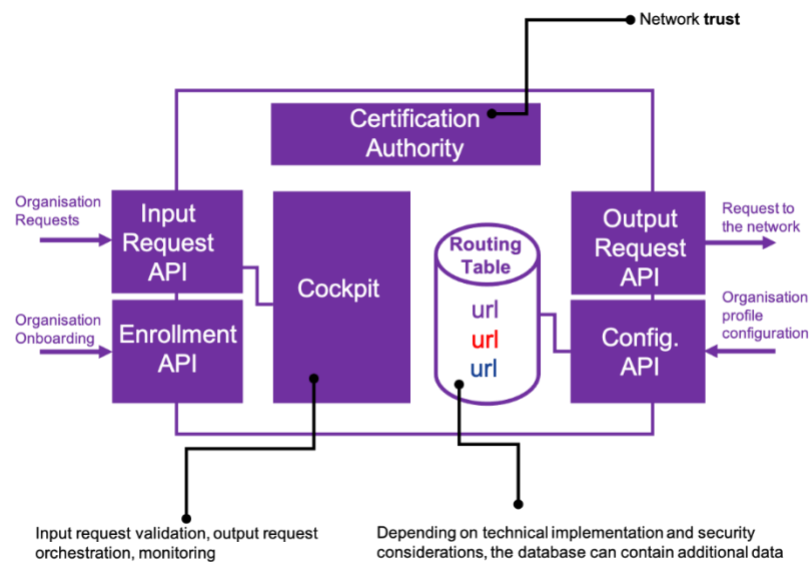


Figure 9: OBSIDIAN server functional architecture

2.1.3.4 Network Operation

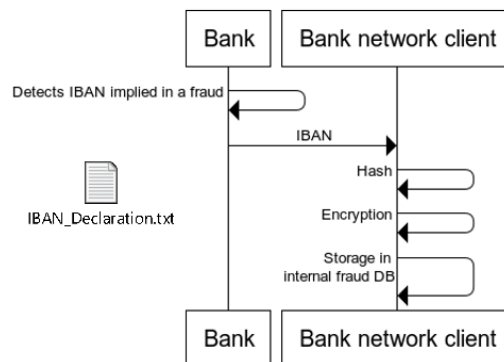


Figure 10 IBAN declaration

Below is an example of an IBAN declaration text; in this first phase, we are only using IBANs which are submitted with a timestamp and an operational mode indicator. Users are provided with an informational pop-up box (figure 11) to guide them through data input which can either be file-based or manual.

File formats ×

Spreadsheet files (xls, csv, xlsx) are accepted. The data needs to be formatted as seen below:

timestamp	iban	opmode
2019-3	IT37B6275383566610705115170	usurpation
2019-11	DE58578639645846954754	cheque

Three type of data are accepted: timestamp, IBAN and operating mode. The header must be specified in the spreadsheet exactly as shown above.

You can also give a '.txt' file containing only one IBAN per line.

OK

Figure 11: File format descriptor

The process of preparing the fraud data is described in figure 10.

```
timestamp;iban;opmode
2019-3;FR2086731326479752779667932;cheque
2019-8;GB06MVBV76966243972507;cheque
2019-5;SI47506064452931647;usurpation
2019-5;ES1489931407043356870584;usurpation
2019-7;DE20337609957863189931;cheque
2019-2;ES3984188871230420737607;manipulation
2019-9;ES6747733292821434852583;usurpation
2019-5;ES5343685390702122851572;manipulation
2019-8;GB10OIZA10220492691499;manipulation
2019-5;IT32G5914176675MMWHZIPDHSZY;usurpation
2019-8;GR0501072341269518441633288;manipulation
2019-5;HR7925000092925423384;usurpation
```

Table 2: Sample fraud data

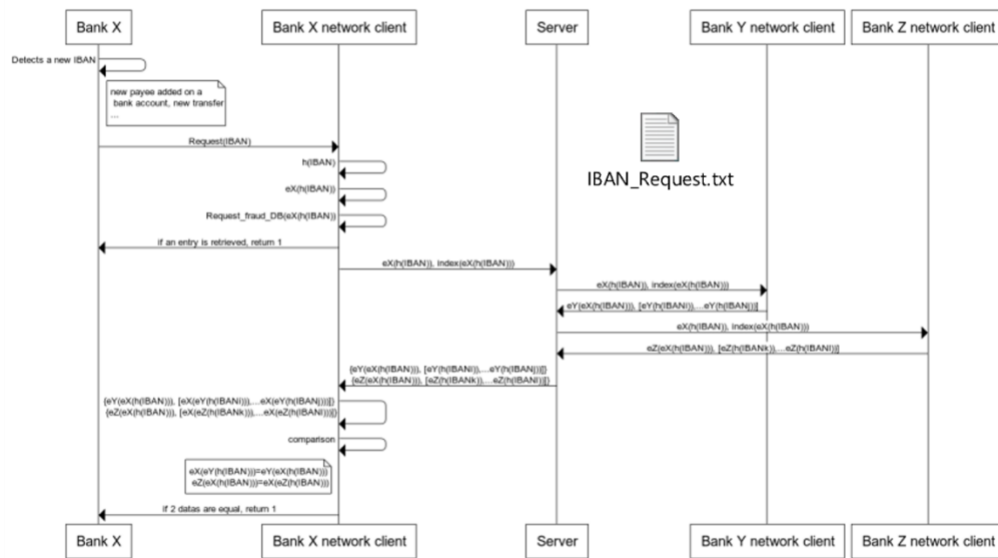


Figure 12: IBAN request

To meet performance requirements, several optimisations were studied:

- ❑ Instead of being able to encrypt a network response with her own key, the requester can only decrypt her request data (IBAN hash), this way avoiding x encryption operations – x being the number of potential matched IBANs transmitted in the network response.
- ❑ Using asymmetric encryption to protect privacy, it would be possible for the requester to directly encrypt her own request data by using the public keys of the other participants in the network. This operation could be realised in parallel with the network request to save necessary encryption time. However, in this circumstance, the encryption key would become public, with a data security impact.

2.1.3.5 Usability

Initial trials of the OBSIDIAN network took place with the actors listed above and a live demonstration of the network took place to an online audience of about 100 participants as part of the CyberSec4Europe session during the CONVERGENCE event on the morning of 10 December 2020. 5,000 IBANs were introduced by one of the participants and a number of checks were made against them to demonstrate IBANs recognised as being suspicious or dangerous as well as not being recognised (i.e., not known to be dangerous etc). For the purposes of the experimentation, both at the event and privately, the IBANs used were false.

The demonstration is launched from the dedicated use case website – <https://experiment.obsidian-project.eu/> – which provides a number of demonstration options (yet to be completed) and access to the ‘OBSIDIAN Experimentation’ for authenticated users who are presented with the OBSIDIAN dashboard. Figures 13-17 show the welcome screen and the process of importing a data file followed by the validation and pseudonymisation processes.

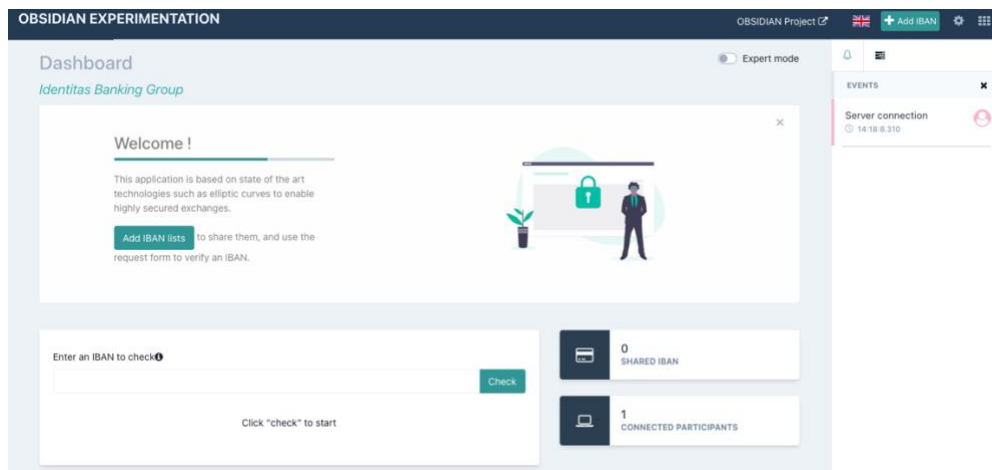


Figure 13: The OBSIDIAN dashboard

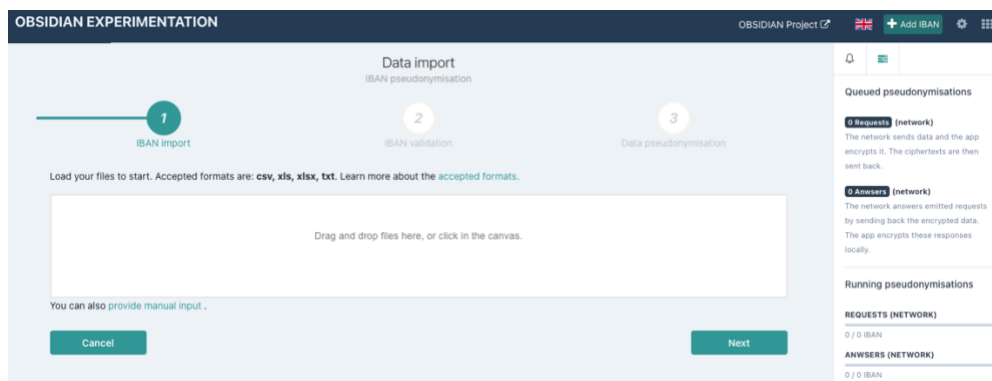


Figure 14: The OBSIDIAN dashboard: data import (1)

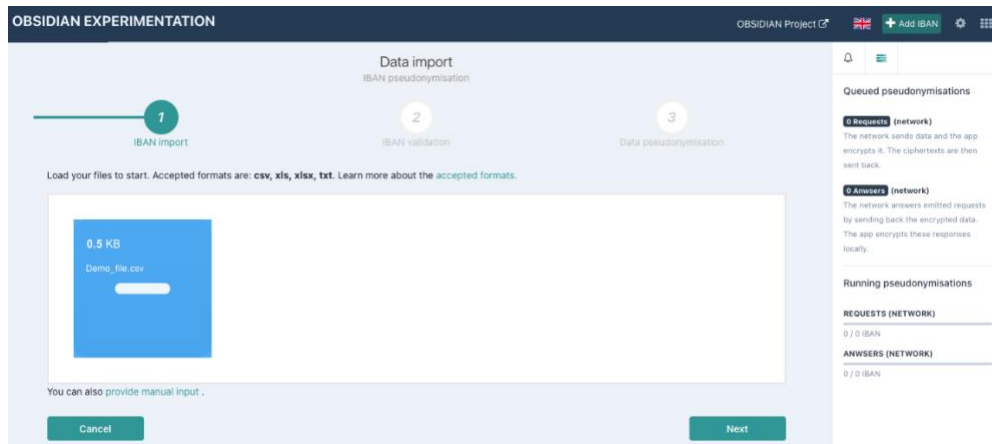


Figure 15: The OBSIDIAN dashboard: data import (2)



Figure 16: The OBSIDIAN dashboard: IBAN validation

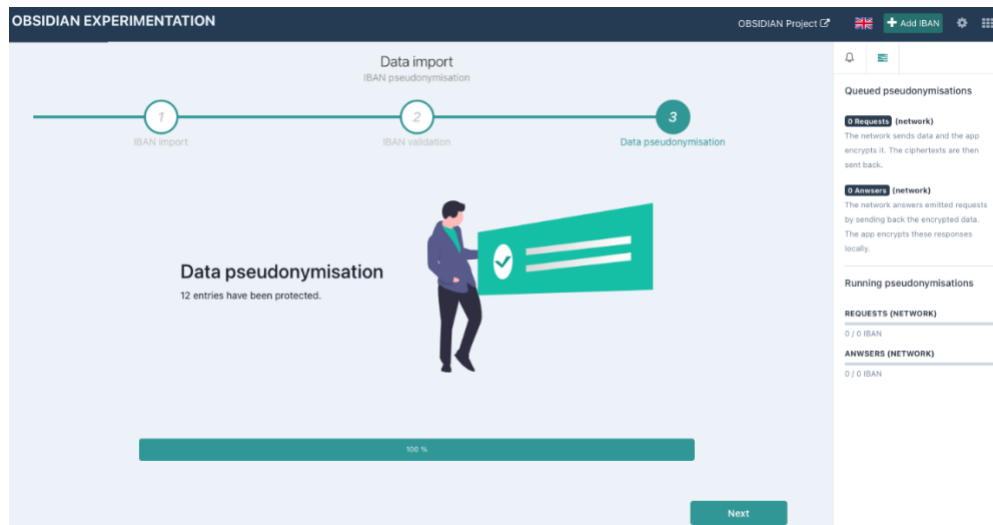
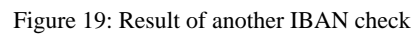


Figure 17: The OBSIDIAN dashboard: IBAN pseudonymisation



2.1.4 Quality Indicators

This category comprises the following sub-categories:

- Although we have been focused on the demonstrator use case, we are also looking beyond to running OBSIDIAN and later developments in a production environment as a commercial deployment. Hence, the

quality indicators and supporting questions were partially designed to provide the project with a consistent methodology in order to validate the solution in a real-world production environment; for example, the KPIs on fraud fight efficiency. Not surprisingly, as we still are in a prototyping phase, it is complicated to answer some of the questions validating some aspects of performance aspects and the efficiency in fighting fraud until we have real-world feedback resulting from a production deployment.

To succeed in deploying such a sharing practice in our production environments, the next steps are to work on plausible use case scenarios, involving:

- European actors to provide legal /regulatory solutions and lobbying efforts particularly in the context of regulatory compliance; and
- European banking partners to build the value of the network value

We have made good progress in both these respects but there is more work to do in the second phase of this task.

2.1.4.2 Questions

Identified are five sets of key performance indicators.

(1) Requirements

Taking part in the OBSIDIAN network, the number of:

- Stakeholders should be equal to or greater than three
- Fraud experts should be equal to or greater than three
- Countries should be equal to or greater than two
- IBANs shared by each stakeholder should be greater than two thousand

(2) Threat resilience

We anticipate the following threat scenarios:

- Illegal enrolment to the network
- Illegal access to the APIs requesting access to the network
- Unauthorised modification
- Unauthorised escalation of privilege
- Data leak
- Sharing of compromised or fake data

In addressing these threat scenarios:

- What is the percentage of threat scenarios covered?
- What is the number of threat scenarios covered?

(3) Quality of service (QoS)

- What is the average API call response time?
- What is the average API availability?
- What is the rate of successful API calls?
- What is the number of failed or rejected API calls due to a technical incident?

(4) Efficiency in fighting fraud

- What is the number of requests producing a risk alert?
- What is the rate of requests producing a risk alert?
- What is the rate of OBSIDIAN alerts producing a false positive?
- How many potential frauds were prevented due to OBSIDIAN alerts?
- What is the maximum and average financial loss from fraud prevented by OBSIDIAN alerts?
- What is the total value of the financial loss from fraud prevented by OBSIDIAN alerts?

(5) User adoption / usability

- How many teams are there for each stakeholder using OBSIDIAN?
- What is the total number of people for each stakeholder using OBSIDIAN?
- What is the average and maximum number of requests per day of each stakeholder?
- What is the total number of requests for each stakeholder?
- What is the average and maximum number of queries processed by each stakeholder?
- What is the average and maximum number of queries processed per day by each stakeholder?
- How many IBAN updates were shared by each stakeholder?
- How many user incidents were posted by each stakeholder?

2.1.4.2.1 Feedback

(1) Requirements

- Stakeholders should be equal to or greater than three. **Four (Groupe BPCE, Caixa Bank, Poste Italiane, ABI Lab)**
- Fraud experts should be equal to or greater than three. **Three (Groupe BPCE, Caixa Bank, ABI Lab)**
- Countries represented should be equal to or greater than two. **Three (France, Spain, Italy)**
- IBANs shared by each stakeholder should be greater than two thousand. **In total we shared 5,000 (fake) IBANs amongst the stakeholders**

(2) Threat resilience

- What is the percentage of threat scenarios covered? **70%**
- What is the number of threat scenarios covered? **Four (out of six)**

(3) Quality of Service

- What is the average API call response time? **Less than a second**
- What is the average API availability? **Although we do not have a more holistic answer for the moment as we still are prototyping the targeted solution, nevertheless, the prototype's API was always available when we tested it.**
- What is the rate of successful API calls? **100%**
- What is the number of failed or rejected API calls due to a technical incident? **Zero**

(4) Efficiency in fighting fraud

We cannot answer these aspects of the quality indicators accurately at present as we are still prototyping the targeted solution with fake data.

(5) User adoption / usability

- How many teams are there for each stakeholder using OBSIDIAN? **One team (Fraud CERT)**
- What is the total number of people for each stakeholder using OBSIDIAN? **Between one and five**

For the remainder of the quality indicators in this section, as with fraud fight efficiency, we cannot answer realistically answer the rest of the indicators at present, as we still are prototyping the targeted solution with fake data/activity.

2.1.5 Requirements Coverage

The following table lists the requirements this use case implements and whether they were validated or not.

ID	Validated	Strategy	Result	Mandatory
OB-SP01	Yes	Technology analysis	Success	Yes
OB-SP02	Yes	Technology analysis	Success	Yes
OB-SP03	Yes	Technology analysis	Success	Yes
OB-SP04	Yes	Technology analysis	Success	Yes
OB-SP05	Yes	Technology analysis	Success	Yes
OB-SP06	Yes	Technology analysis	Success	Yes

ID	Validated	Strategy	Result	Mandatory
OB-SP07	Yes	Technology analysis	Success	Yes
OB-SP08	Yes	Technology analysis	Success	Yes
OB-SP09	Partially	Network governance analysis	Success	No
OB-SP10	Partially	Network governance analysis	Success	No
OB-SP11	Yes	Technology analysis	Success	Yes
OB-SP12	Yes	Technology analysis	Success	Yes
OB-SP13	Yes	Technology analysis	Success	Yes
OB-SP14	Yes	Technology analysis	Success	Yes
OB-SP15	Yes	Technology analysis	Success	Yes
OB-SP16	Yes	Technology analysis	Success	Yes
OB-SP17	Yes	Technology analysis	Success	Yes
OB-SP18	Yes	Technology analysis	Success	Yes
OB-SP18	Yes	Technology analysis	Success	Yes
OB-SP19	Yes	Technology analysis	Success	Yes
OB-SP20	Yes	Technology analysis	Success	Yes
OB-SP21	Yes	Technology analysis	Success	Yes
OB-SP22	Yes	Technology analysis	Success	Yes
OB-SP23	Yes	Technology analysis	Success	Yes
OB-SP24	Yes	Technology analysis	Success	Yes
OB-SP25	Yes	Technology analysis	Success	Yes

Table 2: OB-UC02 validation requirements' coverage.

2.2 Use Case OB-UC4 Open Banking API Architecture Platform (OBACHT)

During the course of the preparation for investigating into the proposed use cases outlined in D5.2, it became increasingly clear that there could be some difficulties in finding a suitable platform on which to carry out the tests. This was primarily due to the unwillingness of many financial institutions to open their

infrastructure as a testbed environment, due to the technical and commercial sensitivities associated with providing access for the cybersecurity tests.

Again as part of the investigation, it transpired that, although CyberSec4Europe's associate partner Poste Italiane was willing and prepared to participate in the use case demonstration, the bank had taken a very different approach to the design and implementation of its Open Banking infrastructure architecture from the one designed by ABI Lab. As a consequence, it could not be meaningfully used to demonstrate the proposed test cases in the manner originally intended, and, as such, a decision was taken to perform a comparison of the model architecture and the Poste implementation.

2.2.1 Open Banking Architecture

The main objective of the following analysis is to investigate the main aspects in which the Open Banking Architecture (hereinafter, OBA) developed in the CyberSec4Europe project and a real OBA implemented by a selected stakeholder differ. To this end, Poste Italiane was selected as a stakeholder for piloting activities. To achieve our objective, we will make a high level comparison of both logical architectures.

Among the differences found, we will see that, despite Poste Italiane implementing one of the most important set of technical reference standards (Berlin Group, Open Banking Implementation Entity, etc), the architectural model adopted is non-standard. It essentially provides for an additional stakeholder who plays the role of "broker" of services and therefore forms a "front end" to the users of the PSD2 Open API.

The marked differences found "in the field" will certainly provide good feedback for the project, because, in addition to highlighting a considerable gap between the two approaches, it could position the CyberSec4Europe project's OBA solution as a model for integrating existing solutions, proposing itself as a layer of measures that apply regardless of the technological context in a complementary and advantageous way.

In addition, we depicted the Auth2 flow in the user access case, as OAuth 2.0 is the foremost security standard for delegating authorisation and is supposed to be implemented in most Open Banking Architecture deployments as well as at Poste Italiane.

2.2.1.1 Poste Italiane

Alongside its historical business as a mail and logistics service provider, underpinned by the most widespread distribution network in Italy, Poste Italiane has also become a major national player in the financial services and insurance market. The *Deliver 2020 strategic plan* additionally identified a new business area for the group, dedicated to mobile and digital payments, based on the growing convergence of these sectors.

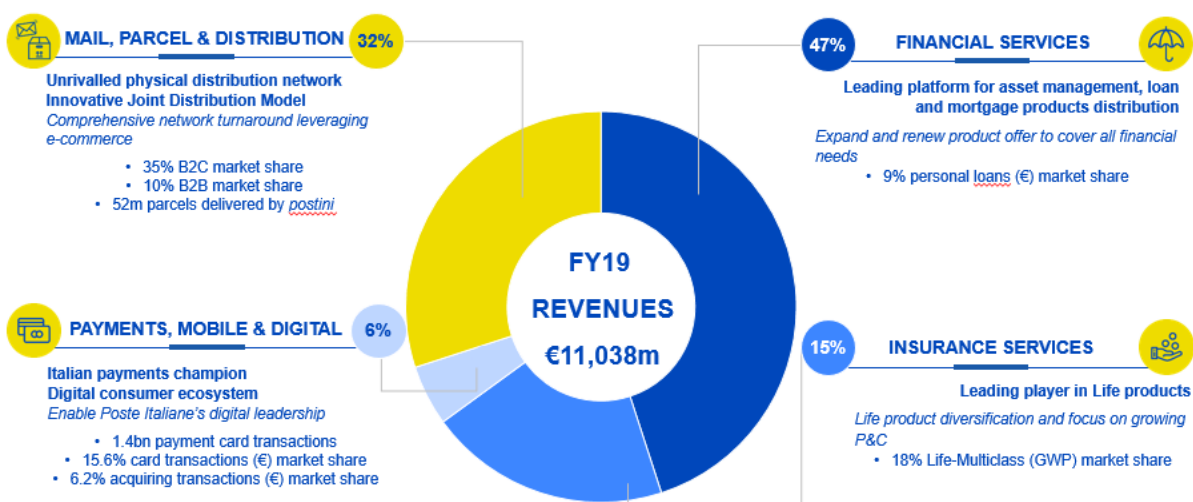


Figure 20: Poste Italiane breakdown of revenues (2020)

The unified and integrated management of the group means Poste Italiane is able to develop synergies and ensure a uniform, coordinated approach to the market, building on the strength of its brand and of its multi-channel distribution platform. All four business areas revolve around the central focus placed on the customer and on building long-term relationships of trust with households, enterprises and the public sector, offering them a wide range of simple, transparent services.

Payments, Mobile and Digital

This new business division is the outcome of the Deliver 2022 strategic plan, which groups together:

- The e-money and electronic payments sector;
- 'Poste Mobile' mobile telephone operations;
- all new initiatives tied to the digital world.

The new division is also tasked as an internal competency centre for driving digital transformation.

2.2.1.1.1 Financial Services

Poste Italiane provides traditional and online digital financial services through the separate operations of BancoPosta, one of the biggest players today in the Italian financial services market.

In particular, offered services include:

- current accounts (digital and mobile operations);
- promotion and distribution to the public of loans provided by banks and financial intermediaries;
- collection of postal savings.

Poste is still expanding its collective asset management operations.

2.2.1.1.2 Financial Targets

- Forecast 2022 consolidated revenues: €11.2 billion, compound annual growth rate (CAGR): 1%;
- Forecast 2022 operating profit: €1.8 billion, with a CAGR of 10%;
- Forecast 2022 net profit: €1.34 billion, with a CAGR of 13%;
- 2022 Return On Equity (ROE): 13% (+3.4 p.p.);

- Customer's Total Financial Assets: €581 billion (2019: €536 billion)
- 2018–2022 capital investments: €2.8 billion of capex to support the digitalisation, automation and reorganisation of the service model;

2.2.1.1.3 Key Consolidated Financial Targets (in euro unless stated otherwise)

	2017	2018	2019	2020	2022	CAGR 17 - 22
Revenue	10.6	10.86	11.4	11.1	11.2	+ 1%
EBIT	1.1	1.50	1.77	1.8	1.8	+ 10%
EBIT Margin %	11%	14%	16%	17%	16%	
Net Profit	0.7	1.40 ¹	1.34 ²	1.3	1.2	+ 13%
Dividend (€/share)	0.42	0.44	+0.463%	+5%		

Table 3 – Poste Italiane: key consolidated financial targets (2017 – 2022)

3.2.1 Actors

The following case describes the OAuth 2.0 authentication and authorisation process in which the following parties are involved :

- TPP: Trusted Third Party (website or app) ;
- ASPSP: Account Servicing Payment Service Provider (banks) ;
- End user(s)

2.2.2 Test Case: Account Access APIs

2.2.2.1 Description

To access the API endpoint, the app will first make a call to the OAuth API to get a client access token, then create an account request which will have the details of the access required. The account request contains information like account information permissions, the permission expiration time etc. Once the account request is created, the app requests an access token. While providing the consent, the user selects the list of accounts they want the app to get access to.

The application now gets an access token to access account(s) on behalf of the user. We assume also that the OAuth APIs support both the implicit grant flow whereby the access token is returned directly to the app once the user has authenticated. If the app wishes to keep the authentication more secure, then the app could also use the authorisation code flow whereby a code is returned back to the app which should then exchange it for an access token.

The third party application can then use this access token to make the calls to the account APIs. When the API is called, the customer information is retrieved from the access token and the account information is then presented to the user.

2.2.2.2 Test case workflow

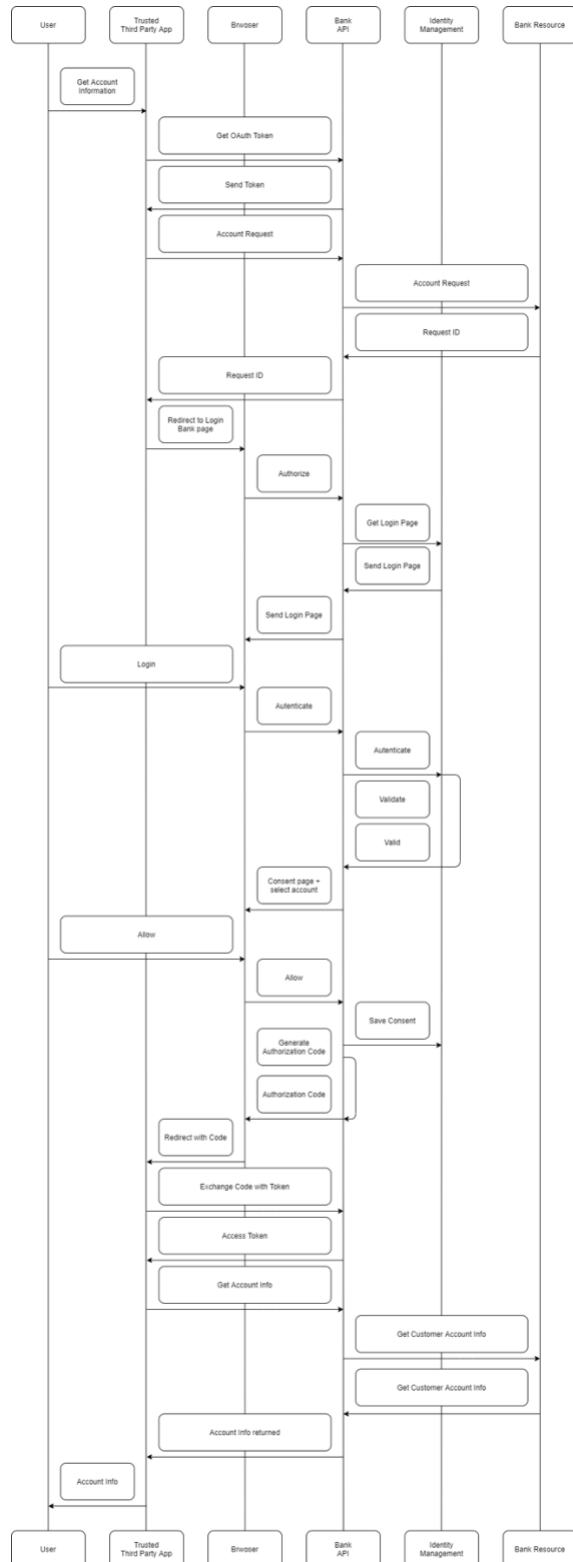


Figure 21: OAuth 2.0 Account Access Flow

2.2.3 Technology Based Analysis

2.2.3.1 Architecture

The following are the main components of the OBA developed in the CyberSec4Europe project.

- The *Identity Provider(ID)* component provides several functionalities as *authentication, service provider, user interface and storage functions*.
- The *API Gateway* component provides several functionalities as *access to function and data, authorization management and operation allowed*.
- The *API Manager* component provides several functionalities as *running support components and running system control*.

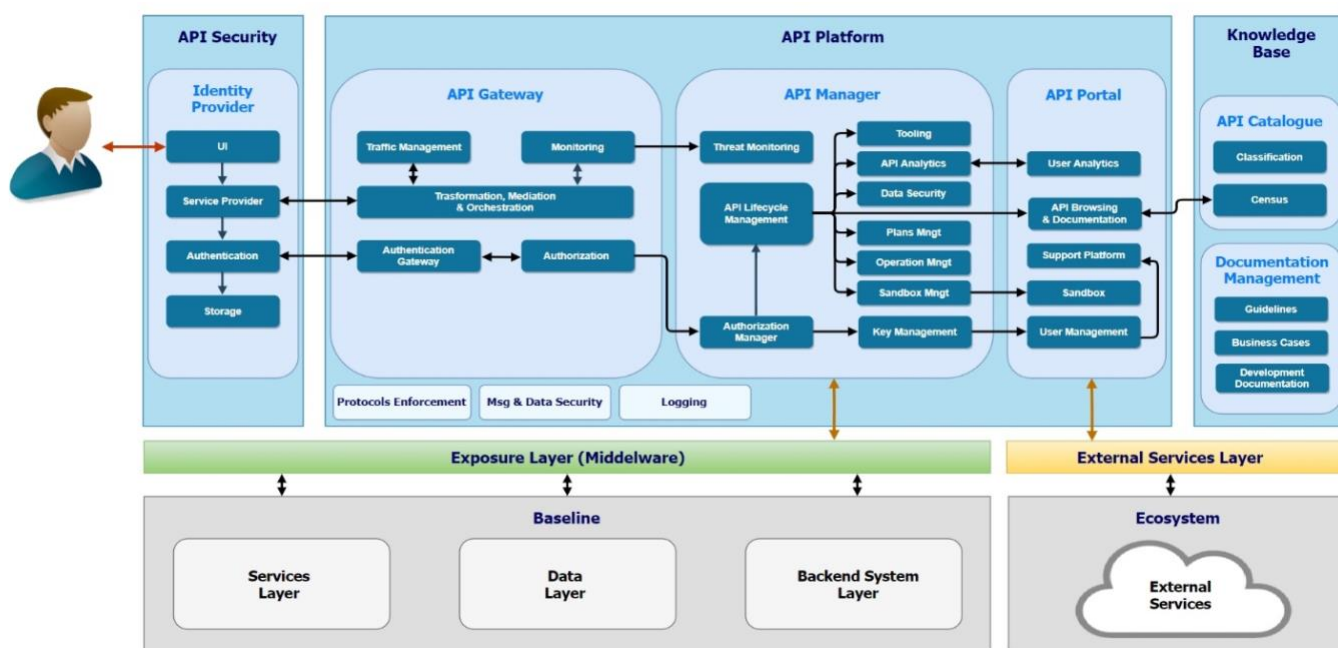


Figure 22: General Open Banking Architecture

2.2.3.1.1 Poste Italiane's OBA

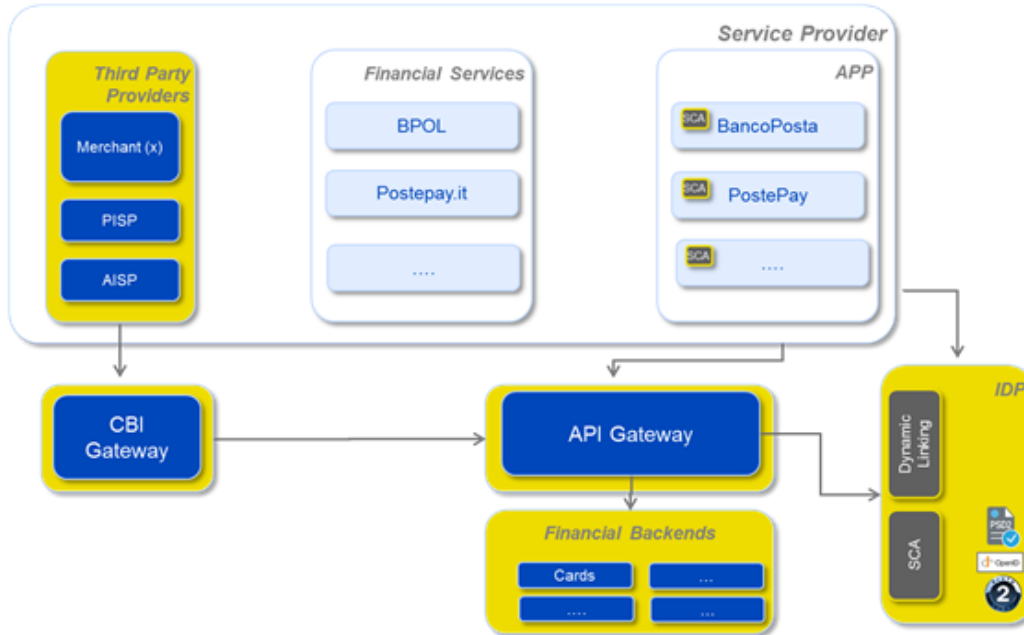


Figure 23: Poste Italiane's Open Banking Architecture

2.2.3.1.2 The architectures in comparison

Poste Italiane's approach to the implementation of the PSD2 Open API was extremely pragmatic and started with the definition of extremely detailed technical and security specifications.

A first substantial difference with respect to the proposed Open Banking API Architecture concerns the abstraction level: while in the CyberSec4Europe OBA architecture a general and conceptual approach is proposed, Poste Italiane implemented a very complex and detailed technical architecture. In this regard, the differences are multiple : as, for example, some of the security requirements implemented in the Poste Italiane architecture:

- *"Tokens must be base 64 encoded, signed and encrypted" ;*
- *"The endpoint of the authorization server must be indicated via the FQDN and must use the HTTPS protocol";*
- *"It is necessary to use SHA-2 as a HASH function in the HMAC signature"*

Concerning the conceptual design of the architecture, a big difference is that, despite Poste Italiane implementing one of the most important technical reference standards (Berlin Group, Open Banking Implementation Entity, etc.), its architectural model is 'non-standard' because it essentially provides an additional stakeholder who plays the role of 'broker' (see figure 23) of services and therefore forms a "front end" to users of the PSD2 Open API.

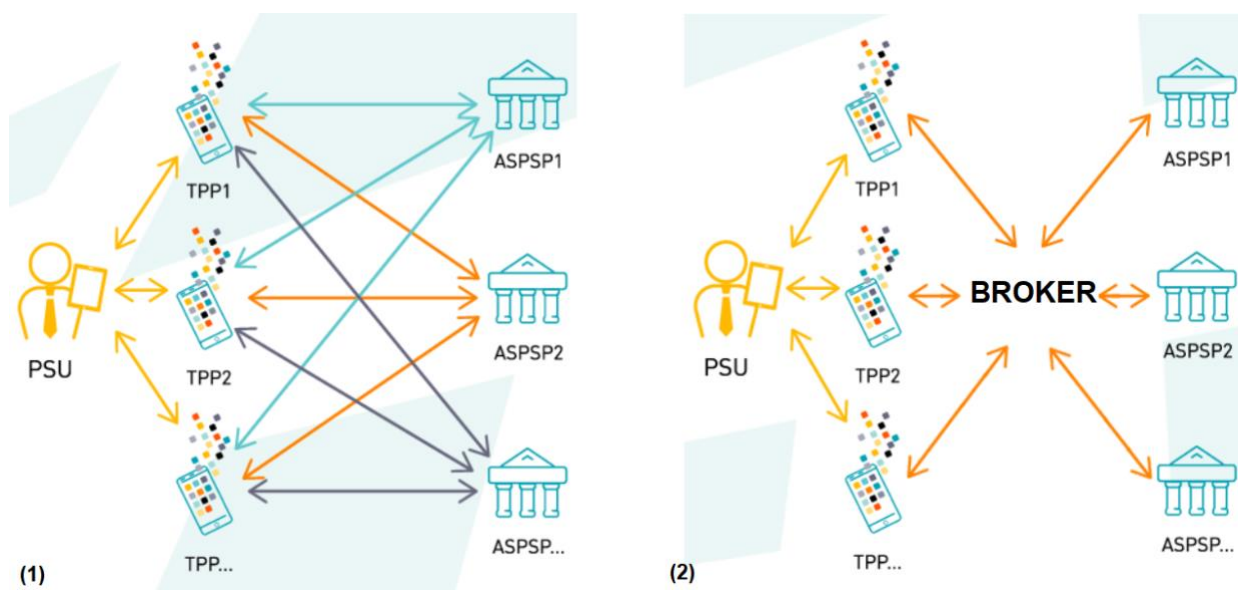


Figure 24: An OBA with and without an intermediary

In fact, this solution is used by various payment institutions that, to be compliant to PSD2, can connect their IT systems to the middleware (also indirectly through their own service providers such as IT providers, technical subjects etc.). The following are some of the reasons for payment institutions to use these services:

- Sharing common services otherwise charged to individual institutes;
- More effective fraud monitoring with provided system data to adherents to the solution;
- Easier to implement additional cooperative APIs and competitive/value-added services;
- Central evolution monitoring / supervision team legislation;
- As a single point of access between TPP and ASPSP;
- Less compliancy costs;
- Highest security standards.

Figure 24 reflects the operative model of the PSD2 Gateway which Poste Italiane joined. It is composed of a front-end API for displaying the services offered by the ASPSPs. In addition, it provides an SDK publishing environment, a preparation API test for centrally-managed developers/TPP. It provides operational monitoring and supports the resolution of any disputes. The API monitoring is centralised and enriched with the periodic publication of reports and KPIs. Finally, a module dedicated to the management of functional APIs and «PSD2 core» is included: for example, the "core PSD2" API provides access for:

- Payment initialisation
- Customer authorisation
- Accounts list
- Account balance
- Movements list
- Fund availability

The following are the access and security-related capabilities:

- **TPP handling** (TPP approval and authentication): validation of eIDAS certificates and authorised TPP verification;
- **Consensus handling** (PSU authentication and consensus): a module dedicated to the management and archiving of user consent and its lifecycle ;
- **SCA management**: orchestration of the SCA application of preliminary SCA exemption checks on transactions made;
- **Fraud management and transaction risk analysis**: system-wide fraud management checks on transactions carried out. Sharing of level enriched information system for internal evaluations to individual ASPSPs;
- **Help desk/Dispute resolution**: module dedicated to the management of eleventh level contacts with ASPSP/TPP. The solution is also equipped with an application for reporting and the management of any disputes

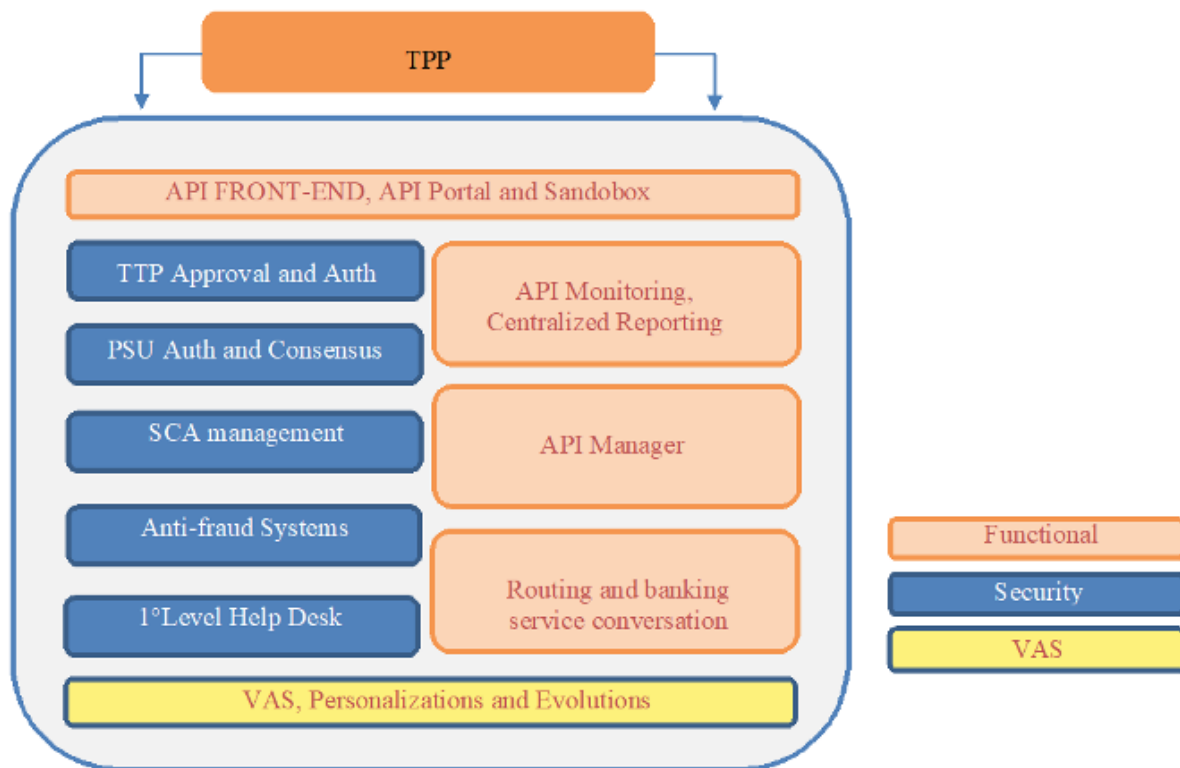


Figure 25: PSD2 Gateway Operative Model

Finally, the solution technically supports the development of value-added services, developed both at a cooperative level (defined collectively by the financial institutions) and competitive (defined by institutions, individually e.g. personal financial management, etc.) with the possibility of using partitions of the solution for exposing services and sandboxes.

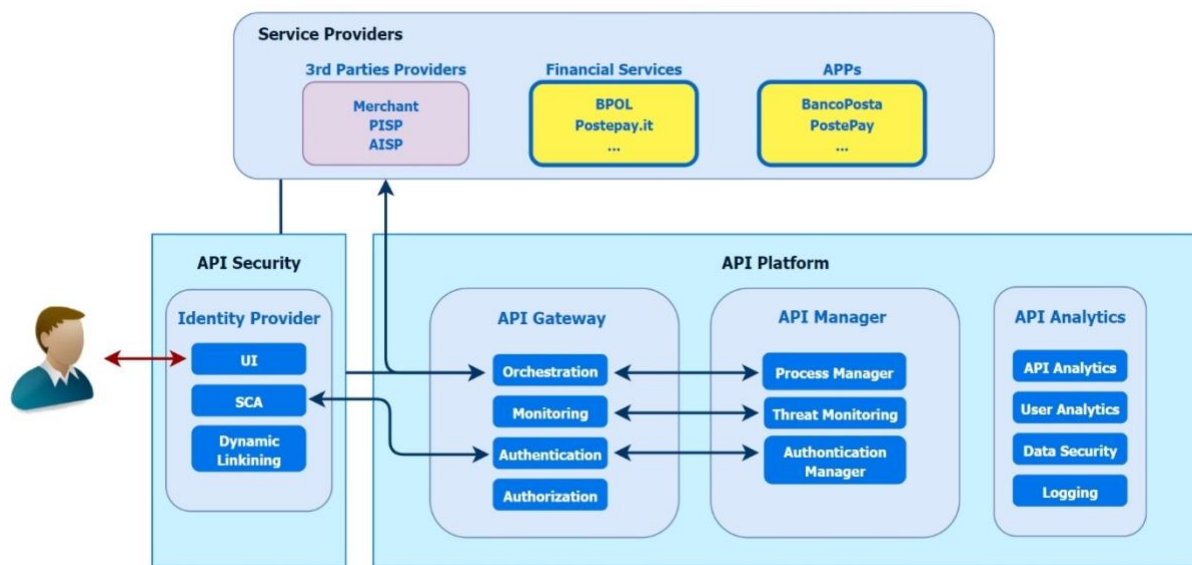


Figure 26: The positioning of Poste Italiane's architecture with respect to the high level OBA

Figure 25 shows a possible positioning of the Poste Italiane architecture with respect to the general Open Banking Architecture designed and developed in the CyberSec4Europe project. Despite the big difference in the analysed architectures, these two different approaches are not incompatible, and in fact can be considered complementary. We suppose they have common requirements, such as preventing an unauthorised user/use to provide controls to ensure that unauthorised users cannot access the system, through the use of, for example, OAuth 2.0.

OAuth 2.0 is the main security standard for delegating authorisation and is widely used in the Open Banking context. OAuth overcomes the potential vulnerability that would enable a user to allow a third party to act on their behalf. In addition, it is used to permit sharing website data with others. Usernames and passwords are not shared but an OAuth access token is issued and used by third parties to access a user's data.

An OAuth 2.0 flow has the following roles:

- **Resource Owner:** Entity that can grant access to a protected resource. Typically, this is the end-user.
- **Resource Server:** Server hosting the protected resources. This is the API you want to access.
- **Client:** Application requesting access to a protected resource on behalf of the Resource Owner.
- **Authorisation Server:** server that authenticates the Resource Owner and issues access tokens after getting proper authorisation.

2.2.4 Requirements Coverage

As the use case was not carried out physically, there was not the opportunity to validate the stated requirements.

2.3 Validation Summary

ID	Validated	Result	Comments
----	-----------	--------	----------

OB-UC01	No		Planned for the second piloting phase
OB-UC02	Yes	Success	
OB-UC03	No		Planned for the second piloting phase
OB-UC04	Partially	Partially	An architectural comparison rather the intended use case scenarios

Table 4: Open Banking demonstrator use case validation summary.

2.4 Lessons Learned and Future Work

2.4.1 OB-UC2 OBSIDIAN

2.4.1.1 Lessons Learned

In this use case, the lessons learned – or rather the obstacles overcome – at an early stage concerned which architectural approaches to adopt and the legal impediments to data sharing, notably in France.

2.4.1.1.1 Alternative Architectural Approaches

Before the adopted OBSIDIAN network architecture was chosen, there were two other approaches that were considered. – one based on MISP and the other on blockchain.

2.4.1.1.1.1 MISP-based

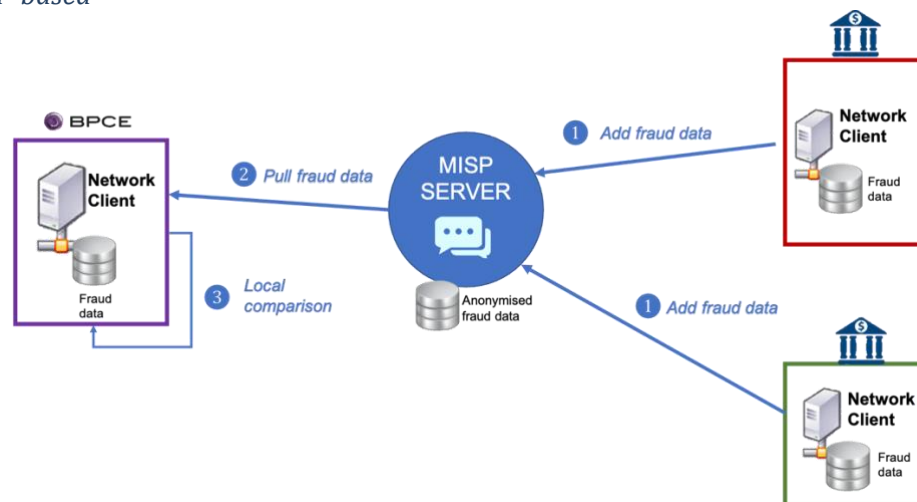


Figure 27: MISP architecture

In this version of the OBSIDIAN architecture, the central server is a MISP (malware information sharing platform) used to exchange IOCs (indicators of compromise) that transmits fraud data either by hashing the IBAN or integrating Cuckoo with the MISP. In figure 26, the transaction process is shown in table 5:

	MISP with hashes	MISP with cuckoo filters
1	Add IBAN hashes	Update cuckoo filter

2	Pull IBAN hashes	Pull all cuckoo filters
3	Query hashes	Query cuckoo filters

Table 4: MISP transaction processes

The MISP-based approach demonstrated some advantages but were outnumbered by the disadvantages. The only experience of using OSINT is at the CERT level (consumption of OSINT and IoC cyber):

- ☐ Aggregation of feeds via MISP
- ☐ No connection to decision-making processes
- ☐ Limited analyst resources

The advantages and disadvantages of the MISP-based approach are listed at table 6:

Advantages	Disadvantages
Used by CERTs	Documentation not user-friendly
Main goal is to share data	Data is handed over (control lost)
	Cannot be used with more advanced protocols without high integration effort

Table 5: MISP pros and cons

2.4.1.1.2 Blockchain-based

A different approach to setting up the OBSIDIAN architecture would be based on distributed ledger technology (DLT), which would be completely decentralised with no central server. Unfortunately, many of the defining characteristics of blockchain make it unsuitable to meet the requirements of the OBSIDIAN network.

The advantages and disadvantages of the blockchain-based approach are listed at table 7:

Advantages	Disadvantages
Decentralised network	High integration cost
Unalterable trust chain	Complex technology – few experts truly understand how it works
	Traceability oriented
	Data deletion difficult (the GDPR right to erasure)
	Hardly fits the projected use case and constraints

Table 6: Blockchain pros and cons

2.4.1.1.2 Legal compliance barriers

Although no sensitive data is stored on the OBSIDIAN server, each of the OBSIDIAN clients, the nodes in the network, are responsible for storing pseudonymised data relating to IBAN suspected of being involved in fraudulent activity and for transmitting that data, encrypted as described above, across the network.

In this decentralized architecture, the central server is trusted to protect the anonymity of each bank. As a result, when a bank sends a request to OBSIDIAN, the banks receiving the request do not know its origin. The same principle applies to the responses. The only entity capable of tracing back which bank sent a

request or response is the central server – but, even then, the central server is not capable of understanding the data transmitted since it is pseudonymised.

Banking secrecy, also referred to as financial privacy, banking discretion, or bank safety, is a conditional agreement between a bank and its clients that all foregoing activities remain secure, confidential, and private. Banking secrecy also refers to confidentiality obligations and disclosure constraints arising under the regulations protecting a country's sovereignty with exceptions often arising in cases when data is to be shared with the country's judicial authorities.

For example, in Austria, under Article 38 of the Austria Banking Act, credit institutions (banks included), **must not divulge or exploit secrets which are revealed or made accessible to them** exclusively on the basis of business relations with customers, or on the basis of Article 75 paragraph 3 (banking secrecy). The obligation to maintain secrecy applies for an indefinite period of time.

In France, banking secrecy entails both criminal and civil penalties. Governed by article L. 511-33 of the French Monetary and Financial Code (FMFC), banking secrecy protects banking clientele from the dissemination of information collected by banks. As banking secrecy is designed to protect clients' privacy, it only concerns confidential information (i.e. only precise information/figures about the situation of a specific client's account), but not general information (e.g. commercial information). Therefore, banking secrecy can be waived either by the client or under legal exemptions.

Needless to say, all banks in France adhere to the GDPR, the primary aim of which is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Although the key information sources in the OBSIDIAN network are IBANs – belonging to potential fraudsters, terrorists or money launderers no less – in France an IBAN is considered to constitute personal data and as such the CNIL[22] initially stipulated that the exchange of IBAN data would require the consent of the owners i.e., the potential fraudsters, terrorists or money launderers.

OBSIDIAN uses several layers of computation to protect the IBAN (hash and encryption), but even then the protected data is not anonymised: according to the Article 29 Data Protection Working Party, hash functions and encryption algorithms are pseudonymisation techniques, and as such, the GDPR is applicable.

However, after repeated interventions to overturn this ruling, the French authorities consider this added security a good practice that would help minimise the data protection risks.

In addition, the decentralised architecture offers a better control over the data shared by each bank. Since there is no entity centralising the fraud data, each bank can add, delete or modify fraud entries they share with the network. This compartmentalisation also helps to minimise data leaks and their impact on individuals' privacy.

Through discussions with other partners, it became clear that the approach taken in each Member State varies to the status of IBAN as personal data varies considerably e.g., in Italy, it is not an issue, whereas the Spanish position is closer to the French. See table 8 for an initial breakdown of banking secrecy approaches across Europe.

Country	Legislated rules
France	Yes, in both criminal and civil law (known as duty of discretion).
Spain	Yes, specifically as stated within law 44/2002

Luxembourg	Yes
Austria	Yes, established in the Austrian Banking Act.
Ireland	Not under statutory law but under common law, there exists a contractual duty of secrecy.
Belgium	Yes, but not from a criminal law point of view.

Table 7: Banking secrecy in Europe

2.4.1.2 What's Missing

In the next phase of the project, we would like to:

- Ascertain the regulatory situation regarding privacy and data protection in the context of sharing fraud data across all Member States, particularly as we intend to extend the scope of the data shared,
- Finalise the work on the OBSIDIAN client and carry out usability tests
- Leverage the initial network experimentation in 2020-21 to fully scale to the European level, connecting French open banking players in a national network, through local connections in the OcSSImore Toulouse-based network and more widely through the French Banking Federation
- Extend in parallel the French network instance to other European open banking players / existing sharing networks

2.4.2 OB-UC4 OBACHT

2.4.2.1 Lessons Learned

Through the comparison performed in this use case, it has been shown that the Open Banking Architecture designed for the CyberSec4Europe project and a real world implementation of Open Banking are complementary. The result of this use case can effectively offer support to financial institutions that have to face the new challenges raised by PSD2 and Open Banking.

The solution adopted by Poste Italiane allows simplified access (through a single point of access) that allows a huge number of banks to be reached and at the same time allows the banks themselves to 'play a new role' in the financial services market.

It is also worth mentioning that the solution adopted by Poste Italiane is based on the more advanced technologies and provided the foremost security standard (such as OAuth 2.0). Such standards and security requirements allow the best practices in terms of procedures for opening the services of banks to the market to be respected and encourage the creation of an ecosystem of payments. It is also reasonable to assume that a security requirement such as OAuth 2.0 to prevent an unauthorised user/use (providing controls to ensure that unauthorised users cannot access the system) is common to the two architectures. Finally, from the assumptions made about the two architectures, it was possible to reconstruct a use case common to the two approaches, that is an account access through the bank APIs.

We have provided an access account implementation model utilisable by banks as they must provide secure access to user data to TTPs. Using the proposed OAuth 2.0 based implementation model, it is possible to meet the three foremost requirements for an Open Banking ecosystem architecture which include methods for:

- **Consent:** to establish whether the granted consent has been released by a user through the authorisation of a TTP to access her data and to authenticate the TTP;
- **Onboarding:** to verify that the TTPs are to be trusted with personal account data;

- **Access model:** to allow access to account data by the TTPs.

Given that Open Banking doesn't define many aspects of the OAuth implementation, banks can use the model as a framework and starting point to develop their architecture and/or evaluate how to integrate the services provided by additional stakeholders (as in the case of Poste Italiane). In addition, TPPs that want to consume a bank's API can analyse the account implementation model to learn how to use the API in their apps. Our implementation model should be a guide to understand authentication and authorisation at a deeper level.

3 Supply Chain Security Assurance

As end-users we want and need to be sure about the quality and origin of the goods we consume, like vegetables and fruits or commercial products like smartphones or cars. Ensuring goods' quality and reliability becomes even more important for a society's critical infrastructure, where complex components such as power generators are produced and integrated by multiple sub-contractors. To realize the described properties, a reliable and secure supply chain is a must. In addition, not only compliance violations must be

prevented, but also when violations occur they must be detected so that the responsible parties can be held liable.

These requirements are addressed by the use cases SCH-UC1 and SCH-UC2 of the demonstrator on Supply Chain Security Assurance. The use cases demonstrate ways to model and validate a supply chain processes efficiently before deploying them; replacing common paper-based audit trails by means of a digitised equivalents; avoiding out-of-band communications and sharing of information with a platform for recording and tracking supply chain information; reducing costs and time needed for handling disputes; and replacing centralised trust models with a distributed trust architecture, where single entities alone will not have the power to manipulate and change any information. SCH-UC1 (Section 3.1) is primarily focusing on dispute resolution, e.g., in the context of retail. SCH-UC2 (Section 3.1) is addressing compliance and accountability in distributed manufacturing scenarios.

3.1 Use Case SCH-UC1 Supply Chain for Retail

This use case models the supply chain for the retail business, with special attention to dispute resolution: a dispute is the result of one or more inconsistencies along the supply chain. Disputes management costs a considerable amount of time and money to all the parties involved. This use case leverages the blockchain capabilities to manage supply chains and to bring considerable time and cost advantages to dispute management.

In this first cycle of the project, we validate a subset of the requirements listed in D5.1 [1]. We focus on those that the fundamental properties of the underlying blockchain platform satisfy by design. The validation strategy is principally based on technology based analysis, that is, we outline in detail the characteristics of the technologies we use and why we think they satisfy the given requirement(s).

Presently, the development of this demonstrator is still ongoing. We cannot validate all its requirements, nor approach target groups because of the prototype's incomplete functionalities. Therefore, in this deliverable we partially validate the use case, with the intention of providing a full validation by M42.

3.1.1 Actors

Developers and solution architects are responsible for the validation process. Developers, which cover the role of testers as well, contributed to the development of the demonstrator, and chose the proper technologies to adapt for its implementation. Solution architects designed the system's architecture, ensuring it would comply to the requirements listed in D5.1.

3.1.2 Test Cases

The validation strategy does not employ technical test cases at this stage of the demonstrator's development.

3.1.3 Technology Based Analysis

Our technology-based analysis focuses on the main technology behind our demonstrator: Hyperledger Fabric [2] (abbreviated HLF in the following). HLF is an open-source permissioned distributed ledger offering a set of functionalities suitable for many industry use cases. Plus the additional security guarantees that blockchains bring to the table.

In what follows, we map HLF's functionalities to our demonstrator's requirements, arguing that they meet them.

3.1.3.1 SCH-UC1-TB1 – Identity Management and Authentication

Fabric handles identity management and authentication with a combination of the traditional Public Key Infrastructure (PKI) and a HLF component called Membership Service Provider (MSP). The different actors in a blockchain network include peers, orderers, client applications, and administrators. Each actor has an

X.509 digital identity certificate.³ These identities determine the permissions over resources and access to information in a blockchain network. The union of an identity and the associated attributes is called principal.

HLF does not allow nodes to join or leave the network as they please (like Bitcoin does, for example, or any of the so called *permissionless* blockchains); rather, every node must have a verifiable digital identity in the form of a X.509 certificate issued by a certificate authority (CA). A certificate is akin to an ID card for that node: it stores a set of attributes that uniquely identify that node – its public key, for example. A certificate authority is a trusted third party that issues digitally signed certificates. Presenting a certificate signed by a CA that everybody trusts gives assurance to the validity of that identity.

X.509 certificates and CAs are paired with MSPs to provide authentication. An MSP verifies a node's certificate to prove its identity and to ensure it has the permission to do whatever action it tried to initiate on the ledger. HLF's documentation [2] explains the relationship between CAs and MSPs with a simple example: a CA is like a credit card provider, that is, it issues a variety of cards holding unique attributes of the card holder (e.g., the cards number, the holder's full name, etc.); an MSP determines which credit card is accepted at a particular store. If the store accepts the credit card owned by the holder, she can buy goods from that store.

Every node in HLF must be a member of an *organization*, the blockchain counterpart of a real-world entity such as a company or a national government. HLF organizations must define their own MSPs to provide authentication. Namely, an organization's MSP lists the identities of its members, and defines which CAs are authorized to issue valid identities for their members. Thus, an MSP links identities to organizations. HLF implements this design by distinguishing two MSP domains in any given network: local MSP and channel MSP. Their function is the same: verify identities and ensure that operations are carried out only by nodes with the right permission. Their scope, however, is different. Local MSPs pertain to individual *nodes*, while channel MSP pertain to individual *channels*.

- A *local MSP* implements authorization for nodes and clients. An example of node level authorization is defining who has the authority to install a smart contract in the node (typically, an organization's admin). As for clients, a local MSP gives them, for example, the ability to authenticate themselves in their transactions.
- A *channel MSP* defines who is an authorized member of a given channel. Members of a channel must authenticate themselves whenever they issue a transaction. The MSP verifies that their identity is in the list of authorized members of the channel. Unlike local MSPs, which are specific to each node, the channel MSP is the same for all channel members, allowing them to authenticate each other. In practice, HLF implements channel MSPs by including the member organizations' MSPs in the channel configuration files.

We argue that HLF's design satisfies the demonstrator's need for authentication and identity management. Organizations wanting to join the network, must replicate their own chain of trust structure in the form of an MSP, listing the identities of its members who are authorized to represent the organization and act on its behalf within the network. To join a channel to interact with other organizations, its MSP must be included in the channel configuration, otherwise all transactions by its members will be rejected. Individuals, must have a valid digital identity, and must be listed as authorized members of their organization. Node operations

³ <https://hyperledger-fabric.readthedocs.io/en/release-1.1/identity/identity.html>

(e.g., installing a smart contract) and transactions are all checked against local and channel MSP to authenticate the identity of the operator.

Action initiated by invalid identities (e.g., invalid X.509 certificate) or by identities not explicitly listed in an MSPs are promptly rejected.

3.1.3.2 SCH-UC1-TB2 – Integrity

HLF authentication and identity management features ensure that only authorized parties have read/write access to the ledger (see Section 3.1.3.1). On top of that, HLF defines default policies and allows members of a network to customize them and add new ones. Policies allow members to come to an agreement on how changes to the network, channels, or smart contracts can happen. For example, they define the rules for adding or removing members from a channel, or specify the number of endorsements required to approve a transaction.

HLF defines policy for data integrity. They are called endorsement policies, and they are defined in relation to a smart contract. Namely, every smart contract has an associated endorsement policy that specifies how many nodes need to execute and validate a transaction in order for the transaction to be considered valid. These so called endorsement nodes are of course authenticated via the mechanisms described the previous section.

The default endorsement policy is a “majority” endorsement: a transaction is valid only if a majority of the nodes execute and validate it. Naturally, members can define new policies better tailored to their use case(s). This may seem somewhat obscure or unrelated to data integrity, but it is indeed very relevant for our discussion: only transactions that are signed by a set of endorsing nodes that satisfy the existing endorsement policy will be “accepted” and lead to a modification of the ledger. That is, if a transaction is *not* signed by sufficient endorsers, it will not result in a change of the ledger.

Endorsement policies are not the only mechanism promoting data integrity. Sending a transaction and executing a smart contract to process that transaction are both operations designed to prevent unwanted or unauthorized changes to the ledger. When invoking a smart contract, the caller provides a set of parameters, called *transaction proposal*, that the smart contract uses when accessing the ledger to evaluate the effects the incoming transaction will have on it. Namely, the smart contract creates two sets of data: the *read set* – the ledger’s state *before* applying the transaction on it – and the *write set* – a projection of the ledger’s state *after* applying the transaction on it. The smart contract puts them in a *transaction response* which it will or will not endorse. At this point the ledger is still not updated, that is, the execution of a smart contract does not directly modify the ledger.

A ledger update happens only after a transaction is validated. This entails two steps: there is a first verification that the transaction has enough signatures (and from authorized nodes) to satisfy the endorsement policy; and a second verification ensuring the ledger’s current state and its state at the time the transaction was signed by the endorsing nodes match (that is, it compares the respective read sets). A transaction is valid if and only if it passes both verifications. Nevertheless, HLF adds *all* transactions to the blockchain’s history – even invalid ones – but only those marked as valid will result in an update to the ledger.

We argue that the policy mechanism and the smart contract execution life cycle guarantee data integrity once stored in the blockchain’s ledger. Only authorized entities (as defined in the endorsement policy) can mark transactions as valid or invalid. The smart contract execution cycle never modifies the ledger; it only marks transactions as valid or invalid. Only valid transactions update the ledger. Furthermore, HLF’s authorization and identity management features allow only identified and authorized entities to create transactions and interact with the blockchain. Finally, transactions stored in the ledger cannot be modified by anyone, a common property of blockchains.

Overall, caused of the described features of HLF, integrity requirements are realized for use case SCH-UC1.

3.1.3.3 SCH-UC1-TB3 – Confidentiality and Access Control

The distributed ledger layer of the demonstrator is realized by Hyperledger Fabric (HLF). HLF represents a private permissioned blockchain which means that the participating nodes / organizations must be granted access to the network. That is, they must be invited or permissioned to join the network. Because of that, the group of organizations that are part of the network is limited and access is restricted to that group, only. Access control lists can be used to provide additional layers of permission through authorization of specific network operations. A specific user ID could be permitted to invoke a chaincode application but blocked from deploying new chaincode.⁴

HLF enables competing business interests, and groups needing private, confidential transactions, to coexist on the same permissioned network. In addition, blockchain offers further possibilities to control access within this group. In particular, HLF offers the concepts of channels and private data collections:

- A channel “is like a virtual blockchain network that sits on top of a physical blockchain network with its own access rules” **Invalid source specified..** That way, a channel represents a segmentation of the group of participants. If selected partners want to exchange confidential information, they can set up a dedicated channel only they can use. A channel is therefore a logical communication pathway between a set of nodes, which must all agree to join the channel and must authenticate themselves and their members by providing their MSP data in the channel configuration files. Additionally each channel has its own, private ledger whose read/write access rights are granted only to the channel’s members. Nodes, in turn, by joining the channel agree to share and manage identical copies of the channel’s ledger. Naturally, a single node can be a member of more than one channel at a time
- Setting up individual channels in networks with lots of partners is difficult to maintain and keep under control. Better scalability in that case is provided by private data collections. Data that shall only be accessible for a smaller group of nodes – restricted via HLF policies - is exchanged in private communications (i.e., via peer-to-peer communication using the *gossip protocol* in HLF). The peers knowing the confidential data, store it off-chain, i.e., in private state databases. Only a hash of the confidential data will be endorsed and made visible in the blockchain. That means, private data gets stored and is updated alongside the ledger while only hashes and references to that data get committed. “The hash serves as evidence of the transaction and is used for state validation and can be used for audit purposes.”⁵ That way, private transactions building upon private data collections can also offer fine-grained access control.

We argue that in the context of SCH-UC1 channels guarantee data confidentiality between entities. As stated above, only channel’s members have access to its ledger, and indeed are the only members of the network aware of its existence. Access to the channel and read/write to its ledger is regulated via the authentication mechanism described in Section 3.1.3.1, and partly in Section 3.1.3.2. One drawback of channels is that they are truly isolated. There is no exchange of information or assets from a channel A to a channel B, not even if a member of both channels wants to transfer some of its assets from A to B. We plan to enhance the

⁴ <https://hyperledger-fabric.readthedocs.io/en/release-1.1/functionalities.html>

⁵ <https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html>

final version of the demonstrator with a mechanism that allows for the transfer of assets from a channel to another.

3.1.3.4 SCH-UC1-TB4 – Fault Tolerance

Fault tolerance is the ability of a system to keep functioning when part of its components break down. Availability is a key requirement in industrial use cases. However, availability is difficult to achieve in a distributed system, because multiple computers have to sync to carry out tasks and agree on the data they have to store. The most effective solution to this problem so far, is to use *consensus* algorithms. Consensus algorithms must be resilient against many threats. Processes, machines, devices, and networks can fail.⁶ Malicious components and man-in-the-middle attacks can send malicious / forged messages.

The architecture of Hyperledger Fabric (HLF) factors out consensus into the orderer service. Thus, it can support different consensus algorithms by substituting the orderer implementation. The orderer determines which transactions to add to the blockchain and in what order. The HLF orderer service should be jointly controlled by the network's members using an algorithm that resists malicious activities by bad actors. There must not be a single organization to control the orderer, because that organization itself may not be trustworthy.

HLF itself provides support for crash-fault tolerance. Crash fault tolerance algorithms allow the system to still reach consensus (i.e., agreement) if components fail or in the presence of an unintended network partition. There is a limit of how many components' failures the system can 'tolerate', which usually is $N/2$, where N is the number of components in the system. In other words, a distributed system using a CFT algorithm can still function if less than half of its component fail ("crash"). Distributing the system's component across different organizations and geographical location will not change this fact.

Unfortunately, CFT algorithms do not guarantee correct system behavior in the presence of malicious actors, that is, they protect against accidental failures, not against actors purposefully trying to break the system/protocol. Byzantine Fault Tolerant (BFT) algorithms can provide this additional protection. Byzantine Fault Tolerance (BFT) is the feature of a distributed network to reach consensus even when some of the nodes in the network fail to respond or respond with incorrect information. The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making (both, correct and faulty nodes) which aims to reduce the impact of faulty nodes. BFT is derived from Byzantine Generals' Problem **Invalid source specified..** Byzantine fault tolerance can be achieved if the correctly working nodes in the network reach an agreement on their values. The authors proved that a consensus can be reached if more than two-thirds of the total number of nodes are honest. The following provides examples if initiatives that plug HLF with a BFT-capable consensus algorithm. For instance,

- PBFT (Practical Byzantine Fault Tolerance) **Invalid source specified..**, based on a MIT paper, has reportedly been used in HyperledgerFabric. It is suitable for private blockchains due to its relatively high performance and finality. However, it offers limited scalability, only. In PBFT, if a node receives enough matching prepare messages and one corresponding commit message, it executes the request. All backup nodes must confirm that everyone received the same sequence number by broadcasting a message in the prepare phase. Subsequent optimizations normally use speculative approaches (like Zyzzyva) or optimistic approaches (like ReBFT).
- MinBFT (or Efficient BFT) was proposed in 2013 **Invalid source specified..** and optimizations were presented, e.g., by authors of **Invalid source specified..** It utilizes a secure hardware environment (Trusted Execution Environment, TEE) to make the protocol more efficient. MinBFT can omit the

⁶ <https://medium.com/kokster/understanding-hyperledger-fabric-byzantine-fault-tolerance-cf106146ef43>

pre-prepare phase due to utilizing the TEE. MinBFT is available as a pluggable software component implemented by NEC Invalid source specified. that allows to achieve Byzantine fault-tolerant consensus with fewer consenting nodes and less communication rounds comparing to the conventional BFT protocol. It implements the MinBFT consensus protocol using Golang, C, and an Intel SGX (Software Guard Extensions) enclave as TEE. SGX guarantees that every node receives the same requests. The MinBFT project is hosted by the Linux Foundation.

- FastBFT is introduced by the authors of **Invalid source specified..** This scheme uses a message aggregation technique that (with an optimistic BFT paradigm) combines hardware-based trusted execution environments (TEE, like Intel SGX) with light-weight secret sharing (no public key operations). After a certain threshold of detected failures is reached, FastBFT uses a combination of MinBFT with a hardware-assisted message aggregation technique as temporary fallback solution. This requires only a subset of replicas to commit and reply. The more expensive polynomial-based secret sharing of MinBFT is replaced by an XOR-based one. Their implementation is also based on Golang and Intel SGX.

We argue that HLF's consensus algorithm satisfies the fault tolerance requirement for our demonstrator. However, we believe we can improve it further in the next iteration of the project. Our plan is to shift to a BFT algorithm for the final version of our demonstrator.

3.1.3.5 SCH-UC1-TB5 – Performance

Concerning the architecture used for the supply chain use case, the layer which is seen most critical concerning performance is the distributed ledger layer which is used to store activities with the workflow in an immutable way. Interactions with the distributed ledger layer are controlled via smart contracts which are querying states in the ledger or append new entries to it.

As distributed ledger technology we are using Hyperledger Fabric (HLF) v2.1.0. Concerning HLF, Hyperledger Caliper⁷ is a well-known tool for creating blockchain benchmarks. The tests evaluate the performance with regard to varying the complexity of smart contracts and their interaction with the blockchain. Because of the nature of blockchain as a distributed ledger, the performance of write operations (submitting changes to the blockchain by transactions) differs significantly for read operations (evaluating the blockchain's status) that offer significantly higher numbers of transactions per second (TPS). Furthermore, test results also heavily depend on the overall deployment schema. In particular, network latency has a significant impact on the overall performance. The test results published online⁸ are hence based on datacentre-like infrastructure with deployments of peers and orderers on a single node. The tests vary regarding complexity of the blockchain operations and batch sizes. Best case scenarios for read operations on the given environment were >1400 TPS. Likewise, best case scenarios for write operations were >600 TPS. As stated in 3.2.3.8, HLF by default provides support for crash fault-tolerant protocols. The authors of **Invalid source specified.** showed that also Byzantine fault-tolerant protocols could be used and introduce FastBFT as an alternative, showing that their protocol in comparison to alternatives like MinBFT, CheapBFT or Zyzzyva provide significantly higher TPS and lower latency rates. The RAFT white paper [3] shows that a modest network of 3 servers and 100 client threads is capable of handling about 19000 writes per second. HLF's team has published a performance study [4] showing that RAFT brings less latency and more transactions per second than before – about 2000 in their tests. HLF's number is lower than pure RAFT

⁷ <https://www.hyperledger.org/use/caliper>

⁸ <https://hyperledger.github.io/caliper-benchmarks/fabric/performance/2.1.0/nodeContract/nodeSDK/configuration/>

because it has to go through the smart contract and transaction life cycles explained in the previous section in order to process a transaction.

We argue that these performance results satisfy the requirements of our demonstrator. In the next cycle, we plan to improve it by shifting to a BFT algorithm that has proven to produce even higher throughput [5], further improving our demonstrator’s performance.

3.1.3.6 SCH-UC1-TB6 – Logging and System Monitoring

HLF provides complete and comprehensive logging functionalities, allowing for a close monitoring of its operations. Moreover, HLF stores *all* transactions to the blockchain’s history – even those marked as invalid – a useful feature supporting transparency, auditing, and accountability procedures.

3.1.4 Quality Indicators

The validation strategy does not employ target group questionnaires to assess the fulfilment relevant quality indicators at this stage of the demonstrator’s development.

3.1.5 Requirements Coverage

Table 8 below provides an overview of the validation of requirements for demonstrator SCH-UC2 Supply Chain for Retail.

ID	Validated	Strategy	Result	Mandatory	Comments
SCH-SP01	Yes	Test Case SCH-UC1-TB1	Success	Yes	Please N/A
SCH-SP02	Yes	Technology based SCH-UC1-TB1	Success	Yes	N/A
SCH-SP03	Yes	Technology based SCH-UC1-TB2	Success	Yes	N/A
SCH-SP04	No	Test Case		Yes	Requirement will be addressed in next iteration via test cases.
SCH-SP05	Yes	Technology based SCH-UC1-TB3	Success	Yes	N/A
SCH-SP06	Yes	Technology based SCH-UC1-TB3	Success	Yes	N/A
SCH-SP07	No			Yes	Requirement will be addressed in next iteration.
SCH-SP08	No			No	N/A

ID	Validated	Strategy	Result	Mandatory	Comments
SCH-LF01	No	Test Case		Yes	Requirement will be addressed in next iteration via test cases.
SCH-U01	No	Test Case		Yes	Requirement will be addressed in next iteration via test cases.
SCH-U02	No	Test Case		Yes	Requirement will be addressed in next iteration via test cases.
SCH-OP01	Yes	Technology based SCH-UC1-TB5	Success	Yes	N/A
SCH-OP02	Yes	Technology based SCH-UC1-TB4	Success	Yes	N/A
SCH-OP03	No	Test Case		Yes	Requirement will be addressed in next iteration via test cases.
SCH-OP04	Yes	Technology Based SCH-UC1-TB6	Success	Yes	N/A
SCH-MP01	No	Test Case		No	Requirement will be addressed in next iteration via test cases.
SCH-LR01	No			Yes	Requirement will be addressed in next iteration.
SCH-LR02	Yes	Technology based SCH-UC1-TB1	Success	Yes	Actors (human users and/or automated processes) need to have unique identifiers (e.g., unique IDs, RFIDs, certificates) in an unforgeable way.
SCH-LR03	Yes	Technology based SCH-UC1-TB1	Success	Yes	HLF's authentication mechanisms and data integrity functionalities make it hard for a

ID	Validated	Strategy	Result	Mandatory	Comments
		and SCH-UC1-TB2			malicious actor to commit fraud.

Table 8: Supply Chain Security Assurance - SCH-UC1 Requirement Coverage

3.2 Use Case SCH-UC2 Compliance and Accountability in distributed Manufacturing

SCH-UC2 introduces a supply chain use case for industrial products which specifically focuses on compliance assurance and accountability in distributed manufacturing. For this use case a demonstrator has been developed as described in D5.2, section 3.2.2. The demonstrator illustrates the interactions of different actors like EPC (engineering, procurement and construction), suppliers and notification bodies for constructing an electric sub-station or powerplant. As this scenario represents a quite complex workflow, the demonstrator concentrates on an exemplary section which can be used to illustrate different lines of interaction and later also conflict situations.

An end user application referred to as the workflow execution application e.g., used to manage the execution of a power plant construction, will offer a graphical user interface (GUI) that allows users to easily upload documents, check states and perform approvals. The workflow application for SCH-UC2 was developed with the aim of demonstrating the functionality and interaction of the technology used. Therefore, the demonstrator provides a user interface that illustrates the interaction and states of the architectural layers, i.e., the business logic layer and distributed ledger layer as illustrated in Figure 33 on page 51 of D5.2. The demonstrator's user interface is thus not intended to represent a realistic interface for end users but is specifically highlighting the technology behind, like views on the workflow and on the states of the execution. For instance, Figure 28 represents a screenshot of the developed wf-gui application, showing that different workflows (after successful logon took place) can be managed or executed. Figure 29 provides an overview of the transitions and tokens per state. It thus represents the current workflow state, showing which transaction (i.e., step in the business process) can be executed, next. Figure 30 provides a visualization of the Petri Nets.

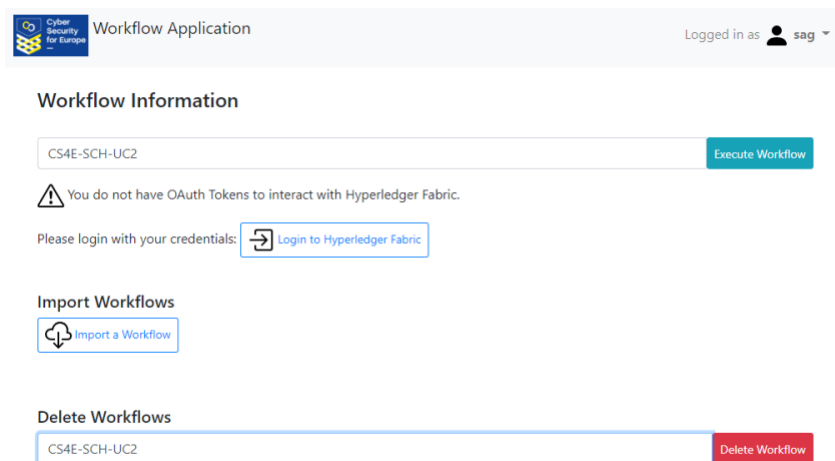
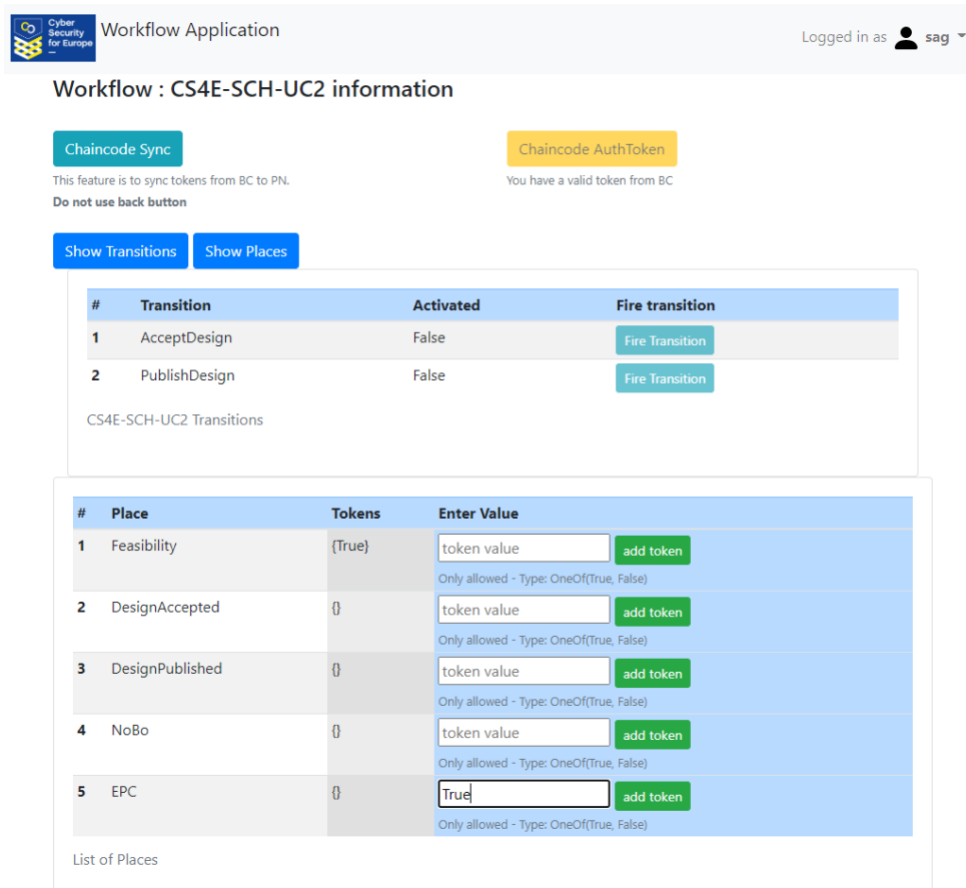


Figure 28: Workflow management features

Workflow management features such as importing, executing, and deleting workflows can be performed by authorized user for example, user: “sag” is authorized to execute CS4E-SCH-UC2 .



The screenshot displays the 'Workflow Application' interface. At the top, it shows the Cyber Security for Europe logo and the user 'sag' is logged in. The main heading is 'Workflow : CS4E-SCH-UC2 information'. Below this, there are two buttons: 'Chaincode Sync' (blue) and 'Chaincode AuthToken' (yellow). The 'Chaincode Sync' button has a note: 'This feature is to sync tokens from BC to PN. Do not use back button'. The 'Chaincode AuthToken' button has a note: 'You have a valid token from BC'. Below these buttons are two more buttons: 'Show Transitions' and 'Show Places'. The 'Show Transitions' button is active, displaying a table of transitions.

#	Transition	Activated	Fire transition
1	AcceptDesign	False	<button>Fire Transition</button>
2	PublishDesign	False	<button>Fire Transition</button>

CS4E-SCH-UC2 Transitions

The 'Show Places' button is also visible, displaying a table of places.

#	Place	Tokens	Enter Value
1	Feasibility	{True}	token value <button>add token</button> Only allowed - Type: OneOf(True, False)
2	DesignAccepted	{}	token value <button>add token</button> Only allowed - Type: OneOf(True, False)
3	DesignPublished	{}	token value <button>add token</button> Only allowed - Type: OneOf(True, False)
4	NoBo	{}	token value <button>add token</button> Only allowed - Type: OneOf(True, False)
5	EPC	{}	True <button>add token</button> Only allowed - Type: OneOf(True, False)

List of Places

Figure 29: An excerpt of SCH-UC2 plant construction compliance approval

In Figure 29 an excerpt of SCH-UC2 plant construction compliance approval is modelled as a Petri Net workflow. The workflow participants interact with the workflow by inserting tokens in appropriate & authorized places e.g., user ‘sag’ approves the feasibility design information by inserting token ‘True’ in place ‘EPC’.

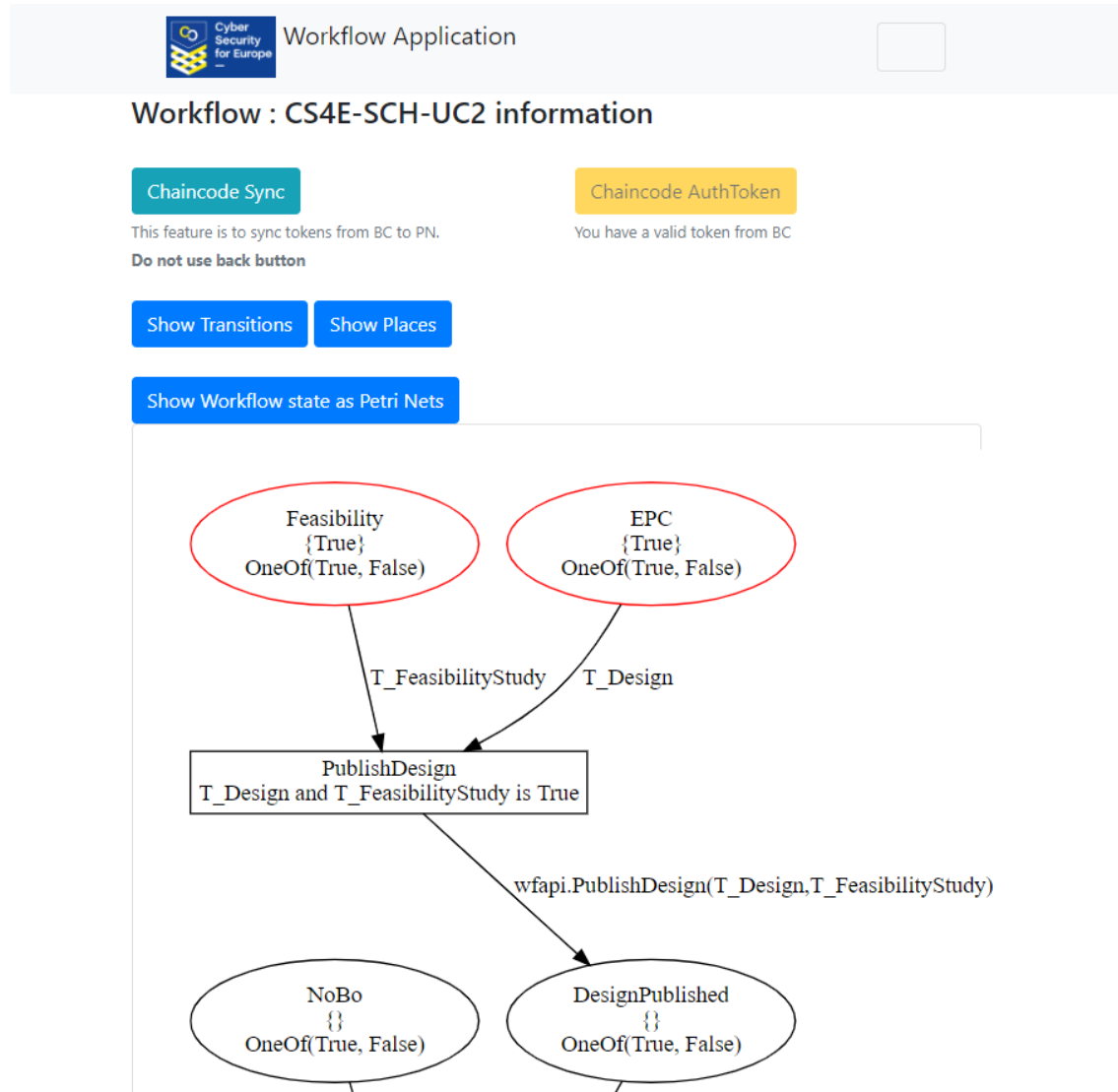


Figure 30: SCH-UC2 use case workflow

In Figure 30, SCH-UC2 use case workflow's current state can be viewed via Petri Nets workflow, the red-highlighted places show that they have valid tokens.

The following provides a summary of the validation of SCH-UC2's requirements that are introduced in section 3 of D5.1.

The scope of the evaluation is on the validation of the functional and non-functional requirements of the demonstrator's architecture and its implementation. For the validation we will mainly use a two-fold validation strategy:

On the one side we will present test case implementations showing features and qualities of the demonstrator. For instance, requirements like the consistent logging and protection of data in transit and at rest will be proven via test cases that are presented in section 3.2.2.

On the other side certain architectural qualities will be validated through technology-based analysis. As the architecture of our demonstrator is based on a distributed ledger layer, we will validate requirements like

accountability and non-repudiation by referring to the key qualities of a distributed ledger technology like blockchain. Those validations will be presented in section 3.2.3.

At the time of writing this report, the development of the demonstrator for SCH-UC2 is still in progress. Therefore, some requirements are only partially addressed and will be completed until M42. The validation is performed on the demonstrator version as-of December 2020.

3.2.1 Actors

The validation of the identified requirements for SCH-UC2 is conducted by architects, developers and testers who were contributing to the development of the demonstrator.

Technical test cases are defined by security architects together with testers and implemented and evaluated by testers. In concrete, testers are using the PyUnit framework for implementing blackbox and whitebox unit test cases. Concerning user interface related tests, they are making use of the Selenium⁹ framework for automated web application tests. Finally, some use cases require a combination of automated tests and manual checks, like the proof of encrypted communication, which is performed by intercepting the network traffic of automated test suites and analysing them retrospectively in expert tools like Wireshark.

Concerning technology-based analysis, software architects and security architects focus on the evaluation of the demonstrator's qualities by evaluating the technology stack and the qualities of integrated sub-components. For instance, aspects like accountability and non-repudiation will be inferred from features and qualities provided by the distributed ledger technology, i.e., in our case Hyperledger Fabric (HLF).

3.2.2 Test Cases

3.2.2.1 SCH-UC2-TC1 Authentication

PyUnit tests integrated with Selenium (Chrome based web browser testing framework) are used to validate different valid and invalid username/password combinations. Furthermore, SQL injection attacks are performed via automated PyUnit tests, as well.

3.2.2.1.1 Description

The test case validates that only an authenticated user can login successfully to the developed workflow application. This test cases do not validate complete end-to-end authentication to HLF smart contracts. The integration of credentials between the workflow application and the HLF's certificate authority (CA) is managed via a middleware. In the next development phase, we will extend this test case as a complete integration test including the workflow application, middleware, and the HLF CA issued user certificates.

3.2.2.1.2 Test Case Workflow

Precondition:

1. Using a supported browser (e.g., Chrome)
2. Use of configured credentials provided via a config file

Test Steps:

1. Navigate to login page URL

⁹ <https://www.selenium.dev/>

2. Input credentials and click login
 - a. If successful login, then open dropdown menu and click logout
 - b. If login fails, then it create a failure report

3.2.2.1.3 Test Results

Only authorized users were able to login and logout, and it is successfully demonstrated by the test results shown in Figure 31.

Test Results	
Start Time: 2020-12-08 14:10:41	
Duration: 25.752s	
Status: Pass: 7	
Test Title	Status
SCH-UC2-TC1 Authentication 01 - Sanity check - Workflow login URL is reachable	Pass
SCH-UC2-TC1 Authentication 02 - A workflow participant client user can log in successfully	Pass
SCH-UC2-TC1 Authentication 03 - A workflow resource admin user can log in successfully	Pass
SCH-UC2-TC1 Authentication 04 - An admin user can log in successfully	Pass
SCH-UC2-TC1 Authentication 05 - Unknown username/password login fails	Pass
SCH-UC2-TC1 Authentication 06 - SQL injection with known username('admin') and password(' OR ""=""') fails	Pass
SCH-UC2-TC1 Authentication 07 - SQL injection on username/password with (' OR ""=""') fails	Pass
Total Tests Executed: 7	Pass: 7

Figure 31: Test results of SCH-UC2-TC1 Authentication

3.2.2.2 SCH-UC2-TC2 Encryption

This test case is validating that any communication between the client (e.g., a user's browser) and the workflow application (wf-gui) is encrypted using TLS. Also, communication between the workflow layer and the underlying Hyperledger Fabric architecture is encrypted via TLS.¹⁰

3.2.2.2.1 Description

The test case intercepts (i.e., wiretaps) communication between the client and the workflow application and evaluates the network traffic via the tool Wireshark. The interaction between client and backend can be automated using other test case procedures that follow a predefined interaction sequence (e.g., see SCH-UC2-TC3, below).

3.2.2.2.2 Test Case Workflow

The evaluation in Wireshark is done manually.

3.2.2.2.3 Test Results

The figures below illustrate results from a test run. Figure 32 shows a DNS request to the workflow application (wf-gui) and Figure 33 illustrates TLS-encrypted communication that has been recorded and analysed by Wireshark.

¹⁰ https://hlf.readthedocs.io/en/latest/enable_tls.html

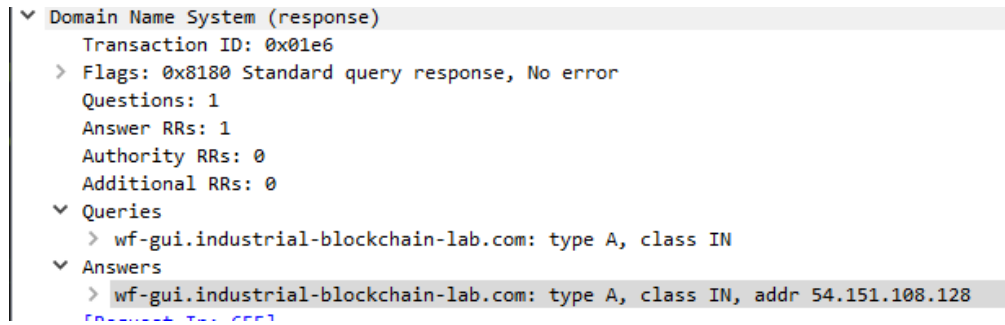


Figure 32: DNS query

Figure 32 illustrates the DNS query to wf-gui.industrial-blockchain-lab.com returns the IP 54.151.108.128

1284	144.561...	192.168.0.240	54.151.108.128	TLSv1.2	623 Client Hello
1290	144.733...	54.151.108.128	192.168.0.240	TCP	60 443 → 5832 [ACK] Seq=1 Ack=570 Win=62208 Len=0
1291	144.733...	54.151.108.128	192.168.0.240	TLSv1.2	202 Server Hello, Change Cipher Spec, Encrypted Handshake Message
1292	144.735...	192.168.0.240	54.151.108.128	TLSv1.2	97 Change Cipher Spec, Encrypted Handshake Message
1296	144.905...	54.151.108.128	192.168.0.240	TCP	60 443 → 5832 [ACK] Seq=149 Ack=613 Win=62208 Len=0
1601	189.904...	192.168.0.240	54.151.108.128	TCP	55 [TCP Keep-Alive] 5832 → 443 [ACK] Seq=612 Ack=149 Win=262400 Len=1
1604	190.072...	54.151.108.128	192.168.0.240	TCP	66 [TCP Keep-Alive ACK] 443 → 5832 [ACK] Seq=149 Ack=613 Win=62208 Len=0 ...
1658	204.773...	54.151.108.128	192.168.0.240	TLSv1.2	77 Encrypted Alert

Figure 33: Wireshark packet capture

In Figure 33 Wireshark packet capture shows the TLS exchange between the host IP (192.168.0.240) with wf-gui application IP (54.151.108.128)

Figure 34 illustrates that encrypted communication can also be verified from an end user's view, i.e., via the browser.

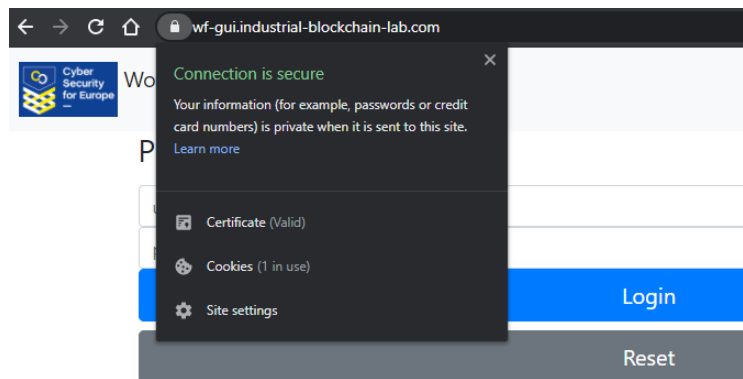


Figure 34: Opening the wf-gui application.

Figure 34 shows the opening the wf-gui application via Google Chrome indicates that the connection to the website is secure.

3.2.2.3 SCH-UC2-TC3 User Interface

This test case is validating the user interaction via the graphical user interface (GUI) provided by the workflow application. This test suite will perform a series of tests against the workflow GUI.

3.2.2.3.1 Description

That is, different paths in the user interface will be evaluated and end-to-end tests will be performed to showcase the correctness of application features. The test suite is automated using Selenium¹¹.

3.2.2.3.2 Test Case Workflow

The following provides an overview of the different scenarios that are evaluated via automate tests. For the sake of brevity, details on the user flows are omitted:

Test Steps:

1. An authenticated user logs into the workflow application successfully
2. The user imports a new workflow
3. The user selects the newly imported workflow and executes one or more workflow steps/actions
4. The user completes executing the workflow successfully
5. The user is able to delete the workflow

3.2.2.3.3 Test Results

The test results show that a user's browser actions are successfully simulated automatically via Selenium framework as shown in Figure 35.

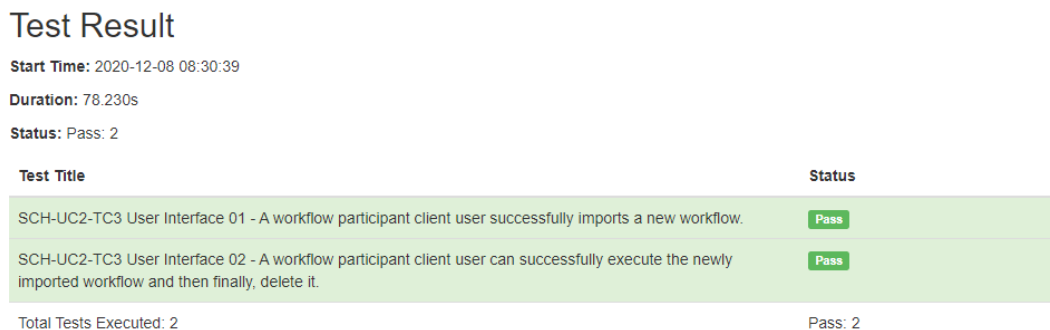


Figure 35: User interface tests

Figure 35 illustrates how user interface tests are successfully automated via Selenium framework

3.2.2.4 SCH-UC2-TC4 Scalability

This test case is not mandatory to be implemented for this particular use case. However, tools like Docker and Kubernetes can be used to achieve scalability for the developed applications.

3.2.2.5 SCH-UC2-TC5 Logging

This test case is validating the logging functionality of developed application.

¹¹ <https://www.selenium.dev/>

3.2.2.5.1 Description

Logging functionality is implemented in the developed application which can be then connected to an external Security Incident and Event Management (SIEM) system for further continuous monitoring and analysis. In this development cycle we focus on log collection on local instances i.e., a log file is generated by the workflow application and an analysis is planned for next cycle of demonstrator development.

3.2.2.5.2 Test Case Workflow

A configuration file is used to specify logging level for the application.

3.2.3 Technology Based Analysis

3.2.3.1 SCH-UC2-TB1 Identity Management and Authentication

Hyperledger Fabric (HLF) represents a private permissioned blockchain. The principles of identity management and authentication provided by HLF are described in Section 3.1.3.1. Those features are applied both, for SCH-UC1 as well as SCH-UC2. For the current implementation of SCH-UC2 we are applying a test instance of a PKI with HLF.

3.2.3.2 SCH-UC2-TB2 Integrity

As discussed in Section 3.1.3.2, using blockchains and committing every action to the blockchain using the agreed-upon consensus mechanism effectively ensures data integrity. Moreover, user access control (via identity certificates) which takes place by executing methods of smart contracts ensures the integrity of transactions in HLF. Prior to commitment, the peers will employ the system chaincodes to ensure that sufficient endorsements are present and derived from the appropriate entities. A versioning check ensures consent on the current state of the ledger, before any blocks containing transactions are appended to the ledger (protection against e.g., double spending, that might compromise data integrity).

This way, by consistently using the blockchain to authorize, consent on and document every action, integrity is ensured effectively for SCH-UC2.

3.2.3.3 SCH-UC2-TB3 Confidentiality and Access Control

Section 3.1.3.3 introduces the concepts of channels and private data collections of HLF. We argue that in particular the usage of channels is well suited to implement confidentiality and access control for distributed supply chains: Concerning SCH-UC2, EPC (the purchaser) has contractual relationships with different suppliers S0 and S1. As price conditions negotiated between EPC and S0 should not be shared with S1 (and vice versa), EPC can set up different channels with S0 and S1. That way, the confidential price information is accessible only to the authorized parties.

3.2.3.4 SCH-UC2-TB4 Anonymization

Though anonymization is not applied for the given use case demonstrator, the applied technology offers several approaches for preserving the privacy of users, also supporting anonymization schemes. The authors of **Invalid source specified**. provide an overview of cryptographic techniques in that context like zero knowledge proofs (ZKP), homomorphic hiding or group and ring signatures. For example, the cryptographic protocol Idemix can be used together with HLF in order for users to hide their identity by applying ZKP

technologies.¹² The secret in this context is the user's/client's identity, whereby an identity consists of a set of attributes like name, age, gender etc. In the blockchain network, other peers need to be able to verify that the creator of a transaction is a valid member of an organization or that he or she has specific attributes that allow him/her to create the transaction – which represents a selective disclosure of attributes, only.

3.2.3.5 SCH-UC2-TB5 Non-repudiation

Non-repudiation is about ensuring that an action or a statement made by one of the actors in a distributed supply chain use case cannot dispute their actions committed earlier. This is relevant, as in distributed supply chain scenarios, such actions and statements are evaluated in the context of contracts between the entities. Non-repudiation is ensured by SCH-UC2 via the workflow engine that ensures that any user activity is tracked in the underlying blockchain layer with a digital signature that is created using the user's identifying credentials. This feature depends on and is assured by the PKI approach used for managing user credentials (cf. SCH-UC2-TB1 Identity Management) – assuming that user credentials are managed following security/PKI best practices, i.e., making sure that private keys of users are not getting released or stolen. Likewise important is the fact that audit log entries are stored in an unforgeable way in the blockchain, i.e., that integrity of the audit log is ensured as stated in SCH-UC2-TB2 Integrity. Unforgeable audit log entries per user activity is, hence, ensuring non-repudiation for SCH-UC2.

3.2.3.6 SCH-UC2-TB6 Accountability

Accountability in the context of supply chain security is about being able to identify the originator of any action and being able to provide proof that he/she did or did not behave according to the agreed upon contractual clauses. In the context of SCH-UC2 we have the Petri Nets workflow implementation of the supply chain process that is ensuring that actions are executed in compliance with the defined workflow. Any action taken is recorded via the workflow and smart contracts layer in the underlying blockchain. Every activity is stored in such a way that it can be traced back to the user as mentioned in SCH-UC2-TB5 Non-repudiation. Because of the blockchain layer – in the case of SCH-UC2 implemented based on Hyperledger Fabric – a distributed and reliable audit log is given. That provides the basis for subsequent auditing and conflict resolution processes to solve disputes amongst supply chain partners. This aspect is illustrated in more details by SCH-UC2.

3.2.3.7 SCH-UC2-TB7 Performance

Performance capabilities and optimization strategies are discussed for SCH-UC1 in Section 3.1.3.5. The references given show that in data centre environments, throughput rates up to thousands of transactions per second (as requested by SH-OP01) can be achieved. Though we don't see this demand to arise immediately for the demonstrator SCH-UC2, further optimization options by means of scaling up of hardware and network configurations are possible here as well.

3.2.3.8 SCH-UC2-TB8 Fault Tolerance

Related work on consensus algorithms supporting crash fault tolerance or Byzantine fault tolerance is presented in Section 3.1.3.4.

For the current setup of the SCH-UC2 demonstrator, we use HLF's crash-fault tolerant approach to address requirement SCH-OP02. As described above, BFT can and will also be applied, if needed.

¹² <https://hyperledger-fabric.readthedocs.io/en/release-2.2/idemix.html>

3.2.4 Quality Indicators

3.2.4.1 Effectiveness and efficiency of the solution

3.2.4.1.1 Integration and interoperability

- Exposure of APIs as JSON-based REST/RPC: the workflow application's (called wf-gui) supports JSON-based REST APIs. By that it can easily be integrated into other distributed systems.

3.2.4.1.2 Documentation

- Installation, configuration, and integration documentation in README: SCH-UC2's application (wf-gui) provides a comprehensive documentation (in form of README files) which provide instructions that describe how to install required software packages and configure the configuration file.
- Additional documentation (examples, tutorials, etc.): a set of workflow examples and additional tutorial documentations are provided as part of the documentation package.

3.2.4.1.3 Usability

- Minimal browser support: our user interface has been tested regarding compatibility with most widely used browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge.
- Multi-platform support and responsiveness: the user interface of SCH-UC02 is browser-based and hence works smoothly with respect to different platforms. Such as standard computer operating systems, mobile platforms such as Android or IOS, and tablets. Also visualization is highly customizable, e.g., regarding different screen sizes.

3.2.4.1.4 Source code management and automated CI testing

- Use of SCM: the SCH-UC02 application (wf-app) is developed and managed via an open source installation of git and an SCM system that provides issue tracking, and automated CI testing for creating documentation and validating test cases.

3.2.4.1.5 Deployment

- Docker containers provided: Dockerized deployments are supported, that is wf-app can be deployed as a Dockerized application and corresponding Docker files for deploying the application are available.

3.2.5 Requirements Coverage

Table 9 below provides an overview of the validation of requirements for demonstrator SCH-UC2 Compliance and Accountability in distributed Manufacturing.

ID	Validated	Strategy	Result	Mandatory	Comments
SCH-SP01	Partially	Test Case SCH-UC2-TC1	Success	Yes	<i>Authentication:</i> Requirement addresses user authentication of the platform. Test case is

ID	Validated	Strategy	Result	Mandatory	Comments
					successfully validated via SCH-UC2-TC1.
SCH-SP02	Yes	Technology based SCH-UC2-TB1	Success	Yes	<i>Identity Management:</i> For the demonstrator the requirement is verified using a self-managed PKI; in a productive environment that one would be replaced by a managed/corporate PKI.
SCH-SP03	Yes	Technology based SCH-UC2-TB2	Success	Yes	<i>Integrity:</i> All transactions stored in the blockchain are getting signed by users' private credentials in an immutable way.
SCH-SP04	Yes	Test Case SCH-UC2-TC2	Success	Yes	<i>Encryption:</i> Data in transit is protected across all layers of the architecture (i.e., between user and UI/middleware and underlying distributed ledger).
SCH-SP05	Partially	Technology based SCH-UC2-TB3	Success	Yes	<i>Confidentiality:</i> The used distributed ledger technology (based on Hyperledger Fabric) provides appropriate means for managing access to confidential information. With the ongoing development of SCH-UC2 these features will be applied.
SCH-SP06	Partially	Technology based SCH-UC2-TB3	Success	Yes	<i>Access Control:</i> The employed distributed ledger technology and the workflow framework supports access control

ID	Validated	Strategy	Result	Mandatory	Comments
					on confidential information. This will be further evaluated and used in the next iteration of improving and extending the demonstrator.
SCH-SP07	Partially	Technology based SCH-UC2-TB4	Success	Yes	<i>Anonymization:</i> In SCH-UC2 all actors need to know each other, and anonymization is not needed for the current use case but will be revisited in upcoming iterations.
SCH-SP08	No	Technology based SCH-UC2-TB4		No	<i>Privacy:</i> Not mandatory requirement for SCH-UC2.
SCH-SP09	Yes	Technology based SCH-UC2-TB5	Success	Yes	<i>Non-repudiation:</i> Similar as for Technology based SCH-UC2-TB2 we are using self-managed PKI for the non-productive demonstrator.
SCH-SP10	Partially	Technology based SCH-UC2-TB6	Success	Yes	<i>Accountability:</i> Information is stored in the distributed ledger. In this revision, this requirement is addressed via technical review but will be extended via a test case exporting logs in the next revision.
SCH-LF01	Yes	Test Case SCH-UC2-TC3	Success	Yes	<i>UI:</i> The user interface functionality is tested using a framework for

ID	Validated	Strategy	Result	Mandatory	Comments
					automated UI-tests (Selenium).
SCH-U01	No	Test Case		Yes	<i>Notification of incidents:</i> Requirement will be addressed in next iteration via test cases.
SCH-U02	No			No	<i>Configuration:</i> Not mandatory requirement for SCH-UC2.
SCH-OP01	Yes	Technology based SCH-UC2-TB7	Success	Yes	<i>Performance:</i> The system performance mainly depends on the performance of the applied distributed ledger technology.
SCH-OP02	Yes	Technology based SCH-UC2-TB8	Success	Yes	<i>Fault Tolerance:</i> We apply consensus algorithms supporting CFT. BFT compliant ones can be applied if needed.
SCH-OP03	Yes	Test Case SCH-UC2-TC4	Success	Yes	<i>Scalability:</i> The infrastructure can be set up via code and deployment can be automated.
SCH-OP04	Yes	Test Case SCH-UC2-TC5	Success	Yes	<i>Logging:</i> Application and systems logs are provided and can/will be used for monitoring purposes.
SCH-MP01	No			No	<i>Availability:</i> Not mandatory requirement for SCH-UC2.

ID	Validated	Strategy	Result	Mandatory	Comments
SCH-LR01	No			Yes	<i>GDPR Compliance:</i> We will review/update this review in the next iteration.
SCH-LR02	Yes	Technology based SCH-UC2-TB1	Success	Yes	<i>Protection against Counterfeiting:</i> Actors (human users and/or automated processes) need to have unique identifiers. This requirement also refers to SCH-SP02.
SCH-LR03	Yes	Technology based SCH-UC2-TB2 and SCH-UC2-TB5	Success	Yes	<i>Protection against financial fraud:</i> This requirement overlaps with SCH-SP03 and SCH-SP09, so that proofs for those apply here as well.
SCH-LR04	No	Technology based SCH-UC2-TB6		Yes	<i>Interfaces to audit log:</i> This requirement is addressed by providing access to audit log. Proof for requirement SCH-SP10 applies here as well but will be extended (providing an appropriate interface).

Table 9: Supply Chain Security Assurance – SCH-UC2 validation requirements' coverage.

3.3 Validation Summary

Both use cases of the Supply Chain Security Assurance demonstrator were partially validated as presented in detail in Section 3.1 (Use Case SCH-UC1 Supply Chain for Retail) and Section 3.2 (Use Case SCH-UC2 Compliance and Accountability in distributed Manufacturing). They are partially validated as they are both in the development phase at the time of writing.

However, overall, for SCH-UC1 10 out of 22 requirements were already successfully verified at this stage. Y were not validated as they do not apply to the use case, respectively do not represent mandatory requirements for SCH-UC1. Only remaining Z are partially validated as of today.

Also, for SCH-UC2 the validation overview provided in Table 9 shows that the development is far advanced: as-of-today out of 19 mandatory requirements, 11 are successfully validated and 5 are already partially validated. Apart from these 19, there are 3 additional requirements which are not mandatory for SCH-UC2 and are, thus, not getting validated.

ID	Validated	Result	Comments
SCH-UC1	Partially	Success	In the middle of the project, we are at <ul style="list-style-type: none"> 52% validated 48% not yet validated mandatory requirements (19 in total)
SCH-UC2	Partially	Success	In the middle of the project, we are at <ul style="list-style-type: none"> 58% validated 26% partially validated, and 16% not yet validated mandatory requirements (19 in total)

Table 10: Supply Chain Security Assurance demonstrator's use cases validation summary.

3.4 Lessons Learned and Future Work

The validation of the requirements of the Supply Chain Security Assurance demonstrator at M24 shows good progress for both use cases. Just taking the already fully successfully validated requirements for both use cases of X% for SCH-UC1 and 63% SCH-UC2 show that more than half of the requirements in the middle of the project duration are already fulfilled. This is further underpinned by the fact that for SCH-UC1 additional X% and for SCH-UC2 additional 21% of the requirements are already partially addressed and implementations are advanced. We foresee good progress also in the coming months and are sure to meet the defined requirements for the demonstrator in time.

The key lesson learned in the first half of the project and what has also been confirmed by the validation of the requirements is that distributed ledger technology, i.e., blockchain, as core layer of the demonstrator's architecture, represents a sound basis to achieve trustworthiness and security in a collaborative, distributed environment. Supply chain use cases can significantly benefit from an open platform like blockchain, helping to dynamically build up, control and extend complex distributed networks. Combined with a workflow engine to enforce business process compliance, the key security requirements of supply chain use cases can be addressed and realized efficiently and in short time.

Many of the security requirements identified for the Supply Chain Security Assurance demonstrator could be validated based on the selection of blockchain as distributed ledger technology. Furthermore, as shown above, test automation can be easily applied for many other test cases which helps us also to re-evaluate and confirm the demonstrator's qualities easily while the development advances further.

For the second half of the project we primarily see validation efforts regarding the following requirements:

- SCH-SP06 and SCH-SP07: those requirements will be the ones we will be focusing on with highest priority. Access control and the possibility to support anonymization will be evaluated in the second

half of the project. To address them, we will evaluate cryptographic approaches provided by Hyperledger Fabric to support the management of confidential information in distributed supply chain environments.

- SCH-LR01: in tandem with the previously mentioned requirements, we will evaluate if and how PII (personally identifiable information) needs to be managed in the demonstrators. The technologies addressed for SCH-SP06 and SCH-SP07 will also apply here.
- SCH-LR04: as addressed in Sections **Error! Reference source not found.** and 3.2, the blockchain layer provides a reliable and unforgeable audit log. To address SCH-LR04 we plan to write test cases to extract and export audit log data in a readable format from the blockchain.
- SCH-U01: concerning the notification of incidents we will evaluate on how to forward generated system and application log data to monitoring/SIEM environments for continuous security monitoring.

4 Privacy-Preserving Identity Management

This demonstrator aims at showcasing an easy to use, cryptographically secured, efficient, and privacy-preserving identity management solution. To this end, an identity management solution based on attribute-based anonymous credentials [8,9,10,11,12,13] has been developed and integrated into a university application portal when applying for a PhD-position.

In the chosen scenario, users receive digital credentials on their finished courses or academic degrees, and can selectively reveal parts of this information in during the job application process; e.g., in order to avoid age discrimination, applicants can present the name, type of degree, or issuing university during the first phase of the application, but hide information such as birth date or issuance date of the degrees they own.

The first phase of the demonstrator aimed at setting up the core functionalities and doing the initial integration of the demonstrator scenario. That is, as specified also in D5.2, the first phase focused on registration of users to the system, issuance of degrees, and the partial and selective presentation of obtained degrees during an application process. Advanced features like the revocation of credentials, de-registration from the system, or privacy-revocation in case of abuse were consciously kept for the second piloting phase. On the one hand, this was because these features are not of key relevance for the described scenario, but might only become relevant when using academic certificates in other contexts (e.g., when proving to a public agency that a certain number of ECTS points was received in order to be eligible for some study allowance without revealing the specific courses or degrees), or when deploying the technology in completely different fields like smart cities, etc. On the other hand, the aim of the first demonstrator phase was to understand the users' perception of the core technology, to select versatile specific technologies that allow for easy integration of further functionalities, and to overcome avoid possible future efficiency bottlenecks.

Architecture. Figure 36 shows the basic components of our demonstrator. Our system uses two mobile applications that must be deployed on user's mobile phone. The Academic Degree verification is the front-end application that utilizes user's interaction with our demonstrator. This mobile app lets the user:

- Obtain a credential that he has a valid credit;
- verify his stored credentials in order to prove that he possesses an academic title; and
- apply for research studies.

The Wallet application stores the issued credentials and interacts with the University Backend server to request and deliver the issued credential. This component is mainly used for issuing and verifying Privacy-ABCs to the users of the system. As the University Backend server is the only issuer in the current demonstrator setup, its parameters have been made available to all other components through a public repository. This repository is the University Backend server Public Directory that can be seen on Figure 36 and later in Figure 37. Finally, the PhD/MSc Submission system is a web application that implements the functionality of the application procedure to a PhD/MSc program. The PhD/MSc Submission system can be accessed only by the users with credentials that satisfy certain policies (e.g., proving possession of a certain degree). The application's access control functionality is implemented by the University Backend server. The PhD/MSc Submission system consists of a database that stores user's application form.

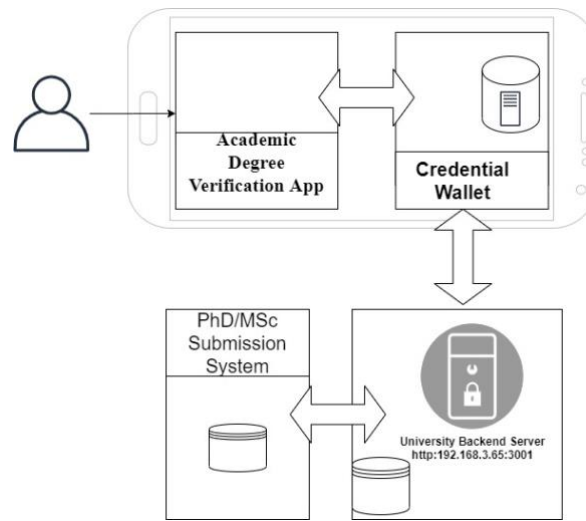


Figure 36: High-level components of the privacy-preserving identity management demonstrator

4.1 Use Case IDM-UC1 – Registration

Registration allows a user to onboard the ecosystem of privacy-preserving identity management. In the original plans for this demonstrator, it was planned to have a physical onboarding phase, during which the technology would be described, and where one-time passwords for registering on the platform are created.

However, due to the COVID-19 pandemic, it was decided to minimize the physical interactions required for the pilot execution phase, and the physical onboarding was postponed to a later phase of the demonstrator.

Resultingly, only a minimal version of this part of the demonstrator was actually evaluated, by providing participants with the necessary mobile apps to install on their mobile phone.

However, we do not consider this as a severe risk for the demonstrator case, as the core technology of the demonstrator is demonstrated in use cases IDM-UC2 and IDM-UC3.

4.1.1 Actors

The actors for the validation of this use case were researchers working on cryptography and privacy to carry out the technology based analysis.

Furthermore, 42 end users were recruited from at different levels of their studies (i.e., BSc and MSc candidates) to give feedback regarding usability, perceived privacy, etc. The participants had mainly computer science related backgrounds, however, without a special focus on cyber security. Future versions of the demonstrator case will also seek for feedback from participants with other backgrounds. About 67% of the participants were male and 33% were female. The age ranged from 22 years to 35 years, with an average of 28 years.

4.1.2 Test Cases

The validation strategy does not employ technical test cases at this stage of the demonstrator's development.

4.1.3 Technology based Analysis

Due to the very close interrelation between the use cases of this demonstrator, the technology based analysis is highly interrelated as well. As most of the requirements regarding, e.g., privacy or authenticity are of even higher importance in the context of UC2 and UC3, the analysis is also presented there, and we refer the reader to the relevant subsections.

4.1.4 Quality Indicators

4.1.4.1 User and stakeholder engagement and impact evaluation

Due to the very close interrelation between the use cases of this demonstrator, they were jointly evaluated using a single questionnaire. We refer to Section 4.3.4 for a common assessment for all use cases.

4.1.5 Requirements Coverage

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-SP03	No			Yes	While implemented, this part of the demonstrator was not part of the evaluation process with end users.
IDM-SP11	No			No	This requirement will be considered in future versions of the demonstrator case.
IDM-U01	No			Yes	This requirement is mainly related to IDM-UC3, and was sparsed out for IDM-UC1 during the first piloting round.
IDM-U02	No			Yes	This requirement is mainly related to IDM-UC3, and was sparsed out for IDM-UC1 during the first piloting round.
IDM-U03	No			Yes	This requirement is mainly related to IDM-UC3, and was sparsed out for IDM-UC1 during the first piloting round.

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-OP01	Yes	Questionnaire	Success	Yes	
IDM-MP01	No	n/a	n/a	No	While compatibility with existing standards is important for actual authentication processes, we consider this of low priority in the specific demonstrator scenario chosen in CyberSec4Europe.
IDM-LR01	Partially	Technology based analysis, Questionnaire	Success	Yes	Our solution supports service providers to achieve data minimization, yet de-registration is only to come as part of IDM-UC7.
IDM-LR02	No			No	At the time of writing this deliverable, the ePrivacy regulation has not yet been put in place.
IDM-LR03	No			Yes	This requirement will be analysed in the next iteration of the demonstrator case.
IDM-LR04	Partially			No	This requirement will be analysed in the next iteration of the demonstrator case. Yet, by setup of our demonstrator case, the user's identity is profoundly checked already when subscribing to the university.

Table 11: IDM-UC1 Validation requirements' coverage.

4.2 Use Case IDM-UC2 – Issuance

Issuance allows users to receive digital credentials on their data. Due to the reduced IDM-UC1, the use case was slightly adjusted: while in the original use case, users would have received credentials from the issuer, and would have synced these credentials to their devices.

4.2.1 Actors

The same actors as for use case IDM-UC1 were participating in the evaluation of this use case.

4.2.2 Test Cases

The validation strategy does not employ technical test cases at this stage of the demonstrator's development.

4.2.3 Technology Based Analysis

Anonymous credential systems. Anonymous credential systems (also known as attribute-based credentials, or ABCs) have first been envisioned by Chaum [8,9], and have subsequently been improved in a long line of research, including but not limited to [10,11,12,13,14]. In a nutshell, they allow users to receive digital certificates on their attributes (e.g., name, title, issuance date of a degree, etc.) in a way that later allows them to selectively reveal subsets of these attributes to other entities, in our case the application portal. This can be done in a way that gives high authenticity guarantees to the application portal, while giving the user full control over which data goes where.

There are two fundamental approaches to achieve this functionality. The first approach, taken, e.g., by UProve [14] is based on blind signatures. There, the issuer (in our case, the university granting a degree) does not learn the digital certificate handed over to the user. The user may then present this certificate at a later point in time, without her actions being linkable. In the second approach, the user receives a signature on her attributes. The signature scheme is selected in a way that allows for efficient zero-knowledge proofs of knowledge, which can be used to prove possession of a signature on some data without revealing the signature itself. This latter approach – followed, e.g., by [10,12,13] – has proven to be more versatile in terms of applications.

We based our demonstrator on the zero-knowledge-based ABC system by Camenisch and Lysyanskaya [10]. This has been done after a profound assessment of existing schemes. While more novel and more efficient schemes exist, we believe that the selected scheme is most versatile in terms of applications, as it also supports proving predicates over attributes, such as, e.g., that one is over 18 years old without revealing the specific birth date. While this is not strictly required for any of the use cases intended for our demonstrator scenario, we believe that this functionality is of high importance for possible future extensions of the demonstrator, within or beyond CyberSec4Europe. Also, because of the computational power of current mobile phones, the complexity of the required computations are no longer an obstacle for real-world deployments of the scheme.

The user's mobile application allows users to display the public key under which the credential has been issued, which can then be manually compared to the key belonging to the university, satisfying IDM-SP04. In large-scale deployments, these keys might be additionally be certified, e.g., by certificate authorities, which however is considered beyond the scope of our demonstrator as this would not give any additional technological insights.

Issuance flow. During issuance, the user logs in to the Academic Degree Verification Application by using a username and a password. The Academic Degree Verification Application interacts with University Backend server in order to get an access token that it includes a certain policy and a refresh token. The

Academic Degree Verification Application delivers the issuance token to the wallet application and stores it. A high-level overview of the issuance flow is depicted below.

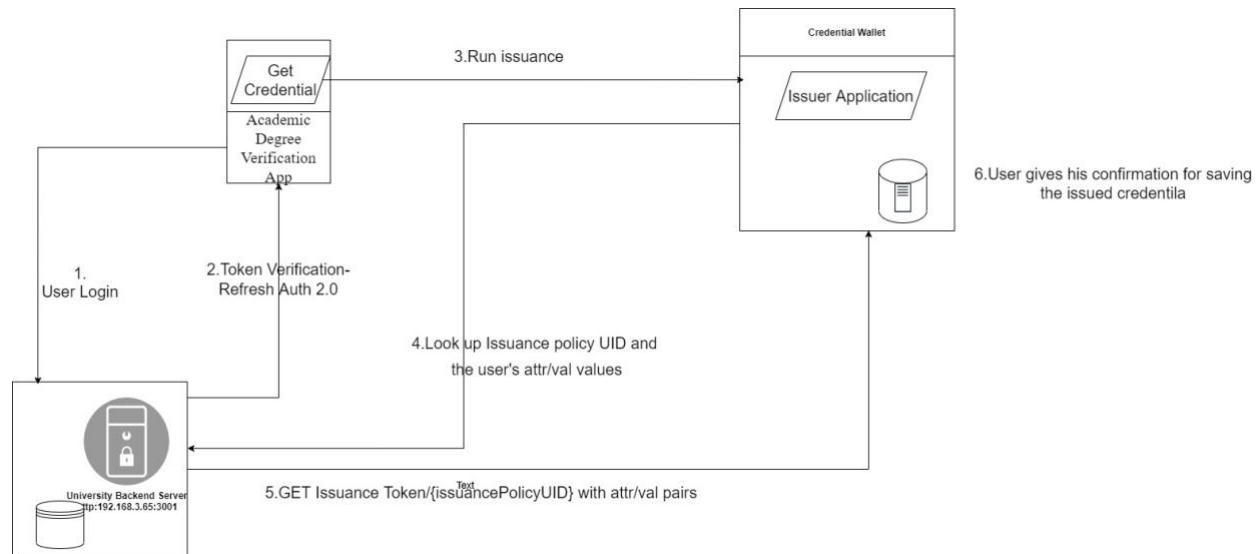


Figure 37: Issuance

User authentication within app. In order to open their mobile application and receive access to the credentials stored within the applications, users need to enter a PIN code that was setup when installing the application. While at this stage only access to the application is PIN protected, future versions of the application will store the contained information using state-of-the-art password-based encryption mechanisms in order to avoid abuse in case that the device is stolen.

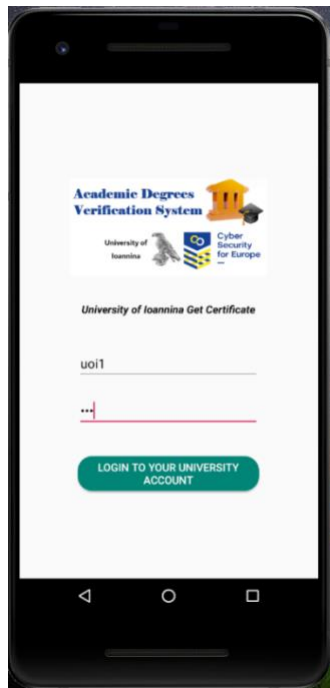


Figure 38: User authentication towards the mobile app using a PIN

4.2.4 Quality Indicators

4.2.4.1 User and stakeholder engagement and impact evaluation

Due to the very close interrelation between the use cases of this demonstrator, they were jointly evaluated using a single questionnaire. We refer to Section 4.3.4 for a common assessment for all use cases.

4.2.5 Requirements Coverage

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-SP03	Yes	Technology based analysis	Success	Yes	
IDM-SP04	Partially	Technology based analysis	Success	Yes	<p>The app allows users to display the key under which a credential was issued, which can then be compared with the key published by the university.</p> <p>Digital certificates on such keys (e.g., via</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					certificate authorities) are considered beyond the scope of the project.
IDM-SP10	Partially	Technology based analysis	Success	No	2FA (having the device and knowing a PIN) to unlock the credentials was implemented.
IDM-SP11	No			No	This requirement will be considered in future versions of the demonstrator case.
IDM-U01	Yes	Test case, questionnaire	Success	Yes	Cf. analysis in IDM-UC3
IDM-U02	Yes	Questionnaire	Success	Yes	Cf. analysis in IDM-UC3
IDM-U03	Yes	Test case, questionnaire			Cf. analysis in IDM-UC3
IDM-OP01	Yes	Questionnaire	Success	Yes	
IDM-MP01	No	n/a	n/a	No	While compatibility with existing standards is important for actual authentication processes, we consider this of low priority in the specific demonstrator scenario chosen in CyberSec4Europe.
IDM-LR01	Partially	Technology based analysis, Questionnaire	Success	Yes	Our solution supports service providers to achieve data minimization, yet de-registration is only to come as part of IDM-UC7.

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-LR02	No			No	At the time of writing this deliverable, the ePrivacy regulation has not yet been put in place.
IDM-LR03	No			Yes	This requirement will be analysed in the next iteration of the demonstrator case.
IDM-LR04	No			No	This requirement will be analysed in the next iteration of the demonstrator case.

Table 12: IDM-UC2 Validation requirements' coverage.

4.3 Use Case IDM-UC3 – Presentation

While the previous two use cases were only validated in a reduced fashion due to the ongoing COVID-19 crises and the associated limitations of physical meetings and events for piloting, the main focus of the first demonstration phase was put on the presentation. That is, the main focus was on the usability, efficiency, security, and privacy during the presentation phase of digital certificates.

To minimize the duration of physical meetings, the main focus was in the privacy-enhancing technology part of the application process. While a full application platform was implemented and tested, the evaluation mainly focused on the non-standard parts of the process, as no additional insights were to be expected, but these other parts were mainly required as a context for the main technologies.

The main part of the validation was done using technology assessments and interviews with end users. While the former was necessary to make profound security claims, the latter was necessary to investigate the users' perception and willingness to use the developed technologies.

The message flow during the verification key is depicted in the following figure.

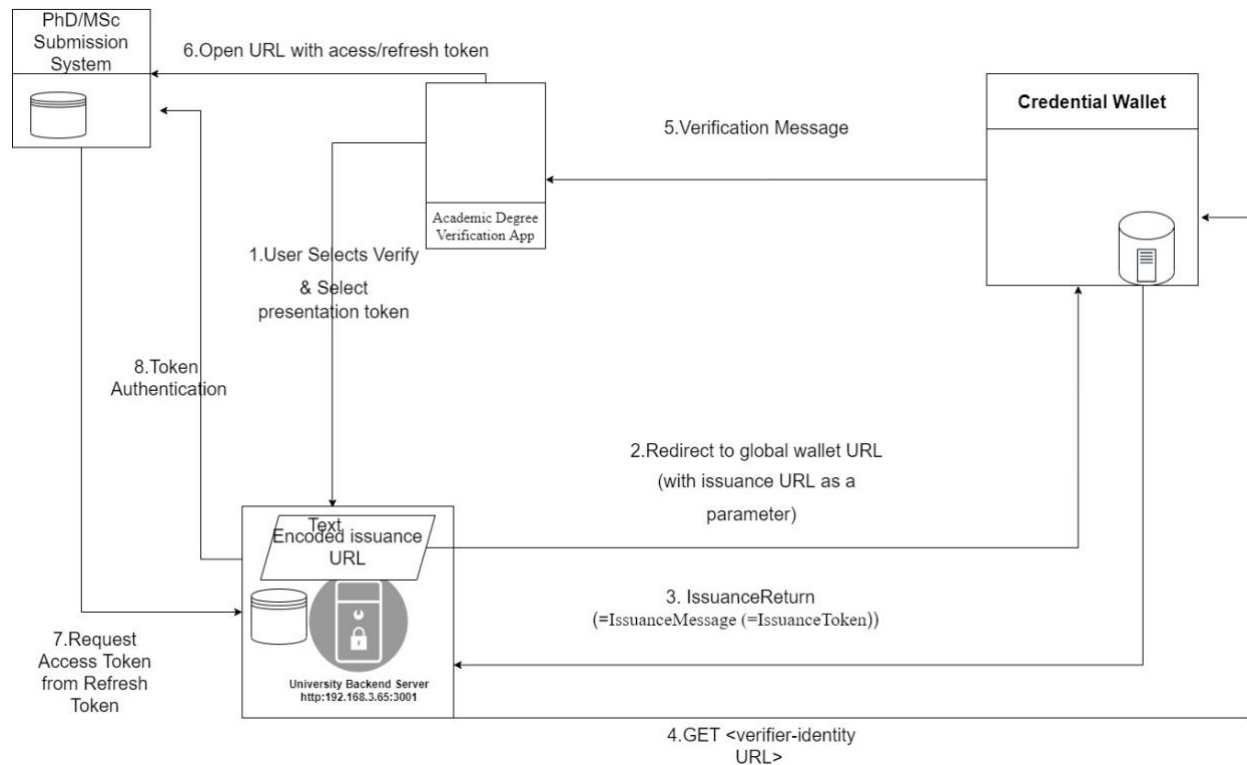


Figure 39: Verification

4.3.1 Actors

The same actors as for use case IDM-UC1 were participating in the evaluation of this use case.

4.3.2 Test Case

4.3.2.1 Description

The goal of this test case was the validation of requirement IDM-U01 by validating the computation times needed on end user devices to receive and to present attribute-based credentials during the application process.

4.3.2.2 Test Case Workflow

To test the efficiency, the relevant parts of the user mobile app were executed 100 times on a Xiaomi Redmi 4A (model 2016) mobile phone, running Android 7.0 (the Academic Degree Verification App can run on all versions from Android 7 onwards). Only the actual computation time was considered, not the time the user required to fill in forms, grant permissions, etc. The reasons for using a relatively old mobile phone were twofold. Firstly, for pragmatic reasons, the mobile phone was available as a test device at the consortium partner performing the tests. Secondly, we considered it important to guarantee realtimeness and responsivity of the developed applications also on older devices, in order to cover a broader set of users.

4.3.2.3 Test Results

On average, the time required to compute the presentation tokens was 439ms, with a maximum of 600ms and a minimum of 380ms.

4.3.3 Technology Based Analysis

By the cryptographic guarantees of digital signatures and zero-knowledge proofs of knowledge underlying attribute-based credential systems, the relying party (i.e., application platform), receives high formal guarantees that the user could **not have altered** any of the revealed attributes, cf. requirement IDM-SP02. Furthermore, as the application portal specifies the accepted issuers of digital certificates, we consider IDM-SP04 as satisfied. In large-scale deployments, these keys might be additionally be certified, e.g., by certificate authorities, which however is considered beyond the scope of our demonstrator as this would not give any additional technological insights.

Having the underlying technology in mind, it furthermore directly follows that on an application level, all user actions are **unlinkable**, as long as a user does not explicitly consent to revealing uniquely identifying attributes (such as her full name), cf. requirement IDM-SP05, IDM-SP06, IDM-SP07.

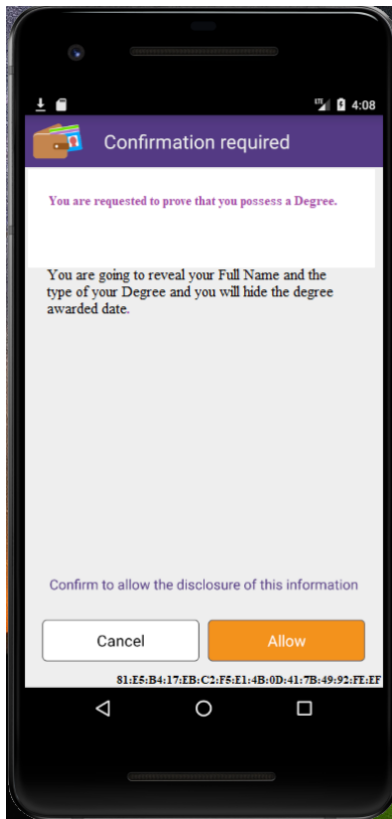


Figure 40: Users need to approve which attributes are revealed to a relying party.

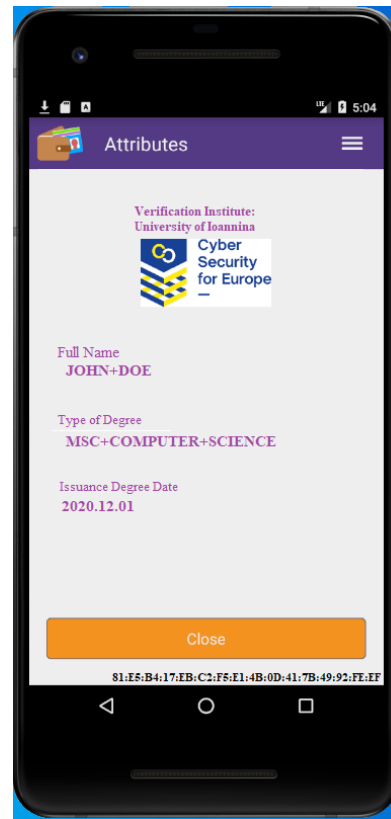


Figure 41: The key of the issuer is displayed at the bottom of the screen.

Network layer privacy. While ABC systems can contribute to the users' privacy on an application layer, they do not give any guarantees on the underlying network layer. This issue was tackled by routing all communication between the mobile phone and the application portal through Orbot, which is a free Android application for the TOR overlay network [15]. By routing the users' traffic over a series of random nodes

in the TOR network, aspects like the local IP address or the geographical source of the applicant are hidden from the application portal. By establishing new TOR circuits for independent sessions started from the mobile phone, also metadata privacy (e.g., regarding access patterns, etc.) are disguised. Thus, metadata privacy is guaranteed as long as a sufficiently large number of users participate in the system; the precise number of required participants depends on the specific requirements and needs additional investigation.

4.3.4 Quality Indicators

4.3.4.1 User and stakeholder engagement and impact evaluation

4.3.4.1.1 Questions

During the execution of the demonstrators, participants were asked a total of ten questions listed below.

The first questions aimed to understand whether the overall setup of the demonstrator was easy to understand, and whether the tasks were clearly communicated and explained to the students. Furthermore, we aimed at finding out whether from an efficiency and usability point of view, the developed solutions were acceptable

- Q1: Have you been able to complete all tasks of the tutorial efficiently? If not, please specify any issues you encountered:
- Q2: Did you feel comfortable using the Postgraduate Research portal system?
- Q3: Did the computations of the various steps in the Postgraduate Research portal process proceed sufficiently efficiently? If not, please specify which steps need efficiency improvements:
- Q4: Compared to traditional (not privacy-focused) job application portals, was it easy to use the proposed application portal?

The second set of questions aimed at understanding whether participants understood the privacy guarantees of the developed solution. Furthermore, we tried to find out whether participants are willing to trust such solutions, and whether they understand the added value of the technology for the specific use case, but also in general.

- Q5: Do you trust technologically enforced privacy-guarantees more than those based on contracts and policies?
- Q6: Do you think that maintaining privacy is important in everyday digital life?
- Q7: Do you think that cryptographically enforced privacy-mechanisms in (at least a first phase of the Postgraduate Research portal) can contribute to fight discrimination (e.g., regarding sex or age)?
- Q8: Do you think that the used privacy-preserving technologies could also be used in other contexts of your everyday digital life? If yes, please let us know where:

The next question checked whether it was clearly understood which attributes were actually revealed to the job application portal.

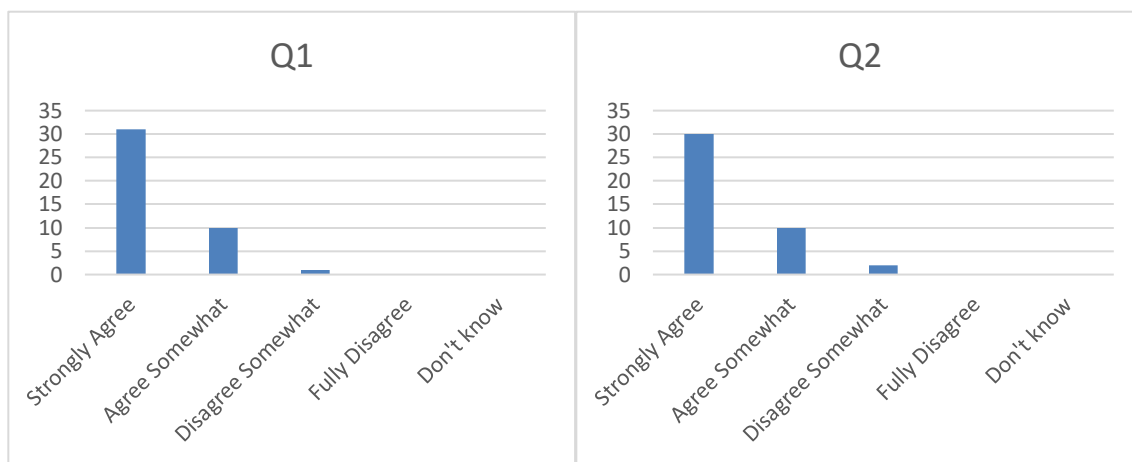
- Q9: Was it communicated clearly which parts of your academic degrees were revealed to the Postgraduate Research portal and which remained private?

Finally, we tried to find out whether participants see the potential benefit in increasing compliance of service providers using privacy-enhancing identity management systems, in order to comply with legal regulations such as the GDPR.

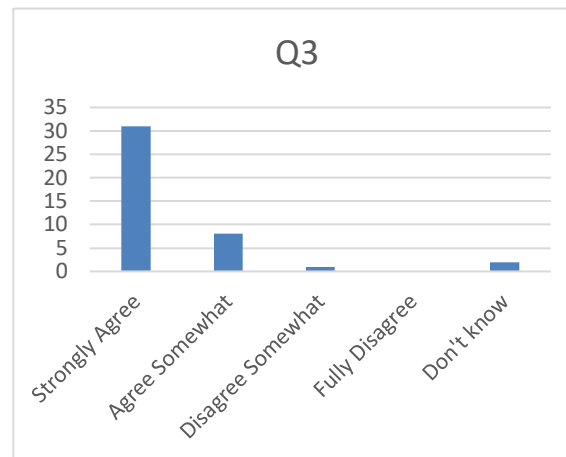
- Q10: Do you think that the given privacy-guarantees make it easier for service providers to comply with legal regulations such as the General Data Protection Regulation (GDPR)?

4.3.4.1.2 Feedback

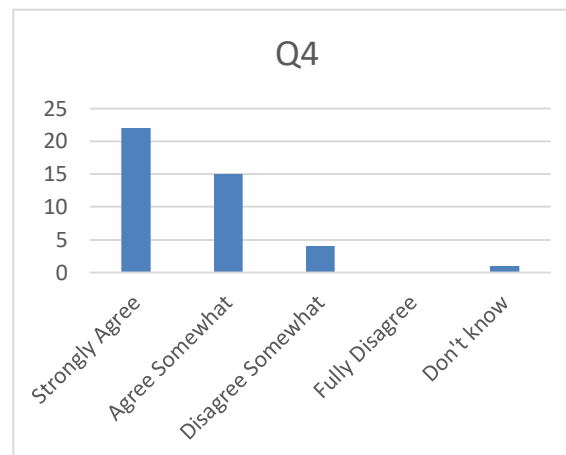
The first two questions related to the overall usability of the application portal and the clarity of the tasks received an overwhelming fraction of positive responses, across all subgroups of the participants. We thus conclude that the task description was clear and the following responses were not distorted by misunderstandings regarding the pilot setup.



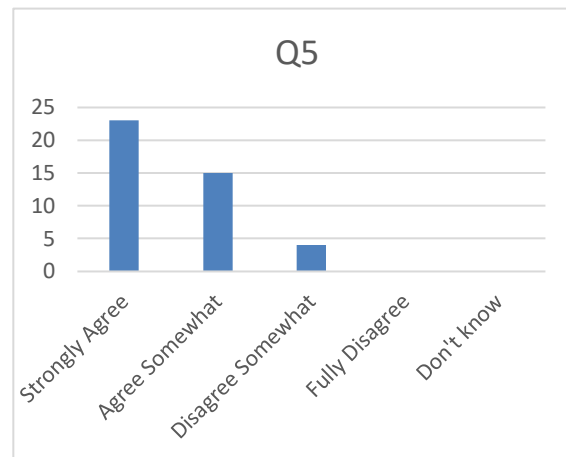
Regarding the overall efficiency of the system, only positive responses were received, demonstrating the practical efficiency of the developed solution. While the users could only evaluate the efficiency on the end user side, we also assume the system to be sufficiently scalable to large numbers of users by using usual load-balancing systems on the server side. It is worth noting that the participant partially disagreed with the efficiency of the scheme left a comment about poor Internet connectivity in the open notes field of the questionnaire.



Furthermore, an overwhelming number of participants (37 of 42) confirmed that the usage of privacy-preserving technologies for single steps during an application process (in our case when uploading the formal cryptographic proofs of possession of an academic degree) is not distracting compared to traditional portals. The small number of negative responses was justified with the additional step that is necessary to upload the certificates, which however is hard to avoid when putting the user into full control over which data goes where.

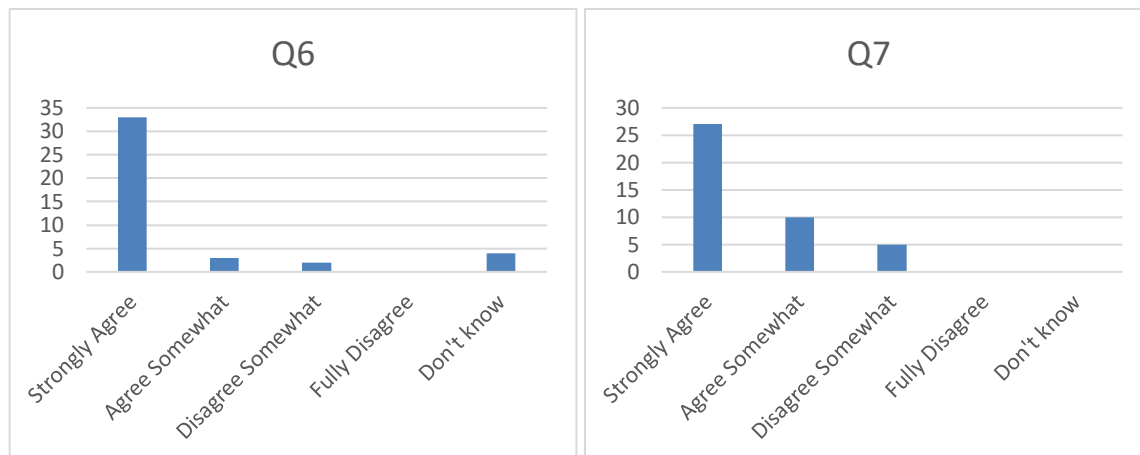


About 90% of the participants would be more willing to trust privacy-enhancing technologies more than privacy guarantees based on policies and contracts. Considering the oral and written feedback of participants during the demonstrator execution, we conclude that technological mechanisms should however not be considered a replacement for traditional policies, but rather be a complementary tool to increase users' trust in digital systems.



Virtually all participants of the demonstrator execution phase agree that maintaining privacy in an increasingly interconnected world is important. However, for the given application scenario a fraction of about 10% of the participants does not believe that privacy-enhancing technologies can contribute to fight, e.g., age or gender discrimination, when redacting parts of the user's identity during the (first phase of the) application process.

When updating the graphical interfaces of the application portal for the next piloting round from a functional to an advanced and more user-friendly version, we will take this feedback into consideration to make sure that the redacted information is not unintendedly provided in other steps of the application, which will hopefully increase the understanding and positive impact of the technology.

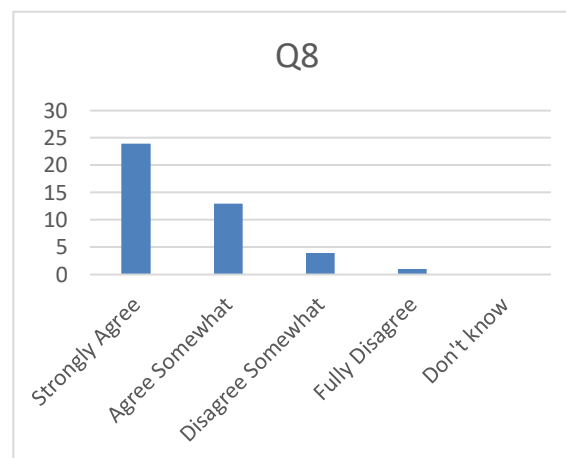


57% of the participants strongly agree that ABC systems would also be useful in other digital scenarios, and 31% participants somewhat agree to this question. Unfortunately, the 12% of participants disagreeing with this statement did not provide details in the open fields of the question. However, it was interesting to see

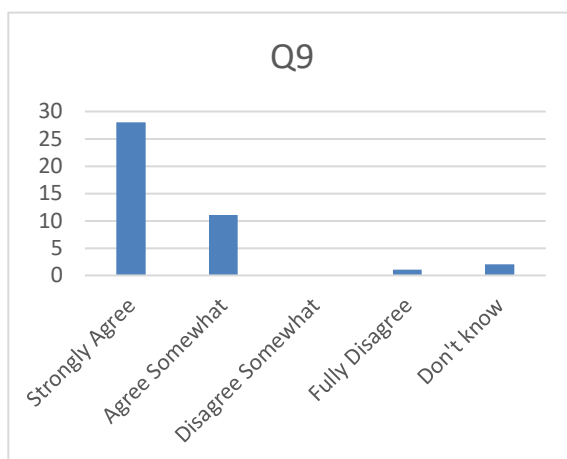
that there was a correlation between age of participants and their enthusiasm about the technology: on average, younger participants were more positive about ABCs than their elder counterparts.

12 of 42 participants provided specific suggestions for application scenarios of ABC systems. Economic institutions and banks were listed 5 times, while interactions with public agencies were suggested twice, and sharing of medical data was suggested by one participants. The remaining feedback was more generic (e.g., “every application that requires access to personal data”).

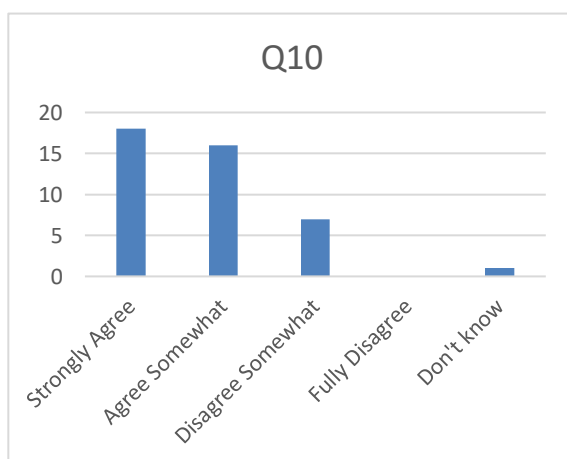
When extending and polishing the user application for the next piloting round, some additional screens explaining the technology and its opportunities will be added to increase the understanding of the versatility of ABC systems.



39 out of 42 users agree that it was clearly communicated which information would be revealed to the application portal when computing a presentation of their digital certificates, such that we consider the corresponding requirement satisfied. However, in order to increase the understanding, we will analyze parallel results from related tasks (e.g., suggesting to require user interactions compared to solely presenting the information to the user) for the next piloting phase.



While most participants agreed that from their understanding, the tested application platform and the deployed privacy-enhancing technologies would help service providers to comply with legal regulations such as the GDPR, as significant fraction of 17% somewhat disagrees with this. We acknowledge that for the given demonstrator scenario, all the redacted information would be revealed to the application portal at some later stage of the application process, thus not minimizing the overall amount of information revealed to the application portal, but rather avoiding, e.g., discrimination during certain stages of the process. In the next user trial phase, the question will be split in order to analyse the understanding of users for our specific scenario, but also for the technology in general.



4.3.5 Requirements Coverage

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-SP02	Yes	Technology based analysis	Success	Yes	Formal guarantees from unforgeability of

ID	Validated	Strategy	Result	Mandatory	Comments
					digital signatures and soundness of zero-knowledge proofs
IDM-SP03	Yes	Technology based analysis	Success	Yes	
IDM-SP04	Partially	Technology based analysis	Success	Yes	The relying party defines accepted issuer keys. Digital certificates on such keys (e.g., via certificate authorities) are considered beyond the scope of the project.
IDM-SP05	Yes	Technology based analysis	Success	No	Follows from the privacy guarantees of ABC systems (application layer) and TOR (network layer).
IDM-SP06	Partially	Technology based analysis, Questionnaire	Success	Yes	Users are clearly informed about which attributes will be revealed. Eligibility checks whether relying parties may actually request these attributes have not yet been considered.
IDM-SP07	Yes	Technology based analysis	Success	Yes	All information revealed to the relying party needs to be confirmed by the user.
IDM-SP11	No			No	This requirement will be considered in future versions of the demonstrator case.
IDM-U01	Yes	Test cases, questionnaire	Success	Yes	

ID	Validated	Strategy	Result	Mandatory	Comments
IDM-U02	Yes	Questionnaire	Success	Yes	
IDM-U03	Yes	Questionnaire	Success	Yes	
IDM-OP01	Yes	Questionnaire	Success	Yes	
IDM-MP01	No	n/a	n/a	No	While compatibility with existing standards is important for actual authentication processes, we consider this of low priority in the specific demonstrator scenario chosen in CyberSec4Europe.
IDM-LR01	Partially	Technology based analysis, Questionnaire	Success	Yes	Our solution supports service providers to achieve data minimization, yet de-registration is only to come as part of IDM-UC7.
IDM-LR02	No			No	At the time of writing this deliverable, the ePrivacy regulation has not yet been put in place.
IDM-LR03	No			Yes	This requirement will be analysed in the next iteration of the demonstrator case.
IDM-LR04	No			No	This requirement will be analysed in the next iteration of the demonstrator case.

Table 13: IDM-UC3 Validation requirements' coverage.

4.4 Validation Summary

ID	Validated	Result	Comments
IDM-UC1	Partially	Success	The physical part of the onboarding process was not validated due to the ongoing spread of the corona virus. However, this mainly concerned administrative processes unrelated to the demonstrated technology.
IDM-UC2	Yes	Success	
IDM-UC3	Yes	Success	
IDM-UC4	No		Planned for the second piloting phase
IDM-UC5	No		Planned for the second piloting phase
IDM-UC6	No		Planned for the second piloting phase
IDM-UC7	No		Planned for the second piloting phase

Table 14: Privacy-preserving identity management demonstrator's use cases validation summary.

4.5 Lessons Learned and Future Work

The first round of this demonstrator case focused in the initial setup of all necessary platforms, performing fundamental integrations with the necessary platform, and validating the core underlying technologies. For future piloting rounds, several extensions need to be considered:

- Firstly, due to the ongoing spread of the coronavirus, the initial registration and joining phase was only tested in a very minimal setting. In the second version of this demonstrator, we will catch up on this to test all phases of the demonstration scenario.
- Furthermore, all missing use cases will be further worked on during the next phase. By adding relevant features, such as, e.g., revocation or deregistration, a fully working ecosystem will be generated. This will also allow us to evaluate, e.g., legal requirements in more details, as deregistration or correction of data will then become possible.
- Thirdly, for the first piloting phase, it was intended to inform users via paper-based documents about privacy policies, etc. Because of the changed scenario, this was now done orally as part of the introduction of the demonstrator case. Future versions might include detailed, multi-layer privacy-policies, which we intend to compile in close collaboration with task T3.6 to achieve high usability and legal compliance.
- Finally, for the next demonstration round, we will aim for a broader set of end users, including participants with non-IT-related backgrounds. Furthermore, a legal analysis in collaboration with corresponding partners in the consortium, is planned.

5 Incident Reporting in the Financial Sector

5.1 Use Case IR-UC1: Data Collection, Enrichment and Classification

The main objective to be validated in this Use Case is the effective possibility to collect all information about the incident. The demonstrator must be able to collect all the information necessary that will be used to evaluate the severity of the incident and the consequent need to report mandatorily the incident to an Authority, and to generate latter the report template with the information required.

In this phase all the functionalities available and applicable with the demonstrator developed till now are validated. In this Use Case the main focus is the data. The validation includes the evaluation of the presence of all the fields indicated as necessary to collect all the information necessary to go on with the process. It will be validated whether the tool is able to collect all the information required for incident reporting, according to the requirements established by the PSD2 (Payment Services Directive) and the ECB/SSM framework (European Central Bank Single Supervisory Mechanism), and whether the tool allows to categorize and classify the incident.

The validation strategy has included the validation of functional requirements, security and privacy requirements and non-functional requirements, such as look and feel requirements, usability requirements, operational requirements, maintainability and portability requirements and legal and regulatory requirements.

The validation has been performed through the execution of different test scenarios of potential security incidents detected in a financial entity. This Use Case will be successfully validated if the information required in those test scenarios is collected and the incident is correctly classified according to the criteria and thresholds established by PSD2 and the ECB/SSM framework.

5.1.1 Actors

The validation of this Use Case has been carried out by the two end-users involved in Task 5.4, BBVA and Intesa Sanpaolo. In this particular Use Case, they represent users from their respective organizations playing the following roles:

- Asset Owner / Incident Management Team (IMT)
- Incident Classification Team (ICLT)
- Administrator

The validation of the quality indicators has been performed by the technology owner, ATOS.

5.1.2 Test Case 1-UC1: Incident Data Collection

5.1.2.1 Description

The objective of Test Case 1 is to validate the effective possibility to collect all the information necessary about the incident in the Incident Reporting Platform. This information will be used to evaluate the severity

of the incident and the consequent need to report mandatorily the incident to a competent authority, and to generate the report template with the information required by the competent authorities.

Test Case 1 has included the validation of the presence of all the fields required for incident reporting according to the requirements established by the PSD2 and the ECB/SSM framework.

The validation has been performed through the execution of different test scenarios of potential security incidents detected in a financial entity:

- **Scenario 1: Cyber incident caused by ransomware due to phishing email**

On the morning of January 14th, multiple employees of the Gamma Bank, a large Italian financial institution, received an email from an address resembling the one of the Bank of Italy and carrying a suspicious MS Word attachment. Although most of the recipients successfully identified the email as a phishing attempt and avoided opening the attachment, a few others, including some members of the IT department, opened it.

The attachment contained a ransomware, which first infected the systems of the users that opened it and then quickly spread inside the network of the financial institution, encrypting a large amount of data and making it inaccessible to all the employees of the bank. When opened, the files prompted a message in which the attackers demanded a ransom of €150.000 in cryptocurrency to unlock the files. The ransomware also affected the database containing the most recent backups, which was not adequately segmented from the rest of the network.

After a crisis meeting involving the CISO and other top management of the bank, the decision to pay the ransom to the attacker was taken. Having paid the ransom and received a decryption key, however, the management soon found out that the key could not unlock the encrypted files and all the affected data was irreversibly lost. The bank was not ensured against cyber incidents, ended up spending more than €2 million to restore its IT infrastructure, and was forced to resort to an older backup copy.

The incident was covered by several major national news agencies and, as a result, many customers lost their trust in the ability of the bank to manage their financial interests. Following the incident, national police started an official inquiry.

Known information:

- The cyber incident was caused by a ransomware which infected the bank's network and devices through a malicious file attached to a phishing email. The identity of the attacker(s) is still unknown.
- The bank solved the incident in 2 weeks. In the process, the bank lost more than €2 million.
- Despite its widespread impact, the incident did not affect the payment services of the bank, which continued to operate normally.
- Following the inadequate management of the incident and the media coverage, the bank suffered a heavy damage to its reputation.

Figure 42 drafts the notification procedure that need to be followed in this scenario.

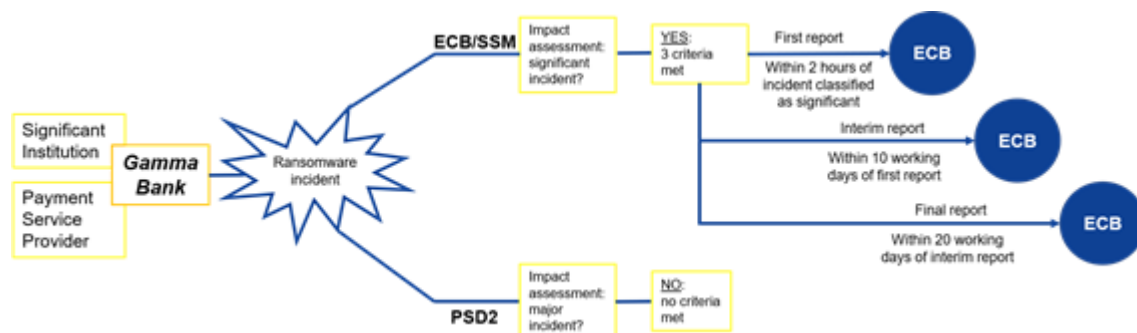


Figure 42:: IR-UC1 - Scenario 1 (Cyber incident caused by ransomware due to phishing email)

- **Scenario 2: Cyber incident caused by DDoS attack on the e-banking website.**

In December 2019, Gamma Bank, a large Italian financial institution, cut more than 500 jobs in its national offices and headquarter in an effort to reduce its expenditure. On December 23rd, a heavy DDoS attack simultaneously hit the web server hosting the home banking service and the mobile application server of the bank, making the bank's website and mobile app both unavailable for about 3 hours.

Although not receiving any media coverage, the incident sparked several complaints of the bank's customers on social media channels, who could not access their accounts and initiate any financial transaction from their computers or mobile devices. The bank's Incident Classification Team estimates that the incident affected more than 15.000 payment service users (more than 10% of the bank's payment users) and more than 10% of the bank's normal level of transactions, exceeding €100.000 in value.

The incident received only a limited coverage, with only a few blogs and sectorial news websites recounting the event.

Known information:

- The cyber incident was caused by a DDoS attack, which made the website of the bank and its e-banking and mobile banking channels entirely unavailable for about 3 hours.
- The bank's Incident Classification Team estimated that the incident affected more than 15.000 payment service users (more than 10% of the bank's payment users) and more than 18.000 transactions – more than 10% of the bank's normal level of transactions (150.000), exceeding €100.000 in value.
- After a week of investigations, the Incident Classification Team found out that the attacker was a former IT employee of the bank who wanted revenge for being fired.
- The incident had a limited economic impact (€ 50.000) and was not escalated to the internal managerial functions.

Figure 43 drafts the notification procedure that need to be followed in this scenario.

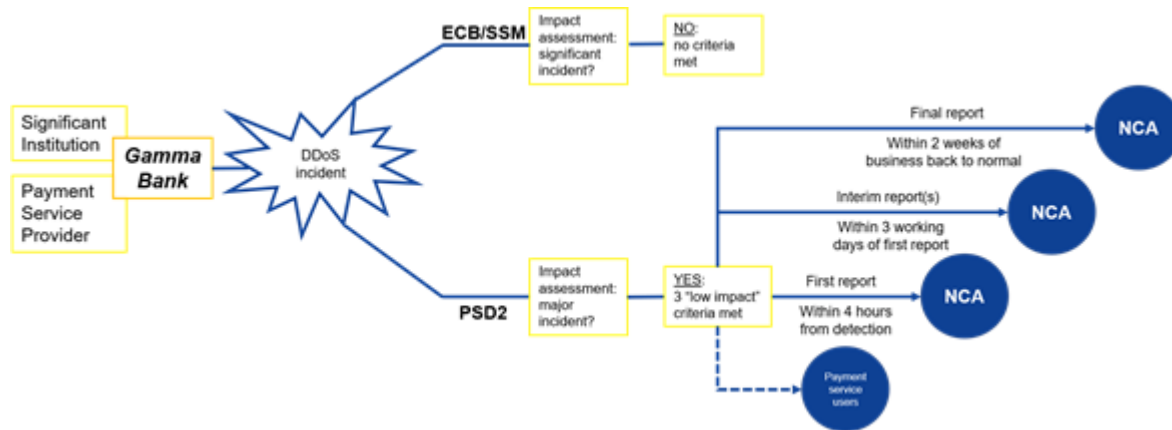


Figure 43:: IR-UC1 – scenario 2: Cyber incident caused by DDoS attack on the e-banking website

• **Scenario 3: Cyber incident caused by DDoS attack on the e-banking website.**

This is the same scenario describe in Scenario 2 but in this case the bank's Incident Classification Team estimates that the incident affected more than 26.000 payment service users (more than 10% of the bank's payment users) and more than 10% of the bank's normal level of transactions, exceeding €100.000 in value. And in this case, the row on social medias caught the attention of some major national news agencies and a few blogs and sectorial news websites also covered the incident, potentially damaging the bank's reputation.

Known information:

- The cyber incident was caused by a DDoS attack, which made the website of the bank and its e-banking and mobile banking channels entirely unavailable for about 4 hours;
- The bank's Incident Classification Team estimated that the incident affected more than 26.000 payment service users (more than 10% of the bank's payment users) and more than 24.000 transactions – more than 10% of the bank's normal level of transactions (150.000), exceeding €100.000 in value;
- After a week of investigations, the Incident Classification Team found out that the attacker was a former IT employee of the bank who wanted revenge for being fired;
- The incident had a limited economic impact (€70.000) but, due to the potential reputational damage resulting from the media coverage, was escalated to the internal managerial functions.

Figure 44 drafts the notification procedure that need to be followed in this scenario.

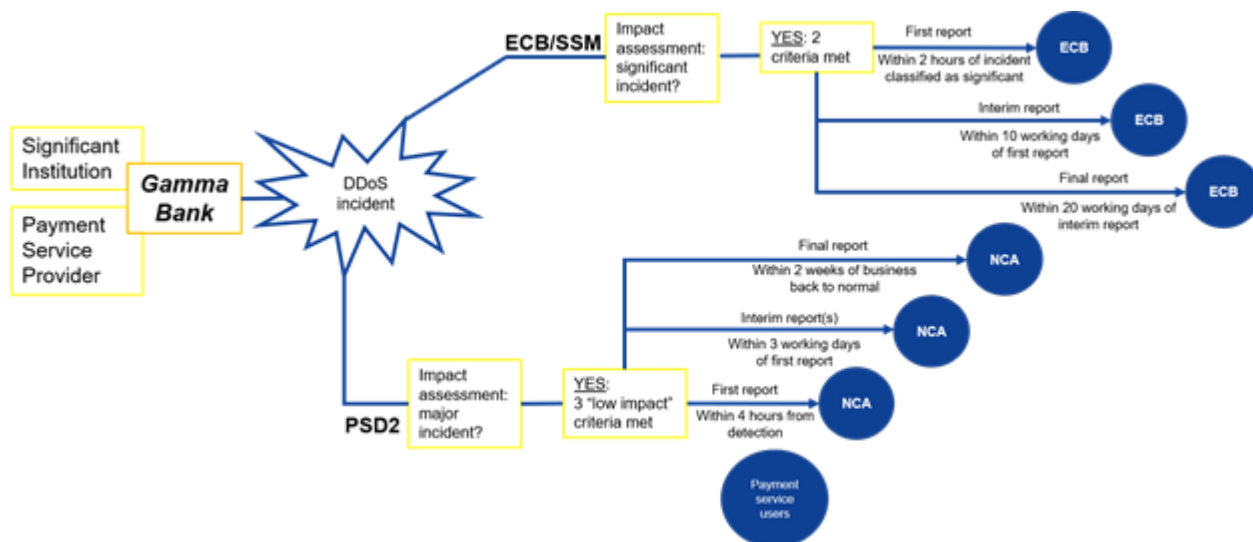


Figure 44: IR-UC1 Scenario 3 (Cyber incident caused by DDoS attack on the e-banking website)

• **Scenario 4: Manual shut down of bank website for investigation after slowdown.**

On the morning of October 17th 2019, the website hosting the e-banking commercial channel of Gamma Bank, a large Italian financial institution, experienced a substantial slowdown for about one hour.

Suspecting an external attack, the IT team of the bank decided to shut down the website to carry out an investigation. After a brief investigation (30 minutes), the IT team was able to link the cause of the incident to a system misconfiguration done the previous evening during a scheduled maintenance operation. They were then able to fix the misconfiguration and to restore the website in 20 minutes.

The incident did not affect a large number of users or transactions, was not escalated, and did not receive noteworthy attention from the media or social channels.

Known information:

- After experiencing a substantial slowdown, the website of Gamma Bank was manually shut down in order to carry out an investigation.
- The cause of the incident was linked to a human error (system misconfiguration) which took place the evening before.
- The issue was fixed and the website of the bank was quickly restored. In total, the incident lasted about 1:50h.
- The incident did not affect a large number of users (8.600) or transactions (5.000), was not escalated, and did not receive noteworthy attention from the media or social channels.

Figure 45 drafts the notification procedure that need to be followed in this scenario.

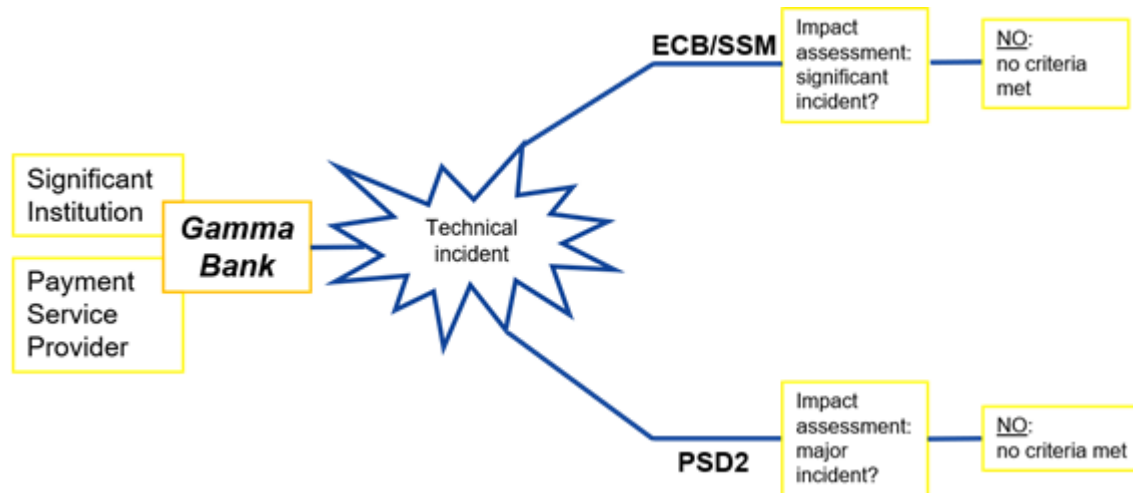


Figure 45: IR-UC1 – Scenario 4 (Manual shut-down of bank website for investigation after slowdown)

5.1.2.2 Test Case Workflow

As it was described in D5.1, Use Case 1 is focused on the Data Collection phase, where the Incident Management Team will introduce all the information related to the security incident through the incident reporting platform web page. All the information required in this phase is 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.

The workflow related to this Test Case is described as follows. First of all, the Administrator has to register all the information about the entities and users that can use the Incident Reporting Platform (name of Entity, type of Entity, country of Entity, contact persons,...).

Then, the Administrator has to assign the roles and the respective permissions of the different users involved in the incident reporting process:

- Incident Management Team (IMT)
- Incident Classification Team (ICLT)
- Controller
- Incident Reporting Team (IRT)

Finally, the Administrator has to configure the Incident Reporting Platform with the information about the different regulatory frameworks required to deal with the mandatory incident reporting process. In particular, in this use case the administrator will select to enable the regulations ECB and PSD2 for the financial entity, will introduce the information about the financial entity first and secondary contacts and data protection officer, and will check the recipients and templates associated to each regulatory framework selected.

Once the configuration of the Incident Reporting Platform has been finished, the incident has to be registered by the Incident Management Team in the Incident Reporting Platform, selecting the option “New Case” in TheHive GUI. The Incident Management Team has to select the template “First Incident Report” and then select the option “Create Case”.

Once the incident has been registered, the Task “Data Collection”, assigned to the Incident Management Team, is shown in the section “Tasks” of the Incident Reporting Platform.

The Incident Management Team has to fill in the questionnaire through TheHive template, providing all the information related to the security incident.

The information to be provided is the information required by PSD2 and ECB/SSM framework:

- General description of the incident.
- Information about the incident: Event timeline, event detection, impact, incident type, incident status, estimated costs, reputational damage, payment transactions affected, payment services users affected,...
- Specific information for mandatory incident reporting (payment services affected by the security event, functional areas affected, type of process/service disruption,...).
- Additional information for mandatory incident reporting (commercial channels affected, business lines affected, information of the attacker,...).

In Phase 1 only the First Report required by PSD2 and ECB/SSM framework is created by the demonstrator, as these are the two frameworks that have been included in the scope of this phase.

Once all available information of the incident has been included, the Incident Management Team has to close the task “Data Collection”.

5.1.2.3 Test Results

The results of Test Case 1 have shown that the Incident Reporting Platform gives the effective possibility to collect all the information necessary about the incident, that will be used to evaluate the severity of the incident and to generate the report template with the information required by the competent authorities.

It has been verified that the Administrator can register all the information about the entities and users that can use the Incident Reporting Platform, and assign the roles of the different users involved in the incident reporting process.

The information gathered by the Incident Reporting Platform is the information required to generate the Initial Report to be sent to the competent authorities according to the requirements established by PSD2 and the ECB/SSM framework (as only the Initial Report has been included in the scope of Phase 1).

5.1.3 Test Case 2-UC1: Data Enrichment

5.1.3.1 Description

The objective of Test Case 2 is to validate the effective possibility for the Incident Classification Team to include in the Incident Reporting Platform additional information about the incident to enrich the data previously provided by the Incident Management Team. This information will be used to evaluate the severity of the incident and the consequent need to report mandatorily the incident to a competent authority, and to generate the report template with the information required.

The validation has been performed through the execution of the four different test scenarios of potential security incidents detected in a financial entity described in 5.1.2.1

5.1.3.2 Test Case Workflow

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 is done using the GUI and taking into consideration the information received by the Supervisory Authorities (if any).

Once the task “Data Collection” has been closed by the Incident Management Team, a new task “Data Enrichment” appears in the section “Tasks” of the Incident Reporting Platform. This task is assigned to the Incident Management Team and the Incident Classification Team.

The Incident Classification Team has to include in the Incident Reporting Platform additional information about the incident to enrich the data previously provided by the the Incident Management Team. “Observables” can be added to the incident (files, suspicious IP addresses, domains or URLs related to the incident or a malware sample file, for example) and analyzers can be run on them from TheHive GUI included in the Incident Reporting Platform. In the specific scenario used in the test case, the analyzer HADES will be invoked on a file suspicious of malware. The result of the analysis will be included as a “data enrichment” task log so it is available for latter analysis if necessary (e.g. by the Controller).

When all the additional information has been included, the task “Data Enrichment” has to be closed by the Incident Classification Team, to continue with the process.

5.1.3.3 Test Results

The results of Test Case 2 have shown that the demonstrator gives the effective possibility for the Incident Classification Team to include in the Incident Reporting Platform additional information about the incident to enrich the data previously provided by the the Incident Management Team.

It has also been validated that “Observables” can be added to the incident (files, suspicious IP addresses, domains or URLs related to the incident or a malware sample file,...).

5.1.4 Test Case 3-UC1: Event Classification

5.1.4.1 Description

The objective of Test Case 3 is to validate whether the Incident Reporting Platform allows to categorize and classify the incident, according to PSD2 and the ECB/SSM framework, in order to verify the applicability of incident reporting regulatory requirements and therefore, the need to report the incident to the competent authorities.

The validation has been performed through the execution of the four different test scenarios of potential security incidents detected in a financial entity described in 5.1.2.1

5.1.4.2 Test Case Workflow

Once all the information about the incident has been collected and included in the Incident Reporting Platform, 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 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.

The impact assessment is performed according to PSD2 and the ECB/SSM framework, in order to verify the applicability of incident reporting regulatory requirements.

The workflow related to this Test Case is described as follows. Once the task “Data Enrichment” has been closed, a new task, “Incident Classification”, appears in the section “Tasks” of the Incident Reporting Platform.

First of all, the Incident Classification Team has to check if all the information necessary to do the event classification has been included in the template. Then, if all the information has been included, the Responder “CS4EU Incident Reporting Event Classifier” has to be invoked.

The following fields are necessary to do the severity impact evaluation, according to PSD2 and the ECB/SSM framework:

- Reputational damage.
- Downtime for the service/process disruption.
- Number of payment service users affected.
- Number of payment service users.
- Payment Transactions affected.
- Regular level of payment transactions.

The Responder “CS4EU Incident Reporting Event Classifier” takes all the information about the incident that has been included during the previous phases of the process, “Data Collection” and “Data Enrichment” and does the impact assessment, classifying the incident according to the criteria and thresholds defined by the regulations included in the scope of this phase (PSD2 and the ECB/SSM framework).

The result of the Responder “CS4EU Incident Reporting Event Classifier” is shown in the incident page and is also automatically updated in the fields of the template. The information provided by the Responder is the Incident Impact Severity and the need to report the incident to a supervisory authority, detailing the authorities the Initial Report has to be submitted to.

The Incident Classification Team has to review the suggestion provided by the Responder and, in case it is necessary, modify the fields related to the Impact Severity and the submission to competent authorities.

Finally, the Incident Classification Team has to close the task “Incident Classification”, so that a new task is created and assigned to the Controller (Use Case IR-UC2, “Managerial Judgement”). The Report will then progress to “Ready For Managerial Judgement”.

5.1.4.3 Test Results

The results of Test Case 3 have shown that the Incident Reporting Platform gives the effective possibility to categorize and classify the incident, according to PSD2 and the ECB/SSM framework, in order to verify the applicability of incident reporting regulatory requirements and therefore, the need to report the incident to the competent authorities.

It has been validated that the Responder “CS4EU Incident Reporting Event Classifier” can be invoked and that its results are shown in the incident page and automatically updated in the fields of the template.

In the scenario 1 (cyber incident caused by ransomware due to phishing email), the security incident is classified as Significant and it only mandatory incident reporting criteria for ECB/SSM have been met.

In the scenario 2 (cyber incident caused by DDoS attack on the e-banking website), the security incident has been also classified as Significant but in this case only PSD2 criteria are fulfilled and it is only required notification to this supervisory authority.

In the scenario 3 (cyber incident caused by DDoS attack on the e-banking website), the security incident has been also classified as Significant and it is required to be notified under ECB and PSD2 regulations.

In the scenario 4 (manual shut down of bank website for investigation after slowdown) the security incident has been classified as Non-significant.

Finally, it has been validated that the incident is correctly classified according to the criteria and thresholds established by PSD2 and ECB/SSM framework.

5.1.5 Technology Based Analysis

In this Use Case we can differentiate four main functionalities:

- Incident data collection
- Data enrichment
- Incident impact assessment
- Incident reporting workflow enforcement

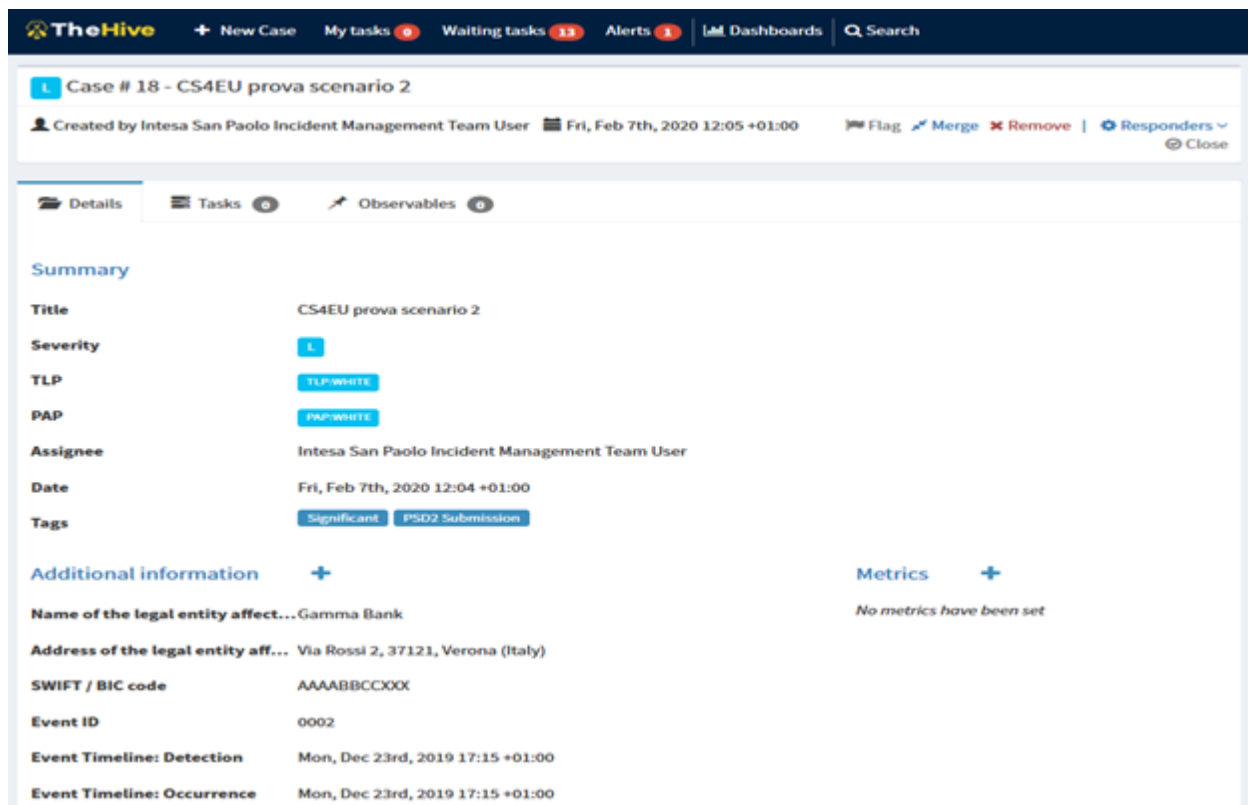
5.1.5.1 Incident data collection

The data about the security incidents to be reported is gathered through a graphical interface which integrates the GUI provided by the asset AIRE (Atos Incident Reporting Engine) with the GUI provided by the open source tool TheHive¹³.

The first one (AIRE asset) allows to collect general information about the financial entities, users and regulations (such as templates required, recipients of the reports and communication channels) that will be used by different incidents reported by a same organization or under a same regulatory framework.

TheHive offers by itself a security incident response platform where information about security incidents can be managed. It supports to register new incidents (“cases” in TheHive terminology) and with this purpose the administrator can define templates with the information necessary. These templates have a predefined structure with the following sections: Summary, Additional information, Metrics and Description. The additional information is composed of a set of custom fields that need to be defined and created by the administrator in advance. For the implementation of the current use case in the demonstrator, we have created our own template for incident reporting in the financial sector with a set of custom fields to retrieve the information necessary for mandatory reporting according to the regulations we are considering in this phase (PSD2 and ECB) and to perform the incident classification. An example is shown in Figure 46.

¹³ <https://thehive-project.org/>



The screenshot shows the TheHive interface for an incident titled "Case # 18 - CS4EU prova scenario 2". The incident was created by "Intesa San Paolo Incident Management Team User" on "Fri, Feb 7th, 2020 12:05 +01:00". The interface includes tabs for Details, Tasks, and Observables. The Summary section displays the following information:

- Title:** CS4EU prova scenario 2
- Severity:** L
- TLP:** TLP:WHITE
- PAP:** PAP:WHITE
- Assignee:** Intesa San Paolo Incident Management Team User
- Date:** Fri, Feb 7th, 2020 12:04 +01:00
- Tags:** Significant, PSD2 Submission

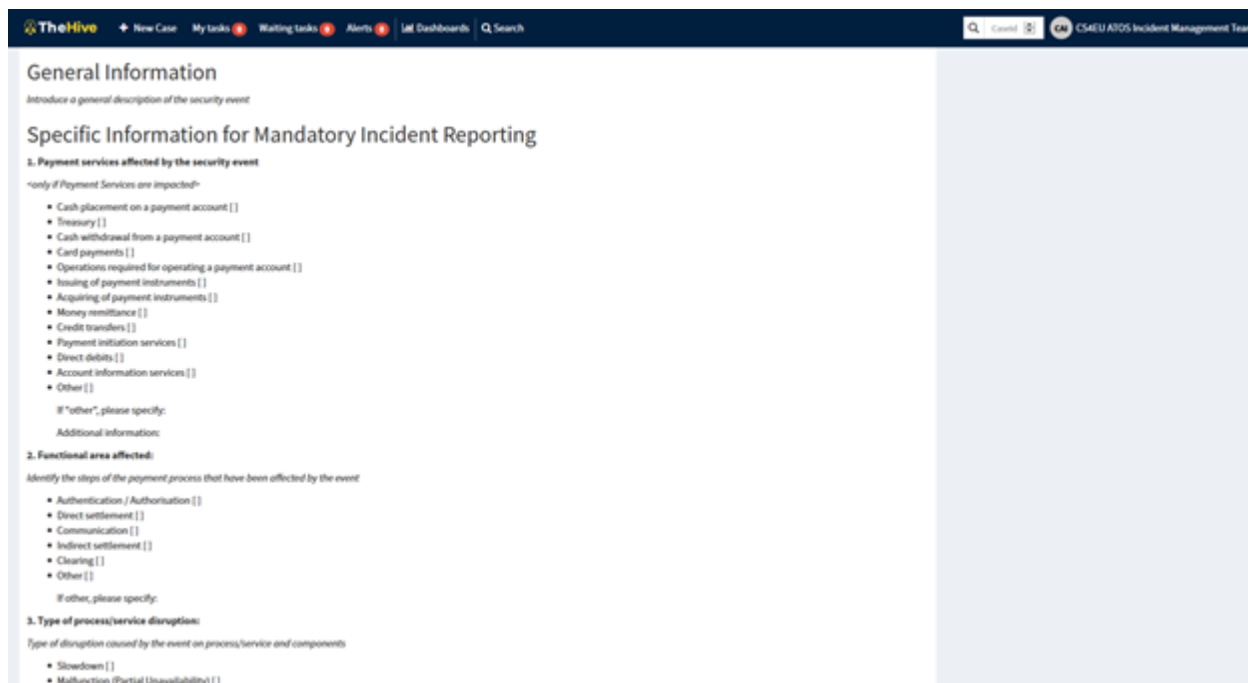
Additional information is provided for the legal entity affected:

- Name of the legal entity affected:** Gamma Bank
- Address of the legal entity affected:** Via Rossi 2, 37121, Verona (Italy)
- SWIFT / BIC code:** AAAABBCCXXX
- Event ID:** 0002
- Event Timeline: Detection:** Mon, Dec 23rd, 2019 17:15 +01:00
- Event Timeline: Occurrence:** Mon, Dec 23rd, 2019 17:15 +01:00

Metrics are currently not set.

Figure 46: Example of TheHive incident template for the IR-UC1

Furthermore, we have defined a form that has been included in the Description of the template to collect specific and additional information for mandatory incident reporting with all additional information about the incident. Some extracts of this form and included in Figure 47 and Figure 48.



The screenshot shows the "General Information" section of the TheHive form, specifically the "Specific Information for Mandatory Incident Reporting" part. The form is titled "Introduce a general description of the security event".

1. Payment services affected by the security event
<only if Payment Services are impacted>

- ☐ Cash placement on a payment account []
- ☐ Treasury []
- ☐ Cash withdrawal from a payment account []
- ☐ Card payments []
- ☐ Operations required for operating a payment account []
- ☐ Issuing of payment instruments []
- ☐ Acquiring of payment instruments []
- ☐ Money remittance []
- ☐ Credit transfers []
- ☐ Payment initiation services []
- ☐ Direct debits []
- ☐ Account information services []
- ☐ Other []

If "other", please specify:
 Additional information:

2. Functional area affected:
Identify the steps of the payment process that have been affected by the event

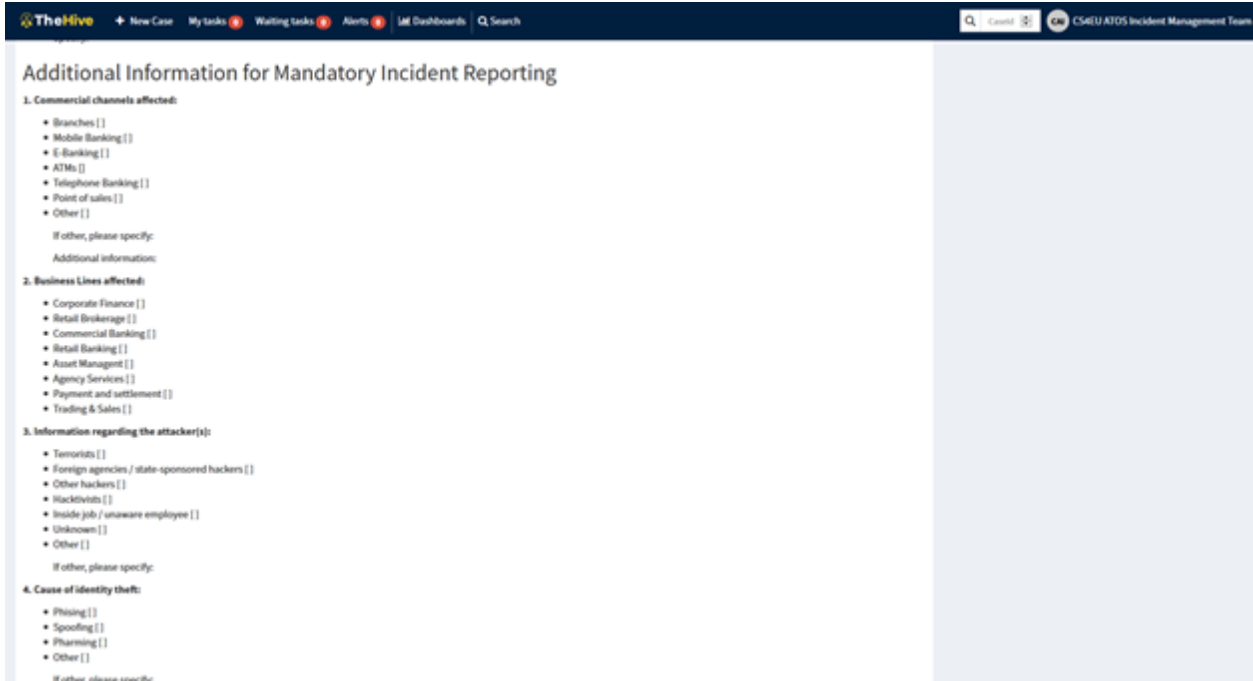
- ☐ Authentication / Authorisation []
- ☐ Direct settlement []
- ☐ Communication []
- ☐ Indirect settlement []
- ☐ Clearing []
- ☐ Other []

If other, please specify:

3. Type of process/service disruption:
Type of disruption caused by the event on process/service and components

- ☐ Slowdown []
- ☐ Malfunction (Partial Unavailability) []

Figure 47: Specific information for Mandatory Incident Reporting in TheHive template for IR-UC1



TheHive + New Case My tasks Waiting tasks Alerts L&E Dashboards Q Search CS4EU ATOS Incident Management Team

Additional Information for Mandatory Incident Reporting

1. Commercial channels affected:

- Branches []
- Mobile Banking []
- E-Banking []
- ATMs []
- Telephone Banking []
- Point of sales []
- Other []

If other, please specify:
Additional information:

2. Business Lines affected:

- Corporate Finance []
- Retail Brokerage []
- Commercial Banking []
- Retail Banking []
- Asset Management []
- Agency Services []
- Payment and settlement []
- Trading & Sales []

3. Information regarding the attacker(s):

- Terrorists []
- Foreign agencies / state-sponsored hackers []
- Other hackers []
- Hacktivists []
- Inside job / unaware employee []
- Unknown []
- Other []

If other, please specify:

4. Cause of identity theft:

- Phishing []
- Spoofing []
- Pharming []
- Other []

If other, please specify:

Figure 48: Additional information for Mandatory Incident Reporting in TheHive template for IR-UC1

5.1.5.2 Data enrichment

This functionality is supported thanks to the combination of the open sources TheHive and Cortex¹⁴. Through the GUI provided by TheHive for the case, the user can integrate in the information collected about the incidents what they call “observables”. They are for example files, IP addresses, domains or URLs related to the security incident under analysis. Cortex allows to automate the analysis of these observables by a set of analyzers enabled in the platform from the own GUI provided by TheHive. There are many open source (AGPL license) available analyzers already integrated with Cortex¹⁵ (such as Abuse_Finder, CIRCLPassive DNS, ClamAV, CuckooSandbox, DNSSinkhole, EmergingThreats, EmlParser, FileInfo, PassiveTotal, Shodan or VirusTotal, just to name some). Furthermore, new analyzers suitable for different situations can be implemented and easily integrated in Cortex and consequently in the incidents. In particular, in the current demonstrator, we have integrated the asset HADES. This is a system based on Cuckoo for the analysis of malware samples. It has been implemented by the UMA and includes the deployment of honeypots to capture malware samples and the generation of reports.

The result of the analysis performed is included in the information about the incident. See an example in Figure 49.

¹⁴ <https://github.com/TheHive-Project/Cortex>

¹⁵ <https://thehive-project.github.io/Cortex-Analyzers/>

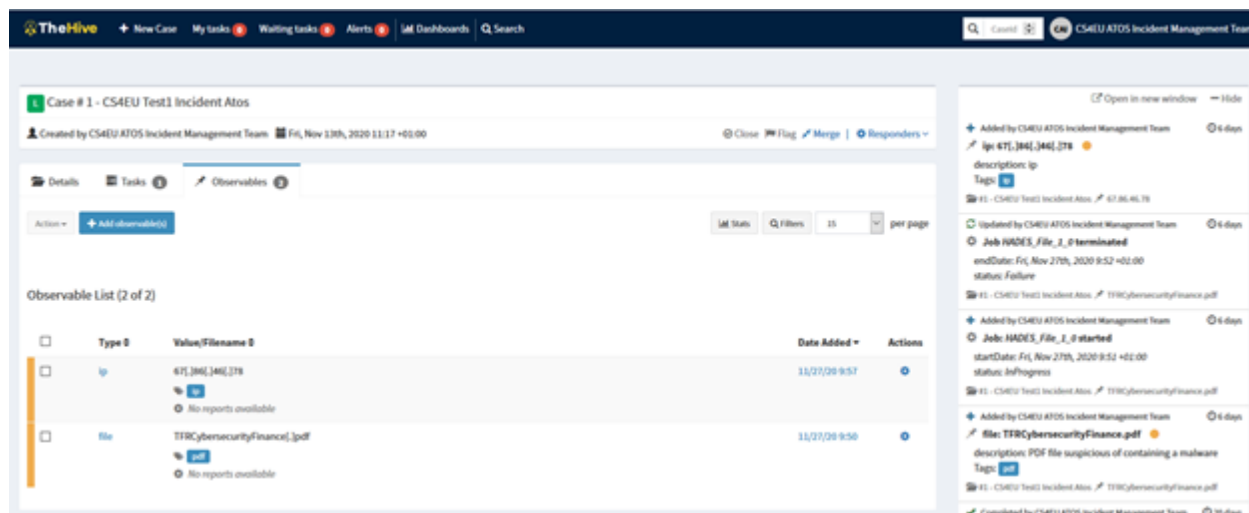


Figure 49: Observables added for data enrichment in IR-UC1

Other advantage of using TheHive is that it can be connected to one or several MISP instances so the threat intelligence data shared using this platform can be easily integrated in the information about the incident. And additionally, information about an incident registered can be shared using MISP. However, this feature will be explored in next phases of the project and they are not included in the current version of the prototype (phase1).

5.1.5.3 Incident impact assessment

Due to the lack of an asset or open source tool that implements the evaluation of the severity of the incidents, classifies them according to the criteria and thresholds defined by the different regulations we are considering in this phase of the project and determine if they need to be reported or not to the different supervisory authorities, we have developed from scratch a basic and limited event classifier for the demonstrator.

In order to integrate this functionality with the incident reporting platform, we have implemented it as a TheHive responder¹⁶. The responders are programs integrated with TheHive which receive the information about an incident registered, perform a set of actions (this is the core of the program which need to be implemented for each specific functionality) and returns a result that will be shown to the user through the graphical interface provided by TheHive.

For this demonstrator, we have implemented a responder called “CS4EU Incident Reporting Event Classifier” which takes the information about the incident and do the impact assessment according to the following subset of PSD2 and ECB/SSM criteria and thresholds. Depending on the conditions, it is determined if the incident has a lower or a higher impact:

REGULATION	CRITERIA	Thresholds
ECB / PSD2	Reputation impact	<ul style="list-style-type: none"> Lower: yes Higher: N/A

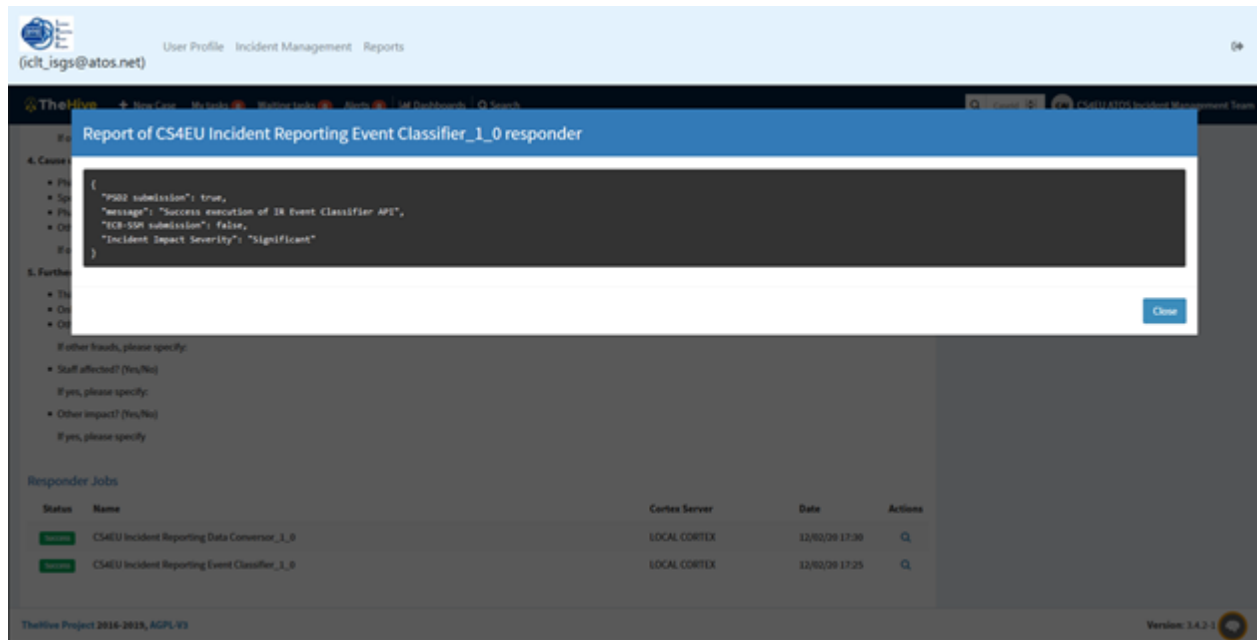
¹⁶ <https://github.com/TheHive-Project/CortexDocs/blob/master/api/how-to-create-a-responder.md>

REGULATION	CRITERIA	Thresholds
PSD2	Service downtime	<ul style="list-style-type: none"> Lower: >120 minutes Higher: N/A
PSD2	Payment Service Users (PSUs) affected	<ul style="list-style-type: none"> Lower: >5000 and >10% total Higher: >50000 or 25% total
PSD2	Transactions affected	<ul style="list-style-type: none"> Lower: >10% regular and >10000 Higher: >25% regular or >5000000

The event classifier evaluates those thresholds on the information provided by the user in the custom fields associated to those criteria and determine that a security incident is “Significant” and need to be submitted in the following cases:

- To ECB in case of one criteria is matched
- To PSD2 in case of one or more criteria at the ‘Higher impact level’, or three or more criteria at the ‘Lower impact level’

Figure 50 shows how the report is shown to the user in the demonstrator graphical interface, in this case when there is only reputational damage but the criteria related to PSD2 are not found in the incident.



The screenshot shows the TheHive web interface. At the top, there's a navigation bar with 'User Profile', 'Incident Management', and 'Reports'. Below this, a modal window titled 'Report of CS4EU Incident Reporting Event Classifier_1_0 responder' is displayed. The modal contains a JSON object:

```
{
  "PSD2 submission": true,
  "message": "Success execution of IR Event Classifier API",
  "ECB-SMR submission": false,
  "Incident Impact Severity": "Significant"
}
```

Below the JSON, there are sections for 'Further Information' with checkboxes for 'Staff affected?', 'Other impact?', and 'Other impact?'. At the bottom, there's a 'Responder Jobs' table:

Status	Name	Context Server	Date	Actions
Success	CS4EU Incident Reporting Data Converter_1_0	LOCAL CONTEXT	12/02/20 17:30	Q
Success	CS4EU Incident Reporting Event Classifier_1_0	LOCAL CONTEXT	12/02/20 17:35	Q

The footer of the interface shows 'TheHive Project 2016-2020, AGPL V3' and 'Version: 3.4.2-1'.

Figure 50: Report generated by the Incident Reporting Event Classifier in IR-UC1

5.1.5.4 Incident reporting workflow enforcement

This functionality is provided by the asset AIRE through the integration of a predefined incident reporting workflow in the open source tool TheHive. Although TheHive is a security incident response platform, there is freedom in the creation and assignement of the tasks by the different users related to a new incident registered.

The responsibility of the service aire-workflow-enforcement included in the AIRE is to manage and enforce the different stages that need to be followed in a common incident reporting workflow of a financial institution when a new security incident is detected, from the registration of it in the platform and the data gathering related to the incident, to the generation of the reports that will need to be sent to the supervisory authorities. And each of these phases will need to be done by users with a different role and following a 4-eye principle with managerial judgement to prevent accidental reporting.

The service aire-workflow-enforcement integrates the light-weight workflow engine Activiti¹⁷ to follow the workflow defined in Business Process Model and Notation (BPMN) file which tries to harmonize the different incident reporting procedures currently existing according to the different regulatory frameworks applicable to the financial institutions. In the current prototype, we have focused only in the workflow required for the generation of a the first mandatory report according to PSD2 and ECB regulations. We foresee to extend it until the end of the project to support also the intermedium and final reports, and extend it to other regulatory frameworks.

The interaction between the aire-workflow-enforcement service and TheHive is done through the service aire-thehive-plugin, also included in the asset AIRE. This asset has been designed in this way so it can be flexible enough to have the possibility in the future to evolve and integrate with other incident management tools different from TheHive. The interaction between the two services included in the asset AIRE is done through REST APIs and the same with the interaction with TheHive.

In particular, the aire-thehive-plugin service is in charge of the following functionalities:

1. Receive in real-time any action performed in the tool TheHive. The service offers an API as a webhook collector that will receive the webhooks generated automatically by TheHive with any action (a new case registered, a field updated, a responder executed, a task closed, etc).

The webhooks received are analysed and translated to invocations to the API provided by the aire-workflow-enforcement service. For example, when a new incident is created, it is translated to an incident according to the data model we have defined in the demonstrator, it is stored in the Incident Register database, and the aire-workflow-enforcement api is invoked to start a new incident reporting workflow process. And when a task is closed, it is also invoked the aire-workflow-enforcement api to move the incident associated to that task to the next step in the workflow. It is responsibility of the workflow enforcement to check if the user has permissions to close the task and actuate in consequence.

2. Execute actions on the TheHive using the API REST provided by this open source tool. This is invoked for example by the aire-workflow-enforcement in each stage of the workflow defined by the incident reporting BPMN file to create the tasks associated to that stage and to assign them to the right user. The relationship between workflow stages, tasks and users allowed is defined in configuration file so they can be adapted if required.

¹⁷ <https://www.activiti.org/>

3. Receive requests from the TheHive responders included in the demonstrator to check if the user who invoked them has permissions to proceed with the execution of the tasks performed by the responders on a specific incident depending on the stage it is in the incident reporting workflow. These requests will be resent to the aire-workflow-enforcement service with the incident associated to the TheHive case where the responders were launched.

5.1.6 Quality Indicators

5.1.6.1 Effectiveness and efficiency of the solution

In the Incident Reporting for financial institutions demonstrator we have evaluated the following indicators which correspond to the following subcategories:

- integration and interoperability (KPI_QAI_*)
- documentation (KPI_QAD*)
- usability (KPI_QAU_*)
- source code management (KPI_QASCM_*)
- deployment (KPI_QAR*)

Indicator	Description	Evaluation
KPI_QAI_01	Both, the asset AIRE and the open source tool TheHive included in the incident reporting platform demonstrator offer JSON-based REST APIs to invoke the different main functionalities (e.g. to register a new incident in the reporting workflow process or to generate an Excel report for a specific incident registered in the Incident Register database)	OK
KPI_QAI_02	It is foreseen to provide support for SSO through the integration of the GUI provided by the asset AIRE and the open source TheHive with Keycloak, but it will be done during next phase.	NOK
KPI_QAD_01	The demonstrator includes a user manual documentation. Since at	OK

Indicator	Description	Evaluation
	this stage of the project the demonstrator has been installed only on the developer partner premises, documentation about installation, configuration and integration of the different components have not been delivered to the end-user for validation. However, the asset AIRE and the open source tool TheHive included in the demonstrator provide README files with documentation about installation, configuration and administration. And it is foreseen to provide the installation manuals for next phase so the end-users can do a deployment “in house” on the FI premises as established in requirement IR-OP01.	
KPI_QAD_02	The APIs provided by the asset AIRE and the open source tool TheHive included in the demonstrator are specified and documented. The asset AIRE also provides a Swagger specification.	OK
KPI_QAD_03	No additional documentation such as examples or tutorials about the demonstrator are available yet.	NOK
KPI_QAU_01	Minimal browser support is provided for the demonstrator. Validation has been done with Firefox, but it has been also verified access using Chrome and Internet Explorer. Let’s Encrypt ¹⁸ SSL certificates have been included to avoid issues	OK

¹⁸ <https://letsencrypt.org/es/>

Indicator	Description	Evaluation
	with self-signed certificates detected during the validation.	
KPI_QAU_02	Multi-platform support and responsiveness for the UI have not been validated at this phase of the demonstrator. The main GUI of the demonstrator is implemented in Django ¹⁹ so it should support any platform supported by Django.	NOK
KPI_QAU_03	Internationalization is not supported by the demonstrator yet and the open source tool TheHive included in the demonstrator does not provide this feature. However, the GUI provided by the asset AIRE is implemented in Django which has support for internationalization ²⁰ , so we foresee to include this feature by the end of the project at least in the main menu of the demonstrator.	NOK
KPI_QASCM_01	The asset AIRE included in the demonstrator make use of SCM and issue tracking through GitLab hosted by ATOS. The open source TheHive also used in the demonstrator uses GitHub (https://github.com/TheHive-Project/TheHive)	OK
KPI_QAR_01	All the components included in the demonstrator (asset AIRE and TheHive with the extensions	OK

¹⁹ <https://www.djangoproject.com/>

²⁰ <https://docs.djangoproject.com/en/3.1/topics/i18n/>

Indicator	Description	Evaluation
	developed) are provided as docker containers.	

5.1.6.2 User and stakeholder engagement and impact evaluation

The evaluation of the users and stakeholders engagement as well as the impact the incident reporting platform developed in this Use Case can have, will not be done at this stage of the demonstrator (phase1).

At this stage of the development the validation has been done by the stakeholders participating in the project, that can validate if the development arranged gives the results expected during the design of the prototype. The validation is a technological testing of the functionality of the tool. For this reason, the better user to test it are the users of the Financial Institutions involved in the development, being also involved in departments in charge of the Incident Reporting in their Organizations. These end users are in the same way the correct people to evaluate the impacts in the Incident Reporting process of the usage of the tool and the real needs to be accomplished. These evaluations will be done at the end of the development of the Incident Reporting Platform.

5.1.7 Requirements Coverage

The following table shows the requirements that have been validated in this Use Case and the results of the validation.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-F02	Yes	Test Case 1-UC1, Test Case 2-UC1	Success	Yes	All the information required related to the cyber incident is collected through different questionnaires.
IR-F03	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The platform supports to include new templates with the information that need to be included in the reports. But it is not implemented yet the

ID	Validated	Strategy	Result	Mandatory	Comments
					possibility to upload/download them from the GUI.
IR-F04	Partially	Test Case 3-UC1	Success	Yes	<p>Functionality partially covered by the responder Event Classifier included in the demonstrator.</p> <p>It only covers a subset of the criteria and thresholds related to PSD2 and ECB for validation purposes.</p>
IR-F05	Partially	Test Case 3-UC1	Success	Yes	<p>Functionality partially covered by the responder Event Classifier included in the demonstrator.</p> <p>It only covers a subset of the criteria and thresholds related to PSD2 and ECB for validation purposes.</p>
IR-F06	Partially	Test Case 3-UC1	Success	Yes	The demonstrator identifies the need for mandatory incident

ID	Validated	Strategy	Result	Mandatory	Comments
					reporting, but it only covers a subset of the criteria and thresholds related to PSD2 and ECB for validation purposes (not all the reporting requirements and related assessment methodologies).
IR-F07	Yes	Test Case 1-UC1, Test Case 2-UC1, Test Case 3-UC1	Success	Yes	<p>The demonstrator suggests the operator the mandatory incident reporting processes to be followed.</p> <p>Different tasks are created in TheHive to indicate the incident reporting process to be followed by the users depending on their functions.</p>
IR-F12	Partially	Test Case 1-UC1, Test Case 2-UC1, Test Case 3-UC1	Success	Yes	The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The

ID	Validated	Strategy	Result	Mandatory	Comments
					tracking is shown in real-time through the capabilities provided by TheHive GUI. However, it is not stored in the Incident Register database yet.
IR-F13	Yes	Test Case 1-UC1, Test Case 2-UC1, Test Case 3-UC1	Success	Yes	An incident reporting workflow is enforced in the demonstrator, creating and assigning the tasks in TheHive that the users need to do depending on their roles.
IR-F14	Partially	Technology based	Success	Yes	It is possible to configure for each stage in the workflow what are the tasks created, the description shown in each of them, the user assigned and the tags shown in the incident. But it is not possible to change the Incident Reporting Workflow by the system administrator

ID	Validated	Strategy	Result	Mandatory	Comments
					without changing the BPMN file and recompiling the code in the demonstrator.
IR-F15	Partially	Test Case 3-UC1	Success	Yes	Functionality partially covered only for criteria and thresholds related to PSD2 and ECB. There is no asset implementing IR-F04 and IR-F05 based on configurable criteria and thresholds.
IR-F17	No	N/A	N/A	No	The demonstrator does not contain a report module that allows access to the information on the number of incidents that occurred in a given time.
IR-F18	No	N/A	N/A	No	The demonstrator does not provide a section where the variables that are going to be present in the creation of the incidents

ID	Validated	Strategy	Result	Mandatory	Comments
					can be configured.
IR-F19	Partially	Technology based	Success	Yes	<p>Each application included in the demonstrator has log files with all the actions performed in the demonstrator as well as errors/messages.</p> <p>They are saved in the system and are also available through the docker containers logs.</p> <p>Log files with actions performed by the user using the application will be added in next phases of the demonstrator.</p>
IR-F20	Partially	Test Case 1-UC1	Success	No	<p>Tooltips with help information are shown in each option of the GUI menu to help the user to understand the actions available.</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					However, a help button has not been included for each screen in the graphical interface.
IR-F21	No	N/A	N/A	No	No regulatory wiki has been included in the demonstrator.
IR-F22	Partially	Test Case 1-UC1	Success	No	There is a Help section in the main GUI where users can find the direct link to mandatory incident reporting regulations, guidelines and directives related to ECB and PSD2.
IR-F23	Partially	Test Case 1-UC1	Success	Yes	The administrator can create/modify/delete users and assign them a function. However it is not possible to assign the same permissions into TheHive tool, so the users are created with default

ID	Validated	Strategy	Result	Mandatory	Comments
					read/write permissions.
IR-F24	No	N/A	N/A	No	The demonstrator does not include the possibility to create and process rules able to identify and notify specific conditions for monitoring user activities.
IR-F25	Yes	Technology based	Success	Yes	The components used in the demonstrator include REST APIs that allow integration with third-party technologies.
IR-SP01	Yes	Test Case 1-UC1	Fail	Yes	The authentication mechanism to access the demonstrator is based on username and password. Strong authentication mechanisms have not been implemented in the demonstrator.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-SP02	Partially	Test Case 1-UC1, Test Case 2-UC1	Success	Yes	<p>The demonstrator grants access to information on a need to know base and matching authorisation profiles. The information shown to the user in the GUI is different depending on his/her profile.</p> <p>At the end of the project, when all the information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the demonstrator is focused on the first Mandatory Report).</p>
IR-SP03	Partially	Test Case 1-UC1, Test Case 2-UC1	Success	Yes	<p>The demonstrator ensures that the information needed is made available.</p> <p>At the end of the project, when all the</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the demonstrator is focused on the first Mandatory Report).
IR-SP04	Yes	Test Case 1-UC1	Success	Yes	There is a section in the demonstrator GUI to configure users and their functions, in order to ensure limiting or granting permissions to each user based on their functions.
IR-SP05	Partially	Technology based	Success	Yes	The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The tracking is shown in real-time through

ID	Validated	Strategy	Result	Mandatory	Comments
					the capabilities provided by TheHive GUI. However, it is not stored in the Incident Register database yet.
IR-LF01	Yes	Test Case 1-UC1, Test Case 2-UC1	Success	Yes	The demonstrator includes a GUI that allows the interaction with the operator
IR-LF02	Yes	Test Case 1-UC1, Test Case 2-UC1	Fail	No	The GUI currently included in the demonstrator only supports English language.
IR-U01	Partially	Test Case 1-UC1, Test Case 2-UC1, Test Case 3-UC1	Success	Yes	The GUI should be improved to guarantee that is user-friendly, offers a better user experience, improves the response times and facilitates the navigation between the different functionalities.
IR-U02	Partially	Test Case 1-UC1, Test Case 2-UC1 Test Case 3-UC1	Success	Yes	The GUI allows the user to include all the required information to generate the first mandatory

ID	Validated	Strategy	Result	Mandatory	Comments
					report under ECB and PSD2. It will need to be completed with the data required for intermedium and final reports.
IR-U03	Yes	Test Case 1-UC1, Test Case 2-UC1	Fail	Yes	The questionnaires presented to the users of the demonstrator are not self-adaptive. They are not customized depending on the information already provided about the incident.
IR-OP01	Yes	Technology based	Success	Yes	The Incident Reporting Platform will be an “in house” standalone application deployed on the FI premises.
IR-OP02	No	N/A	N/A	No	The demonstrator does not include the possibility of selecting currency in the creation of the incidents.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-OP03	No	N/A	N/A	No	The demonstrator supports multiple time zones.
IR-OP04	No	N/A	N/A	No	The demonstrator does not include business calendars.
IR-MP01	Yes	Test Case 1-UC	Success	Yes	The demonstrator includes configuration mechanisms for incorporating additional regulations that may have effect in different sectors.
IR-MP02	Yes	Test Case 1-UC1	Success	Yes	The demonstrator has been 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-LR01	No	N/A	N/A	Yes	Incident reporting requirements established by the NIS Directive for

ID	Validated	Strategy	Result	Mandatory	Comments
					Operators of Essential Services have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR02	No	N/A	N/A	Yes	Incident reporting requirements established by the EU privacy regulation (GDPR) have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR03	No	N/A	N/A	Yes	ENISA Guidance on Incident reporting for eIDAS have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR04	Yes	Test Case 1-UC1, Test Case 2-UC1	Success	Yes	Incident reporting requirements established by

ID	Validated	Strategy	Result	Mandatory	Comments
		Test Case 3-UC1			the ECB framework have been considered in the demonstrator.
IR-LR05	Yes	Test Case 1-UC1, Test Case 2-UC1 Test Case 3-UC1	Success	Yes	Incident reporting requirements established by the Payment Services Directive PSD2 have been considered in the demonstrator.
IR-LR06	No	N/A	N/A	Yes	Incident reporting requirements related to Target2 system have not been considered in the demonstrator, as they are not included in the scope of this phase.

Table 15: Incident Reporting – IR-UC1 Validation Requirements' Coverage.

5.2 Use Case IR-UC2: Managerial Judgement

The main objective of this Use Case is to validate the effective possibility for the Controller to perform the Managerial Judgement about the incident classification. The Incident Reporting Platform must give the Controller the possibility to confirm, increase or lower the Incident Severity Level, as well as the possibility to confirm the need for Incident Reporting suggested by the demonstrator.

This Use Case will be successfully validated if the decision taken by the Controller is reflected in the incident reporting workflow, to proceed with the reporting to the competent authorities or to go back to the previous stage of “Data Enrichment”.

The validation strategy has included the validation of functional requirements, security and privacy requirements and non-functional requirements, such as look and feel requirements, usability requirements,

operational requirements, maintainability and portability requirements and legal and regulatory requirements.

The validation has been performed through the execution of the four different test scenarios of potential security incidents detected in a financial entity described in 5.1.2.1.

5.2.1 Actors

The validation of this Use Case has been carried out by the two end-users involved in Task 5.4, BBVA and Intesa Sanpaolo. In this particular Use Case, they represent users from their respective organizations playing the role of Controller.

The validation of the quality indicators has been performed by the technology owner, ATOS.

5.2.2 Test Case 1 UC2: Managerial Judgement

5.2.2.1 Description

As it was described in D5.1 for the use case, Test Case 1 covers the authorization process in which the Controller performs the Managerial Judgement about the incident classification. In this test case, the Controller will confirm or not the incident severity level and the need for mandatory incident reporting suggested by the platform. With this purpose, the Controller will base on his/her experience and further considerations to analyse the specificities and details of the incident to determine the overall level of severity through a Managerial Judgement, confirming, increasing or lowering the values suggested by the Incident Reporting Platform.

Based on the assigned Incident Impact Severity, the most appropriate action plan to be implemented to handle and respond to the incident will be determined by the platform according to the predefined incident reporting workflow.

5.2.2.2 Test Case Workflow

Once the security incident has been classified, the next step in the workflow is the Managerial Judgement done by the Controller.

First of all, the Controller has to check all the information about the incident that has been included in the Incident Reporting Platform. Under the menu “Managerial Judgement”, the Controller can see the report with the Impact Classification. Selecting the option “Details” (the image of an eye), the Managerial Judgement Form is shown, detailing the Event Severity Classification and the suggested mandatory reporting based on the criteria of the regulations included in the scope of Phase 1 (PSD2 and the ECB/SSM framework).

The Incident Reporting Platform also shows the authorities the Initial Report has to be sent to (European Central Bank, National Central Bank, National CSIRT,...).

The Controller has to confirm the options suggested by the Incident Reporting Platform or change them, in case it is necessary. Therefore, the Controller has the possibility to confirm, increase or lower the Incident Severity Level, as well as to confirm the need for Incident Reporting suggested by the demonstrator.

Once the Managerial Judgement has been done, the Controller has to select the option “Submit” and close the task “Managerial Judgement”.

5.2.2.3 Test Results

The results of Test Case 1 have shown that the Incident Reporting Platform gives the Controller the effective possibility to perform the Managerial Judgement about the incident classification. The Controller can visualize the result of the classification (Significant or not Significant depending on the different scenarios) and has the possibility to confirm it, as well as to confirm the need for Incident Reporting suggested by the demonstrator.

It has also been verified that the decision taken by the Controller is reflected in the incident reporting workflow to proceed with the reporting to the competent authorities or to go back to the previous stage of “Data Enrichment”. Automatically it is closed the task “Managerial Judgement” and the next task “Data Conversion” is created to continue with the processing.

5.2.3 Technology Based Analysis

This Use Case validates the Managerial Judgement functionality of the demonstrator that is described below.

5.2.3.1 Managerial Judgement

The managerial judgement is integrated in the incident reporting workflow BPMN file as “User Tasks”. This means that they are steps requiring interaction with the user, in this case a user with the role of Controller. This interaction is performed through forms integrated in the demonstrator GUI. In particular, we have included two different managerial judgement forms:

1. Form to confirm the incident impact classification suggested by the platform (see Figure 51) and the reports that need to be submitted according to the regulations enabled in the platform

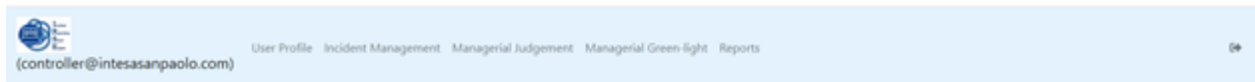
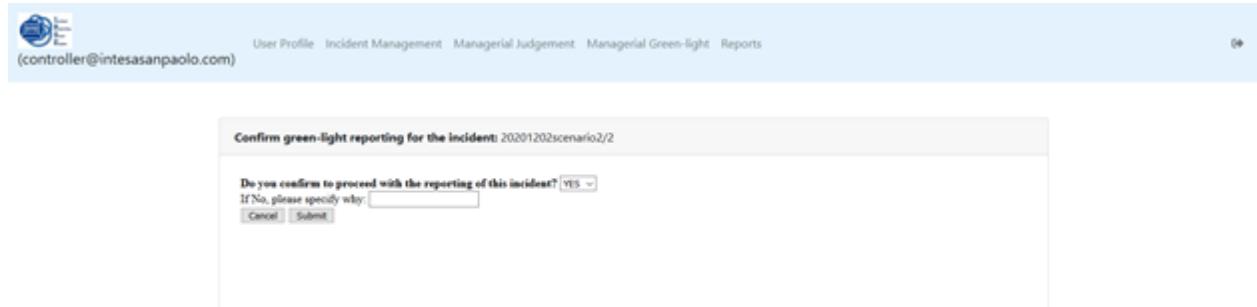


Figure 51: Managerial judgement form (IR-UC2)

2. Form to confirm green-light to proceed with the reporting once the reports have been generated by the platform (see use case IR-UC3).



The screenshot shows a web interface for 'User Profile Incident Management Managerial Judgement Managerial Green-light Reports'. The user is logged in as '(controller@intesasanpaolo.com)'. A modal window titled 'Confirm green-light reporting for the incident: 20201202scenario2/2' is displayed. It contains the question 'Do you confirm to proceed with the reporting of this incident?' with a 'YES' dropdown menu. Below this is a text input field for 'If No, please specify why:'. At the bottom of the modal are 'Cancel' and 'Submit' buttons.

Figure 52: Green-light managerial judgement (IR-UC2)

In these cases, the tasks associated to these steps in incident shown in the graphical interface of TheHive are automatically closed once the user has completed and submitted the form.

5.2.4 Quality Indicators

5.2.4.1 Effectiveness and efficiency of the solution

The indicators evaluated in this use case are the same described in section 5.1.6.1.

5.2.4.2 User and stakeholder engagement and impact evaluation

The evaluation of the users and stakeholders engagement as well as the impact the incident reporting platform developed in this Use Case can have, will not be done at this stage of the demonstrator (phase1).

At this stage of the development the validation has been done by the stakeholders participating in the project, that can validate if the development arranged gives the results expected during the design of the prototype. The validation is a technological testing of the functionality of the tool. For this reason, the better user to test it are the users of the Financial Institutions involved in the development, being also involved in departments in charge of the Incident Reporting in their Organizations. These end users are in the same way the correct people to evaluate the impacts in the Incident Reporting process of the usage of the tool and the real needs to be accomplished. These evaluations will be done at the end of the development of the Incident Reporting Platform.

5.2.5 Requirements Coverage

The following table shows the requirements that have been validated in this Use Case and the results of the validation.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-F01	Yes	Test Case 1-UC2	Success	Yes	The Managerial Judgement form included in the demonstrator guarantees that the Mandatory Incident Reporting is not automatic, to prevent accidental reporting (4eye principle).
IR-F08	Yes	Test Case 1-UC2	Success	Yes	The demonstrator requests the authorization of the FI operator (Controller) to proceed with the reporting.
IR-F12	Partially	Test Case 1-UC2	Success	Yes	The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The tracking is shown in real-time through the capabilities provided by TheHive GUI. However, it is

ID	Validated	Strategy	Result	Mandatory	Comments
					not stored in the Incident Register database yet.
IR-F13	Yes	Test Case 1-UC2	Success	Yes	An incident reporting workflow is enforced in the demonstrator, creating and assigning the tasks in TheHive that the users need to do depending on their roles.
IR-F14	Partially	Technology based	Success	Yes	It is possible to configure for each stage in the workflow what are the tasks created, the description shown in each of them, the user assigned and the tags shown in the incident. But it is not possible to change the Incident Reporting Workflow by the system administrator without changing the BPMN file and recompiling the code in the demonstrator.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-F15	Partially	Test Case 1-UC2	Success	Yes	Functionality partially covered only for criteria and thresholds related to PSD2 and ECB. There is no asset implementing IR-F04 and IR-F05 based on configurable criteria and thresholds.
IR-F17	No	N/A	N/A	No	The demonstrator does not contain a report module that allows access to the information on the number of incidents that occurred in a given time.
IR-F18	No	N/A	N/A	No	The demonstrator does not provide a section where the variables that are going to be present in the creation of the incidents can be configured.
IR-F19	Yes	Technology based	Success	Yes	Each application included in the demonstrator has log files

ID	Validated	Strategy	Result	Mandatory	Comments
					<p>with all the actions performed in the demonstrator as well as errors/messages.</p> <p>They are saved in the system and are also available through the docker containers logs.</p> <p>Log files with actions performed by the user using the application will be added in next phases of the demonstrator.</p>
IR-F20	Partially	Test Case 1-UC2	Success	No	<p>Tooltips with help information are shown in each option of the GUI menu to help the user to understand the actions available.</p> <p>However, a help button has not been included for each screen in the graphical interface.</p>

ID	Validated	Strategy	Result	Mandatory	Comments
IR-F21	No	N/A	N/A	No	No regulatory wiki has been included in the demonstrator.
IR-F22	Partially	Test Case 1-UC2	Success	No	There is a Help section in main GUI where users can find the direct link to mandatory incident reporting regulations, guidelines and directives related to ECB and PSD2.
IR-F23	Partially	Test Case 1-UC2	Success	Yes	The administrator can create/modify/delete users and assign them a function. However it is not possible to assign the same permissions into TheHive tool, so the users are created with default read/write permissions.
IR-F24	No	N/A	N/A	No	The demonstrator does not include the possibility to create and process rules

ID	Validated	Strategy	Result	Mandatory	Comments
					able to identify and notify specific conditions for monitoring user activities.
IR-F25	Yes	Technology based	Success	Yes	The components used in the demonstrator include REST APIs that allow integration with third-party technologies.
IR-SP01	Yes	Test Case 1-UC2	Fail	Yes	The authentication mechanism to access the demonstrator is based on username and password. Strong authentication mechanisms have not been implemented in the demonstrator.
IR-SP02	Partially	Test Case 1-UC2	Success	Yes	The demonstrator grants access to information on a need to know base and matching authorisation profiles. The information shown to the user in the GUI

ID	Validated	Strategy	Result	Mandatory	Comments
					<p>is different depending on his/her profile.</p> <p>At the end of the project, when all the information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the demonstrator is focused on the first Mandatory Report).</p>
IR-SP03	Partially	Test Case 1-UC2	Success	Yes	<p>The demonstrator ensures that the information needed is made available.</p> <p>At the end of the project, when all the information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					demonstrator is focused on the first Mandatory Report).
IR-SP04	Yes	Test Case 1-UC2	Success	Yes	There is a section in the demonstrator GUI to configure users and their functions, in order to ensure limiting or granting permissions to each user based on their functions.
IR-SP05	Partially	Technology based	Success	Yes	<p>Logging, timestamping and tracking mechanisms have been incorporated at all phases of the Incident Reporting process.</p> <p>The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The tracking is shown in real-time through the capabilities provided by TheHive GUI.</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					However, it is not stored in the Incident Register database yet.
IR-LF01	Yes	Test Case 1-UC2	Success	Yes	The demonstrator includes a GUI that allows the interaction with the operator
IR-LF02	Yes	Test Case 1-UC2	Fail	No	The GUI currently included in the demonstrator only supports English language.
IR-U01	Partially	Test Case 1-UC2	Success	Yes	The GUI can be improved to guarantee that is user-friendly, offers a better user experience, improves the response times and facilitates the navigation between the different functionalities.
IR-OP01	Yes	Technology based	Success	Yes	The Incident Reporting Platform will be an “in house” standalone application deployed on the FI premises.

ID	Validated	Strategy	Result	Mandatory	Comments
IR-OP03	Yes	Technology based	Success	No	The demonstrator supports multiple time zones.
IR-OP04	Yes	Technology based	Success	No	The demonstrator is able to consider different business calendars.
IR-MP01	Yes	Test Case 1-UC2	Success	Yes	The demonstrator includes configuration mechanisms for incorporating additional regulations that may have effect in different sectors
IR-MP02	Yes	Test Case 1-UC2	Success	Yes	The demonstrator has been 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-LR01	No	N/A	N/A	Yes	Incident reporting requirements established by

ID	Validated	Strategy	Result	Mandatory	Comments
					the NIS Directive for Operators of Essential Services have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR02	No	N/A	N/A	Yes	Incident reporting requirements established by the EU privacy regulation (GDPR) have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR03	No	N/A	N/A	Yes	ENISA Guidance on Incident reporting for eIDAS have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR04	Yes	Test Case 1-UC2	Success	Yes	Incident reporting requirements established by

ID	Validated	Strategy	Result	Mandatory	Comments
					the ECB framework have been considered in the demonstrator.
IR-LR05	Yes	Test Case 1-UC2	Success	Yes	Incident reporting requirements established by the Payment Services Directive PSD2 have been considered in the demonstrator.
IR-LR06	No	N/A	N/A	Yes	Incident reporting requirements related to Target2 system have not been considered in the demonstrator, as they are not included in the scope of this phase.

Table 16: Incident Reporting – IR-UC2 Validation Requirements' Coverage

5.3 Use Case IR-UC3: Data Conversion and reporting preparation

The main objective of this Use Case is to validate if the Incident Reporting demonstrator includes all the needed information into the appropriate template/communication to be sent to the Competent Authority. The tool must be able to convert the data collected in the previous phases (Use Case 1) into the appropriate formats and templates required by the Competent Authorities, depending on the nature of the incident. Besides, the tool must be able to perform the actual reporting once the Controller has authorized it.

The validation strategy will include the validation of functional requirements, security and privacy requirements and non-functional requirements, such as look and feel requirements and usability requirements, through the execution of different test scenarios of potential security incidents detected in a financial entity. This use case will be successfully validated if the reports associated to the two regulatory frameworks considered in this phase 1 (PSD2 and ECB) are generated and populated with the information about the incident registered in the platform in the execution of the user case IR-UC1. The reports generated will be sent by email to the Incident Reporting Team (IRT); when the report is validated the IRT proceed with the reporting and releasing of the incident report to the competent Authority.

5.3.1 Actors

The validation of this Use Case will be carried out by the two end-users involved in Task 5.4, BBVA and Intesa Sanpaolo. In this particular use case, they represent users from their respective organizations playing the following roles:

- Controller
- Incident Reporting Team (IRT)

The validation of the quality indicators has been performed by the technology owner, ATOS.

5.3.2 Test Case 1-UC3: Data conversion and reporting preparation to ECB

5.3.2.1 Description

The test case 1-UC3 aims at verifying the automatic generation of the correct template for ECB Authority. The tool must be able to convert data collected in the previous phases (Use Case 1) into the appropriate format and template required by the Authority. The prototype must be able to collect all necessary information to fill in the correspondent sections of the template. In phase 1 it is released only the first report. The first report must have the information about the Financial Institution which identify it, included references of the contact persons. It also provides the incident detection date and a general description of the incident, in a free field. The tests executed aim at verify that the prototype is able to find and report all required information in the correspondent fields in the correspondent template.

This test case is associated to the requirement IR-F09 - It must produce the appropriate template and communication, in the appropriate format to be sent to the Competent Authority.

The validation has been performed through the execution of the tests scenarios 1 and 3 described in 5.1.2.1.

5.3.2.2 Test Case Workflow

The Use Case 3 starts with the data conversion. The task is assigned to the Incident Reporting Team (IRT) that can add additional necessary data for the preparation of the template. Then, the IRT launches the data conversion invoking the responder “Incident Reporting Data Conversor”; it lets the tool able to put the correspondent data in the template and generate the template file. The file is sent to the Incident Reporting Team (IRT); the IRT must validate the written up template closing the task “Data Conversion”; after doing it, the user with role of Controller will confirm if it is possible to proceed with the reporting of that report to the Authority. The Controller will use the platform tab “Managerial Green light” and confirm to proceed with the reporting. After this authorization, the task “Reporting & Releasing” is opened and the Incident Reporting Team can send the template to the correspondent Authority. It is done out of the tool but after doing it, the IRT will have to close the task “Reporting & Releasing” of the tool to proceed with the incident

reporting workflow and then, the report will appear in the dashboard as reported. At this stage, the workflow can start again with the “data enrichment” stage aims at preparing the intermediate template.

5.3.2.3 Test Results

Test conducted confirmed the correct compilation of the ECB template with the data about the Financial Institution. There are correctly reported the name of the Financial Institution, the type of the entity (supervised by SSM), the country of the entity affected, the contact references, primary and secondary contact (name, email and telephone number) and the incident detection date and hours.

It will be detected in phase 2 the possibility of filling in automatically the templates with a more detailed general description of the incident reported in the correspondent field. The field in which describe the incident is present in all three templates, first, intermediate and final.

5.3.3 Test Case 2-UC3: Data conversion and reporting preparation for PSD2

5.3.3.1 Description

Test case 2-UC3 aims at verifying the automatic generation of the correct template for PSD2 Regulation. The tool must be able to convert the data collected in the previous phases (Use Case 1) into the appropriate format and template required by the Authority. The prototype must be able to collect all necessary information to fill in the correspondent sections of the template. In phase one it is released only the first report. The first report must have the information about the Financial Institution which identify it, included references of the contact persons. It also provides the incident detection date, the incident detector and a general description of the incident, in a free field. The tests executed aim at verify that the prototype is able to find and report all required information in the correspondent fields in the correspondent template.

This test case is associated to the requirement IR-F09 - It must produce the appropriate template and communication, in the appropriate format to be sent to the Competent Authority.

The validation has been performed through the execution of the tests scenarios 2 and 3 described in 5.1.2.1.

5.3.3.2 Test Case Workflow

The Use Case 3 starts with the data conversion. The task is assigned to the Incident Reporting Team (IRT) that can add additional necessary data for the preparation of the template. Then, the IRT launches the data conversion invoking the responder “Incident Reporting Data Conversor”; it lets the tool able to put the correspondent data in the template and generate the template file. The file is sent to the Incident Reporting Team (IRT); the IRT must validate the written up template closing the task “Data Conversion”; after doing it, the user with role of Controller confirm if it is possible to proceed with the reporting of that report to the Authority. The Controller uses the platform tab “Managerial Green light” and confirm to proceed with the reporting. After this authorization, the task “Reporting & Releasing” is opened and the Incident Reporting Team can send the template to the correspondent Authority. It is done out of the tool but after doing it, the IRT will have to close the task “Reporting & Releasing” of the tool to proceed with the incident reporting workflow and then, the report will appear in the dashboard as reported. At this stage the workflow can start again with the “data enrichment” stage aims at preparing the intermediate template.

5.3.3.3 Test Results

Tests conducted confirmed the correct compilation of the PSD2 template with the data about the Financial Institution affected, the name of the Financial Institution, the country of the entity, the contact references, primary and secondary contact (name, email and telephone number). Are also present the incident detection date and hours and who detected the event.

It will be detected in phase 2 the possibility of filling in the templates with the general description of the incident reported in the correspondent field. The field in which describe the incident is present in all three templates, first, intermediate and final.

5.3.4 Technology Based Analysis

This Use Case validates the capability of the demonstrator to convert the data collected about the incidents and generate reports based on different templates and formats.

5.3.4.1 Data conversion and generation of reports

The main functionality covered by this use case is the automatic generation of the incidents reports according to the different templates associated to the mandatory incident reporting procedures defined in PSD2 and ECB. Although the data model and the graphical interface are prepared to define different formats of templates for the reports in the platform, this demonstrator is focused on the generation of Excel reports since this is the format required by these regulations.

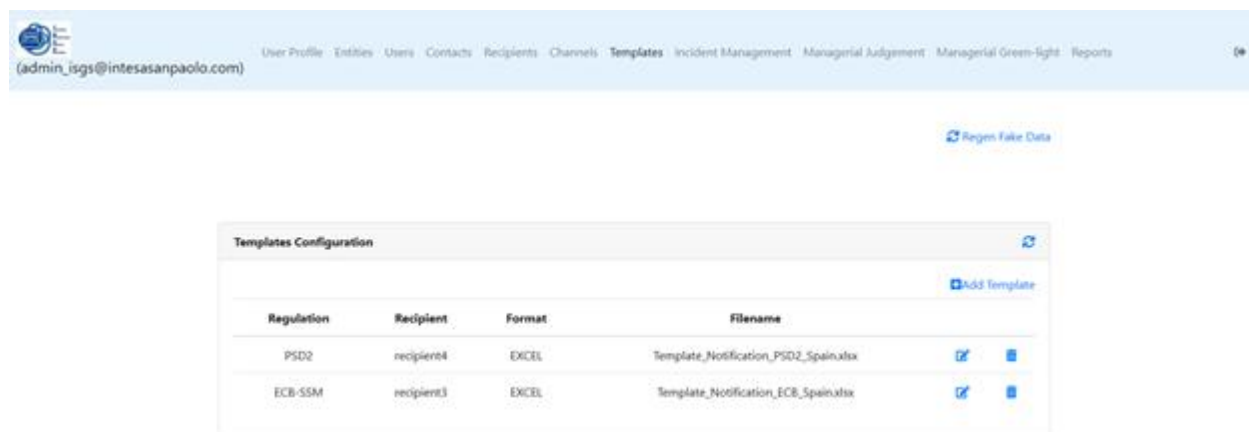


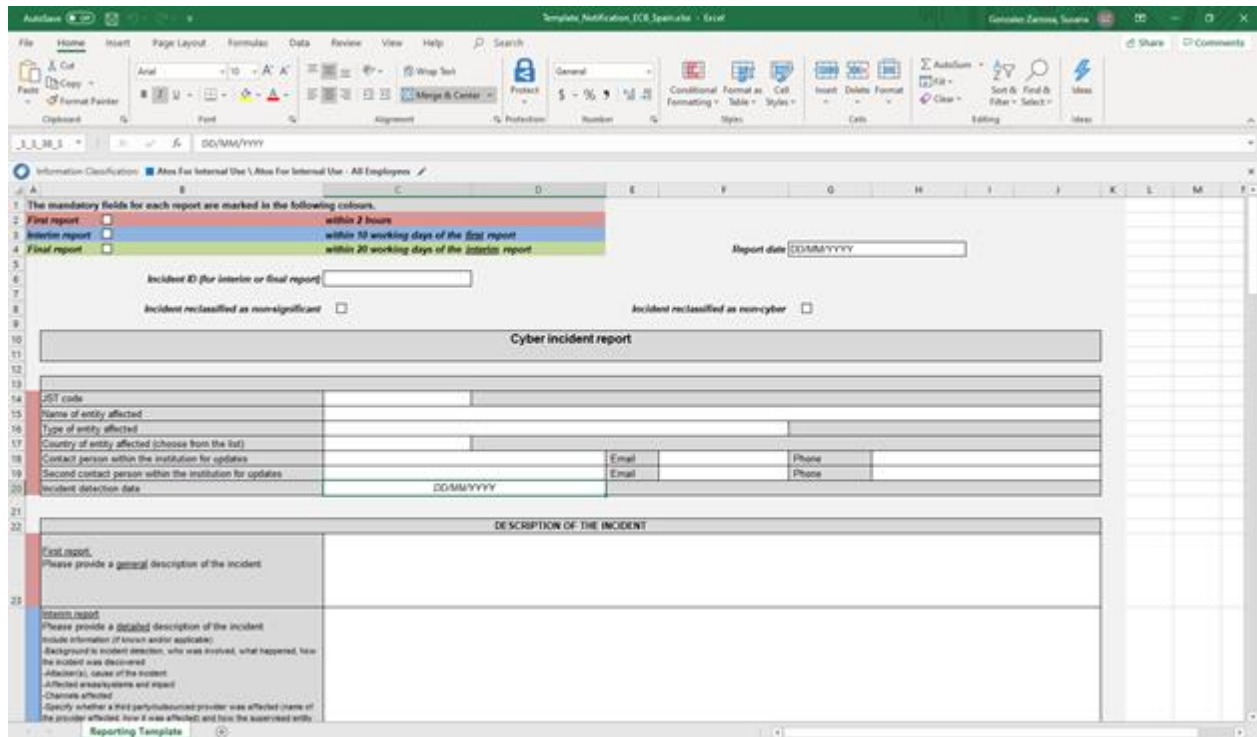
Figure 53: Templates menu in IR-UC3

This functionality is implemented by the service *aire-reports-generator* included in the asset AIRE. It accesses to the information registered in the Incident Register database and uses the templates provided by the supervisory authorities for reporting (see Figure 54 and Figure 55). The Apache POI²¹ library for Microsoft Documents has been used to work with the Excel files.

The mapping between the element in the data model where the information is stored and the name of the cell in the output Excel where it needs to be written is defined in an Excel included in the configuration of

²¹ <https://poi.apache.org/>

the service. In this way, in case the templates or the information required in them change, they can be easily updated without modifying the service.



The screenshot shows the ECB Template (IR-UC3) in Microsoft Excel. The template is titled "Template: Notification, ECB, Spanish". It includes a header section with instructions on mandatory fields and their deadlines. The main body is divided into sections for "Cyber incident report" and "DESCRIPTION OF THE INCIDENT".

Header Section:

- The mandatory fields for each report are marked in the following colours.
- First report:** within 2 hours
- Interim report:** within 10 working days of the first report
- Final report:** within 20 working days of the first report

Cyber incident report section:

- Report date: DD/MM/YYYY
- Incident ID (for interim or final report):
- Incident reclassified as non-significant: ☐
- Incident reclassified as non-cyber: ☐

DESCRIPTION OF THE INCIDENT section:

- First report:** Please provide a general description of the incident.
- Interim report:** Please provide a detailed description of the incident. Include information of known and/or applicable:
 - Background to incident detection, who was involved, what happened, how the incident was discovered
 - Affected entity, cause of the incident
 - Affected assets/systems and impact
 - Channels affected
 - Specify whether a third party/subsourced provider was affected (name of the provider affected, how it was affected) and how the supervised entity

Figure 54: ECB Template (IR-UC3)

Figure 55: PSD2 template (IR-UC3)

5.3.5 Quality Indicators

5.3.5.1 Effectiveness and efficiency of the solution

The indicators evaluated in this use case are the same described in section 5.1.6.1

5.3.5.2 User and stakeholder engagement and impact evaluation

The evaluation of the users and stakeholders engagement as well as the impact the incident reporting platform developed in this Use Case can have, will not be done at this stage of the demonstrator (phase1).

At this stage of the development the validation has been done by the stakeholders participating in the project, that can validate if the development arranged gives the results expected during the design of the prototype. The validation is a technological testing of the functionality of the tool. For this reason, the better user to test it are the users of the Financial Institutions involved in the development, being also involved in departments in charge of the Incident Reporting in their Organizations These end users are in the same way the correct people to evaluate the impacts in the Incident Reporting process of the usage of the tool and the real needs to be accomplished. These evaluations will be done at the end of the development of the Incident Reporting Platform.

5.3.6 Requirements Coverage

The following table shows the requirements that have been validated in this Use Case and the results of the validation.

ID	Validated	Strategy	Result	Mandatory	Comments
OB-SP01	Yes/No/Partially	Test Case XXX, Questionnaire, technology based	Success/Fail	Yes/No	Any comments here.
IR-F01	Yes	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	Mandatory Incident Reporting is manual; the IRT send the Report to the Authority not using the tool
IR-F03	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The platform supports to include new templates with the information that need to be included in the reports. But it is not implemented yet the possibility to upload/download them from the GUI.
IR-F09	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The tool produce the appropriate template and communication, in the appropriate format to be sent to the

ID	Validated	Strategy	Result	Mandatory	Comments
					Competent Authority for the two Regulations considered (phase 1 scope).
IR-F10	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	It provides the appropriate template and send it to the IRT team. This team will send it to Head Office ISO
IR-F11	No	N/A	N/A	Yes	It is not yet possible to validate this functionality
IR-F12	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The tracking is shown in real-time through the capabilities provided by TheHive GUI. However, it is not stored in the Incident Register database yet.
IR-F13	Yes	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	An incident reporting workflow is enforced in the demonstrator,

ID	Validated	Strategy	Result	Mandatory	Comments
					creating and assigning the tasks in TheHive that the users need to do depending on their roles.
IR-F14	Partially	Technology based	Success	Yes	It is possible to configure for each stage in the workflow what are the tasks created, the description shown in each of them, the user assigned and the tags shown in the incident. But it is not possible to change the Incident Reporting Workflow by the system administrator without changing the BPMN file and recompiling the code in the demonstrator.
IR-F16	Yes	Test Case 1- UC3 Test Case 2- UC3	Success	Yes	The Administrator user is able to to configure the regulations, the recipients, the channels and the templates

ID	Validated	Strategy	Result	Mandatory	Comments
IR-SP01	Yes	Test Case 1-UC3 Test Case 2-UC3	Fail	Yes	The authentication mechanism to access the demonstrator is based on username and password. Strong authentication mechanisms have not been implemented in the demonstrator.
IR-SP02	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	<p>The demonstrator grants access to information on a need to know base and matching authorisation profiles. The information shown to the user in the GUI is different depending on his/her profile.</p> <p>At the end of the project, when all the information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the</p>

ID	Validated	Strategy	Result	Mandatory	Comments
					demonstrator is focused on the first Mandatory Report).
IR-SP03	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	<p>The demonstrator ensures that the information needed is made available.</p> <p>At the end of the project, when all the information required to report the incident has been included in the demonstrator, this requirement will be completely validated (Currently, the demonstrator is focused on the first Mandatory Report).</p>
IR-SP04	Yes	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	There is a section in the demonstrator GUI to configure users and their functions, in order to ensure limiting or granting permissions to each user

ID	Validated	Strategy	Result	Mandatory	Comments
					based on their functions.
IR-SP05	Partially	Technology based	Success	Yes	<p>Logging, timestamping and tracking mechanisms have been incorporated at all phases of the Incident Reporting process.</p> <p>The platform supports the tracking of the security event lifecycle registering any action performed in TheHive. The tracking is shown in real-time through the capabilities provided by TheHive GUI. However, it is not stored in the Incident Register database yet.</p>
IR-LF01	Yes	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The demonstrator includes a GUI that allows the interaction with the operator
IR-LF02	Yes	Test Case 1-UC3 Test Case 2-UC3	Fail	No	The GUI currently included in the demonstrator only supports

ID	Validated	Strategy	Result	Mandatory	Comments
					English language.
IR-U01	Partially	Test Case 1-UC3 Test Case 2-UC3	Success	Yes	The GUI should be improved to guarantee that is user-friendly, offers a better user experience, improves the response times and facilitates the navigation between the different functionalities.
IR-LR01	No	N/A	N/A	Yes	Incident reporting requirements established by the NIS Directive for Operators of Essential Services have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR02	No	N/A	N/A	Yes	Incident reporting requirements established by the EU privacy regulation (GDPR) have not been considered in

ID	Validated	Strategy	Result	Mandatory	Comments
					the demonstrator, as they are not included in the scope of this phase.
IR-LR03	No	N/A	N/A	Yes	ENISA Guidance on Incident reporting for eIDAS have not been considered in the demonstrator, as they are not included in the scope of this phase.
IR-LR04	Yes	Test case 1-UC3	Success	Yes	Incident reporting requirements established by the ECB framework have been considered in the demonstrator.
IR-LR05	Yes	Test case 2-UC3	Success	Yes	Incident reporting requirements established by the Payment Services Directive PSD2 have been considered in the demonstrator.
IR-LR06	No	N/A	N/A	Yes	Incident reporting requirements

ID	Validated	Strategy	Result	Mandatory	Comments
					related to Target2 system have not been considered in the demonstrator, as they are not included in the scope of this phase.

Table 17: Incident Reporting – IR-UC1 Validation Requirements' Coverage

5.4 Validation Summary

ID	Validated	Result	Comments
IR-UC1	Partially	Success	The main functionalities specifically related to data collection for the generation of the first report for ECB and PSD2 regulations have been successfully validated.
IR-UC2	Partially	Success	The main functionalities specifically related to managerial judgement for ECB and PSD2 regulations have been successfully validated.
IR-UC3	Partially	Success	The main functionalities for data conversion and generation of the first report for ECB and PSD2 regulations have been successfully validated.

Table 18: Incident Reporting demonstrator's use cases validation summary.

Once validated the requirements defined in D5.1 through the three use cases we can summarize that all the main mandatory functionalities for each of the use cases are covered and most of the rest are partially covered.

We need to highlight that during this first demonstrator we have focused only on the first mandatory report under two regulatory frameworks (ECB and PSD2) whereas six regulations are included in the requirements. For this reason, we have considered “partially” validated those requirements that will need to be validated completely at the end of the project once the intermedium/final reports for the six regulations are available.

On the other hand, in this first version of the prototype we have focused on providing the main capabilities that need to have the incident reporting platform and in this sense we consider all the requirements have been successfully addressed. It is worth noting that there are many mandatory requirements (17/36) related not to functionalities of the incident reporting platform but to security and privacy, look and feel, usability, operational, maintainability and portability which have been also validated “partially” because it has been considered that, although the functionalities are provided, they could be improved during next iterations of the demonstrator. For example, the GUI could be more user-friendly, the administration of users could have more capabilities (currently not supported by the open source tool used in the platform), or the logging and tracking systems could include more details (e.g. specific log files with a register of the actions performed by the users). Additional requirements included in D5.1 and not currently covered, such as strong authentication mechanisms, consideration of different business calendars, support for selecting currency applicable, support for multi-language or self-adaptive questionnaires, will be reviewed to check if they are included in next deliveries of the demonstrator or they are not priority and those requirements can be skipped.

5.5 Lessons Learned and Future Work

Through the validation performed in this deliverable it has been verified that the “*incident reporting in the financial sector*” demonstrator can effectively offer support to the different teams involved in the process of gathering information about security incidents and preparation of the mandatory incident reports that need to be sent to the competent authorities.

However, during the validation of the Incident Reporting Platform it has been verified that the open source tool TheHive included as incident management and response solution in the platform has some limitations for Data Collection. For example, fields to be completed with the information of the incident cannot be grouped depending on the type of information to be provided (impact of the incident, incident type, estimated costs,...) to make the Incident Reporting Platform more user-friendly. And, since it is not possible to create multi-choice fields, it has been necessary to include several fields to select one by one all the options (such as the impacts on personal data, on offered trust services, on essential services provided, etc).

It is also worth mentioning that during the validation we have realized that, although we have a predefined workflow covering all the incident reporting stages that should be followed for the regulatory frameworks included in the demonstrator, the reality can be more complex and exceptions not currently managed by the demonstrator can appear. The current incident reporting workflow needs more analysis to identify all these potential exceptions to the main incident reporting workflow and determine how to proceed in those cases.

We have identified several lines of future work to complete and enhance the incident reporting platform demonstrator validated in this Deliverable. The priority will be to complete the incident reporting workflow with the generation of the intermediate and final reports for the regulations we are currently working, ECB and PSD2. We will also work on completing some of the requirements currently partially covered or not

available yet, such as the single sign-on feature, the multi-language or include the possibility to upload/download report templates from the GUI.

As currently the platform only covers a subset of the criteria and thresholds established by the regulations included in the scope of Phase 1 (PSD2 and ECB framework), in the next phases of the development all the criteria and thresholds defined should be considered.

Tutorials and user manuals including the ones related to the deployment and installation of the incident reporting platform will be also prepared and included in next releases of the demonstrator.

The validation sessions showed the necessity to implement the data model prepared. Next implementation will consider furthermore the ability to support templates for the same regulation but from different countries; as a matter of fact local regulation could modify slightly the template required.

Additionally, related to the research challenge 3 “Promote a collaborative approach for sharing incident reports to increase cyber resilience” presented in the deliverable D4.3, during phase2 we will start the integration of the demonstrator with the threat intelligence platform instances using MISP provided by ATOS, KUL and UMU in the context of the task 3.4.

Finally, we would like to extend in the next iteration of the demonstrator the current platform including the generation of reports according to the templates of other regulatory frameworks (such as NIS directive, GDPR or eIDAS regulation). It will depend on the progress of the development of the tool.

6 Maritime Transport

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. Multiple strategies will be combined to validate the requirements identified in D5.1 for the four use cases, described in the Maritime Transport Demonstration. Below, we describe in detail the validation of each use case scenario.

6.1 Use Case MT-UC1: Threat Modelling and Risk Analysis for Maritime Transport Service

In the context of deliverable D5.2, MT-UC1 was broken down to a set of intertwined functionalities represented by sub use-cases:

- MT-UC1.1: Assets Identification and IT Infrastructure Representation.
- MT-UC1.2: Maritime Services Analysis and Representation.
- MT-UC1.3: Vulnerability Management.
- MT-UC1.4: Threats and Controls Management.
- MT-UC1.5: Threat Scenarios Specification.
- MT-UC1.6: Maritime Transport Risk Analysis.
- MT-UC1.7: Attack Paths Generation and Representation.
- MT-UC1.8: Maritime Transport Risk Management.

For the use cases listed above, multiple aspects will be validated either partially or fully. Most of the requirements that were previously set, and are considered necessary to successfully carry out MT-UC1 are:

- Security and Privacy Requirements.
- Operational Requirements.
- Usability Requirements.
- Legal and Regulatory Requirements.
- Social and Political Requirements.

To validate these requirements, a combination of three approaches will be utilized:

- *Technical Test Cases.* These will be used to validate: (1) the Security & Privacy Requirements (in particular, part of the Vulnerability Assessment), (2) the Operational Requirements (in particular, Installation & Deployment, Functionality Testing, Unit Testing) and (3) the Usability Requirements (in particular, User Acceptance Testing).
- *Target Group Engagement:* Questionnaires will be utilized to enable stakeholder evaluation, to validate (1) the Legal and Regulatory Requirements, (2) the Social and Political Requirements and (3) the Usability Requirements.

- *Technology Based Analysis*: Document analysis will be used to partially validate (1) the Security & Privacy Requirements (i.e., compliance with relevant security standards), (2) the Operational Requirements (i.e., the methodology, software components and libraries utilized to implement the architecture and the relevant functionalities), (3) the Legal and Regulatory Requirements and (4) the Social and Political Requirements with respect to the relevant standards, best practices, directives and guidelines.

Showcase Scenario: The “Vehicles Transport Chain” Service is a massively complex system 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, threshing machines etc. This Service is a relatively long and complicated process that involves domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology. In this framework, the vehicles transport affects many sectors along the supply chain.

6.1.1 Actors

The validation approaches presented above are carried out by two main actors to cover both technical and business aspects of the demonstrator

- Security researchers from UPRC tested the proposed system to identify possible bugs and other problems regarding functionality aspects.
- Piraeus Port Authority (PPA) is a main actor in the Demonstration Scenario, PPA participates in several Maritime Transport Services (such as Vehicle Transport Service). To appropriate the extent to which the system meets the client’s needs, non-technical user questionnaires were filled in by PPA.

6.1.2 Test Case MT-TC1

MT-TC1 can be illustrated as a general Test Case containing a set of specific test cases:

- MT-TC1.1: Installation and Deployment of the Components.
- MT-TC1.2: Technical Evaluation.
- MT-TC1.3: User Testing.
- MT-TC1.4: Vulnerability Assessment.

6.1.2.1 MT-TC1.1: Installation and Deployment of the Components

6.1.2.1.1 Description

The CS4E Maritime Risk Assessment system requires multiple components to be installed before the application can be built and run. The deployment of the system is based on Java jdk 8 and Apache maven (as Building Server), while the execution requires Apache solar (for Distributed search and index replication Server), MongoDB and Mysql server (as Database Servers), Apache ActiveMQ (as Messaging Server), Neo4j(as Graph Database Server) and Apache Spark (as Job Server).

6.1.2.1.2 Test Case Workflow

- The first step of the installation process is to install Java jdk 8 and add its bin folder path to the path environment variable. Java is essential in this case, since it is used to install other components, to build and run the project.
- Then apache maven is installed, and its bin folder path is added to the path environment variable.
- The rest of the servers are installed through executables or through their binary version.
- Test that all servers are functioning, set credentials and ports.
- Vulnerability-Asset-Weakness Data are imported to Mysql.
- Quartz Scheduler tables are imported to Mysql.
- Application.properties file, which is contained in the CS4E MT-RA project is adjusted to the credentials and ports that were set for the installed servers.
- Using CMD or bash, the command mvn install is executed in the main directory of the CS4E MT-RA project, which initializes a procedure called dependency injection, which fetches all the required libraries, connectors and such required to run the project.
- Once the building procedure finishes successfully the application can be launched through a jar file.

6.1.2.1.3 Test Results

The application is installed, configured and deployed.

6.1.2.2 MT-TC1.2: Technical Evaluation

6.1.2.2.1 Unit Testing

6.1.2.2.1.1 Description

An iterative software development process where the smallest testable parts of an application (units) are individually and independently scrutinized to verify their proper operation. It stands at the base of the testing pyramid and is a prerequisite for more complex testing operations (e.g. integration testing, performance testing, functional testing, etc.). Individual software units must be adequately tested before being combined in groups at higher levels of the testing hierarchy. Proper unit testing, aside from verifying the correctness of the individual software units, manages to:

- Improve code quality.
- Enable the adoption of agile methodologies throughout the development life-cycle.
- Facilitate functionality changes.
- Simplify integration between higher-level components.
- Identify design deficiencies through exposing strong coupling of software units.
- Reduce turnaround time required for bug fixing.

6.1.2.2.1.2 Test Case Workflow

For each unit test a file from the source code will be chosen, then a specific scope is set, under which the chosen file will be investigated, regarding the following aspects:

- Proper data retrieval.
- Proper operation of data modifying actions (create, updated, delete).
- Proper authorization enforcement (e.g. business partners can only browse their assets).
- Proper operation of any other supported functionality.

6.1.2.2.1.3 Test Results

Test Results: Table 19 summarizes the results of the unit testing.

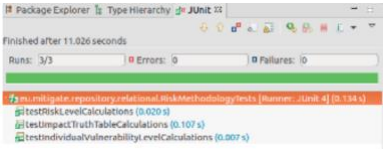
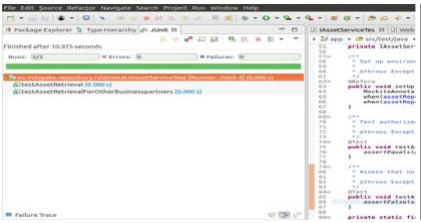
Test Filename	Test Scope	Execution Results
RiskMethodologyTests.java	Assess the correctness of vulnerability impact, vulnerability level and risk level calculations as per the CS4E MT-RA risk assessment methodology.	 <p>Package Explorer Type Hierarchy JUnit 22 Finished after 11.026 seconds Runs: 3/3 Errors: 0 Failures: 0 <ul style="list-style-type: none"> testIntegrateRelationshipsMethodologyTests (Runners: 0.134 s) testRiskLevelCalculations (0.020 s) testImpactTruthTableCalculations (0.107 s) testIndividualVulnerabilityLevelCalculations (0.007 s) </p>
IAssetServiceTest.java	Assesses the correct of all asset service operations. In more detail, data retrieval, data entry, data editing, asset deleting, and unauthorized asset view sub-tests are being performed.	 <p>Package Explorer Type Hierarchy JUnit 22 Finished after 10.975 seconds Runs: 1/1 Errors: 0 Failures: 0 <ul style="list-style-type: none"> testAssetService (0.000 s) testAssetServiceWithOtherBusinessPartners (0.000 s) </p>

Table 19: Summary of the results of Unit Testing

6.1.2.2.2 Integration Testing

6.1.2.2.2.1 Description

Integration testing is the software testing phase where individual modules (units) are combined and tested as a group. This phase succeeds unit testing, and its purpose is to expose faults between integrated components. CS4E MT-RA's integration testing activities involve the data access layer.

CS4E MT-RA works with four different data store types:

- A relational database (MySQL) that serves as the default database for the tool.
- A no-SQL store (MongoDB) that is particularly used for:
 - Creating asset inventory replicas as a result of risk assessment executions and simulations.
 - Storing collected cybersecurity content by the open intelligence module.
- A graph database (Neo4j) to support complex asset hierarchies and relationships.

- An enterprise search platform (Apache Solr) providing document indexing and fast searching for the filtered cybersecurity content.

6.1.2.2.2.2 Test Case Workflow

The integration tests developed for the data access layer of the CS4E MT-RA tool provide 100% code coverage (applies to data access related functions). Table 20 contains the exhaustive list of all data access related integration tests and provides the following information:

- Name of the file containing the test (all files are available in the project's code).
- The type of the associated data store.
- The operations under integration test (read, write, delete).

Integration Test Filename	Data Store	Tested Operations
AssetTestTest.java	MySQL	read, write, delete
NetworkTestTest.java	MySQL	read, write, delete
VulnerabilityTestTest.java	MySQL	read, write, delete
VendorTest.java	MySQL	read, write, delete
ProductTest.java	MySQL	read, write, delete
AttackScenarioTest.java	MySQL	read, write, delete
ThreatTest.java	MySQL	read, write, delete
ControlTest.java	MySQL	read, write, delete
SiteTest.java	MySQL	read, write, delete
BusinesspartnerTest.java	MySQL	read, write, delete
UserRepositoryTest.java	MySQL	read, write, delete
SupplyChainTest.java	MySQL	read, write, delete
ProcessTest.java	MySQL	read, write, delete
PendingActionTest.java	MySQL	read, write, delete
RiskAssessmentTest.java	MySQL	read, write, delete
RiskassessmentRunAssetTest.java	MongoDB	read, write, delete
RAAssetTest.java	MongoDB	read, write, delete

Integration Test Filename	Data Store	Tested Operations
AssetNodeTest.java	Neo4j	read, write, delete
SocialContentTest.java	Apache Solr	read, write, delete

Table 20: Summary of the .java classes included in the Integration Testing

6.1.2.2.3 Test Results

Test Results: Sample Results of BusinesspartnerTest.java are illustrated in Figure 56.

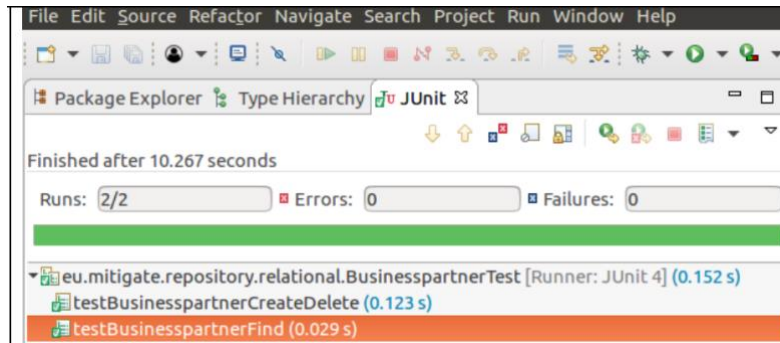


Figure 56: Results of Integration Testing

6.1.2.2.3 Performance Testing

6.1.2.2.3.1 Description

The performance testing has been carried out with all instances. CS4E MT-RA is an application that won't expect high loads of requests and given its REST nature and the underlying design it will always respond in a timely manner. Tasks that take a while to run are executed asynchronously.

The most resource-consuming module of the CS4E MT-RA tool is the risk assessment one. In practice, when an operator initiates and executes a risk assessment, the system performs the following tasks:

- It collects assets that are part of the process under review for all business partners.
- It identifies and collects (if any) the assets that declare cyber-dependencies between business partners.
- It merges the two asset sets in one containing all unique entries.

- It retrieves the vulnerability profile per asset and detects which vulnerabilities are not treated by already applied security controls.
- It performs calculations as per risk assessment methodology and stores the final results.

6.1.2.2.3.2 Test Case Workflow

Figure 57 displays risk assessment execution time as a function of the number of assets it assesses. The time value (in ms) on the vertical axis represents the total execution time needed from the moment a web user clicks the button to initiate/execute a risk assessment on the browser till the latter receives a response from the system (either successful or not). While the turnaround time does not depend solely on the number of assets included (number of vulnerabilities and security controls applied are also important), it is indicative that the system's performance is predictable and the time complexity of the operation can safely be considered as linear. As the goal of this test case was to assess the risk assessment execution time and not the accuracy of the results, both real and synthetic data were used, in order to increase the number of input assets.

6.1.2.2.3.3 Test Results

Test Results: Sample Results of Performance Testing are illustrated in Figure 57



Figure 57: Risk assessment performance results

6.1.2.3 MT-TC1.3: User Acceptance Testing

6.1.2.3.1.1 Description

Implementation of each Scenario is confirmed by either running one or more automated UI Tests, or by visually inspecting the results of test execution in the cases that test automation is not applicable or not available. Automated UI tests provide functional and integration testing of the user interface and validation of user interface controls. They enable CS4E MT-RA consortium to test that the user interface is functioning correctly after code changes. They are quicker to run than manual tests.

6.1.2.3.1.2 Test Case Workflow

Security experts from UPRC carried out the UAC procedure.

- Self-Registration: The user creates a new account in the CS4E MT-RA system.
- Access the System: The user accesses the CS4E MT-RA system to assess the security risks of the Supply Chain Services in which his/her organization participates.
- Initiation of a new Maritime Transport Service: The user creates the SCS that will be examined.
- Management of Maritime Transport Services: The user manages (view, edit, delete) the list of the SCSs.
- Initiation of a new Maritime Transport process: The user manages (view, edit, delete) the list of the SCS's processes.
- Management of the Maritime Transport's Service processes: The user manages (view, create, edit, delete) the list of the SCS's processes
- Business partners Association: The user makes the association of the business partners to the defined SCS processes.
- Acceptance of Business Partner's invitation: Another user confirms the participation of his/her organization to the defined Maritime Transport processes.
- Review Business Partners in the Maritime Transport process: The user explores the business partners involved on a defined SCS processes.
- Process related Assets Identification: The user defines the assets required for the provision of the examined process.
- Asset Management: The user manages (create, view, edit, delete) the list of the assets.
- Asset Related Information (Vulnerabilities, Threats & Controls) Management: The user manages the Asset Related Information (Vulnerabilities, Threats & Controls)
- Asset Networks Management: The user manages the Asset Networks.
- Networks Management: The user manages (view, edit, delete) the list of the networks.
- Site Management: The user manages (view, edit, delete) the list of the sites.
- Initiation of a new Risk Assessment: The user initiates a new Risk Assessment.
- Review of the Assets related Information (Vulnerabilities, Threats & Controls): The user explores the Asset Related Information (Vulnerabilities, Threats & Controls).
- Individual Asset Threat Assessment: The user assesses the probability of occurrence for each possible Threat for the asset under examination.
- Execution of a Risk Assessment: The user executes a Risk Assessment.
- Review of the Risk Assessment Results: The user explores the sample Maritime Transport Scenario Results.
- Threat Management: The user manages (create, view, edit, delete) the list of declared threats.
- Threats Profiles Management: The user manages (create, view, edit, delete) the list of declared threats profiles.

- Vulnerability Management: The user manages (create, view, edit, delete) the list of published/declared vulnerabilities.
- Vendors Management: The user manages (create, view, edit, delete) the list of declared Vendors.
- Controls Management: The user manages (create, view, edit, delete) the list of declared controls.

6.1.2.3.1.3 Test Results

Regarding the usability perspective most of the beta testers confirmed, that the CS4E MT-RA system is efficient due to the required time for its usage is reasonable and improves the productivity of the users. Furthermore, it is easy to learn and provides a comfortable usage. Most of them also stated that the system already has an easy-to-understand logic and structure as well as helpful visualizations and interactive control about the working process and the reports. Regarding the expected functions and functionalities, most of the testers were also satisfied with CS4E MT-RA's capabilities.

Regarding the error messages and error recovery or undo functions, many still saw a considerable potential for improvement. Due to the beta stadium of the system, this is not surprising, but provides valuable suggestions for further improvements. Despite the positive overall rating, many further recommendations, and suggestions for improvements were collected and considered by the developers. For example, early testers mainly recommended a clearer user interface and improved search functions, e.g. for the assets and vulnerabilities, which are imported from external databases and thus form a large number. Both could have been implemented early in the systems' improvement process. In addition, comments have pointed out that especially in larger organizations a huge number of cyber assets must be managed and kept up to date in the CS4E MT-RA system to provide meaningful and up to date cyber risk assessment results. The suggestions to develop and provide an import interface for external third party tools for BPNM or asset inventory management and so make usage of potential already existing repositories and data sources within companies were taken up by the developers.

6.1.2.4 MT-TC1.4: Security Testing and Vulnerability Assessment

6.1.2.4.1 Description

Security testing is basically a type of software testing that aims to check whether a software application is secured or not, identifying if the application is vulnerable to attacks. At this stage our security testing validation will only involve the identification of the assets and the discovery of the relevant vulnerable components.

6.1.2.4.2 Test Case Workflow

To perform a successful vulnerability assessment, the initial step is vulnerability discovery. The procedure is essentially a manual walk-through of the application, to better understand the scope and functionality of the application, the technologies and design principles in use, and potential attack vectors within the application. CS4E MT-RA will be tested using the OWASP (Open Web Application Security Project) Testing Guide as the basis to evaluate the CS4E MT-RA system and the supported services discovering potential flaws, improper configurations, or risky end-user behavior.

6.1.2.4.3 Test Results

Test Results: Table 21 lists the findings of the discovery procedure.

ID	Description
Finding 1.	No Session Timeout
Finding 2.	Stack Trace Debug Output Reveal Sensitive Information
Finding 3.	Deprecated Ciphers Supported
Finding 4.	Lack of CAPTCHA
Finding 5.	Outdated JavaScript library in use
Finding 6.	API Key Exposed On Web Page

Table 21: Results of the discovery procedure

6.1.3 Technology Based Analysis

In this section document analysis will be provided for technical aspects of MT-UC1:

- Compliance of the methodology with existing standards.
- Technical Details on the fulfillment of the requirements through existing technology.

Compliance with Standards

This section reports on the CS4E MT-RA's system compliance to various cybersecurity-related widely-used standards, frameworks, models, programs, best practices and initiatives (including ISO27001, ISO27005, ISO28000, ISPS and more). Also, the report indicates the compatibility of CS4E MT-RA system with the Common Vulnerabilities and Exposures (CVE) and the Common Attack Pattern Enumeration and Classification (CAPEC). Finally, the deliverable will specify the main steps and phases of the adopted software development and integration procedure.

The CS4E MT-RA system offers a bundle of added-value security management services, the cybersecurity-related attributes, indicators and functions contained in those services can be logically grouped in seven domains. Each of the 7 domains contains a structured set of cybersecurity objectives that represents the activities required for establishing and ensuring increased capability in the domain. These domains will be used as reference points to check and evaluate the CS4E MT-RA system's compliance to various selected standards and regulations (including ISO27001, ISO27005, ISO28000, ISPS and more). A brief description of the 7 domains is presented in Table 22.

Domain	Description
Risk Management	Establish, operate and maintain a cybersecurity risk management program to identify, analyze, and CS4E MT-RA cybersecurity risks to the organization taking into consideration the related interconnected infrastructures, and stakeholders.

Domain	Description
Asset, Change, and Configuration Management	Identify and manage all cyber assets which are necessary in the provision of the supported business processes and needed to be protected commensurate with the risk and impact resulting from various threats
Threat and Vulnerability Management	Identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities commensurate with the risk to the involved ICT infrastructure and organizational objectives.
Situational Awareness	Collect, analyze, correlate, and use cybersecurity security and risk related information, including information retrieved from online repositories, to form the security state of the cyber assets.
Information Sharing and Communications	Establish and maintain relationships with internal and external entities which will reveal their commitment to identify all of their organizations' cyber assets, the controls they have undertaken and provide cybersecurity information, including threats and vulnerabilities
Supply Chain and External Dependencies Management	Identify, analyze, and CS4E MT-RA the cybersecurity risks associated with assets that are dependent on other entities, commensurate with the risk to the involved ICT infrastructure and organizational objectives.
Cybersecurity Program Management	Establish and maintain an enterprise cybersecurity program that is aligned with the identified risk to the examined infrastructure.

Table 22: Security Domains

To establish compliance with known standards that the CS4E MT-RA system properly implements and integrates the following four core families of services:

1. **Collaborative Risk Assessment and Mitigation Services:** The core aim of these services is to specify the functionalities of the CS4E MT-RA system in terms of collaborative risk assessment and mitigation for ports and other ontologies in the maritime transport environment. A special focus is laid on the assessment of multi-dimensional risks, spanning over multiple sectors in ports' environment and their cascading effects. Regarding cyber-security, CS4E MT-RA focuses into systems used for protecting the ports' information infrastructure against external access from malicious parties. This group of services covers the main aspects of 5 security domains (Risk Management; Asset, Change, and Configuration Management; Threat and Vulnerability Management; Supply Chain and External Dependencies Management; and Cybersecurity Program Management) and are in line with several cybersecurity standards and approaches (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO 27005:2011, ISO/IEC 21827:2008, ISO 28001:2007, NIST Security Considerations in SDLC, NIST SP800-16, NIST SP800-37, NIST SP800-53, NIST SP800-61, NIST SP800-64, NIST SP800-128, NIST SP800-137, NIST NVD, NISTIR 7622, NISTIR 7628, NISTIR 7628, Key SEI CMM, SCADA AU RMF, Situation Awareness in Dynamic Systems and Supply Chain Risk Management Awareness). Specifically, in order to meet their objectives, these services incorporate a collaborative, multi-attribute risk management approach that collects the diverse security-related knowledge located in the ports,

data from online repositories and the results (e.g. threats, vulnerabilities metrics, prioritization of countermeasures) produced by the automated and semi-automated risk assessment routines and processes in order to: (i) determine the value of the information assets; (ii) identify the applicable threats and vulnerabilities that exist (or could exist); (iii) identify the existing controls and their effect on the risk identified; (iv) determine the potential consequences; and (v) prioritize and rank the derived risks.

2. ***Open Simulation Environment and Services:*** These services facilitate the design, execution and analysis of risk and threats simulation experiments, as well as the calculation of the cascading effects derived from interdependent threats. This group of services use the CS4E MT-RA approach to model the Maritime Transport Services and employ the proposed attack graph generation algorithm in order to cover the several aspects of two security domains, the Situational Awareness & Supply Chain and the External Dependencies Management and to be in line with various security approaches (e.g. ISO/IEC 27001:2013, ISO/IEC 27002:2013, NIST SP800-37, NIST SP800-137, NIST NVD, OECD Reducing Systemic Cybersecurity Risk, Situation Awareness in Dynamic Systems, Supply Chain Risk Management Awareness, ISO 28001:2007 and NISTIR 7622). Specifically, CS4E MT-RA creates a replica of the current state of the asset cartography and performs all calculations and actions on the replica. This approach not only assists in decoupling the current asset cartography from any additional risk assessment activity, but it also manages to keep it as close to the real environment as possible. Binding the state of the asset cartography with each risk assessment execution, enables operators to effectively monitor the risk evolution over time due to asset-based modifications.
3. ***Risk and Vulnerability Visualization Services:*** These services specify the risk visualization functionalities of the CS4E MT-RA system. The first big task that CS4E MT-RA System successfully implements is the specification of the means for a quick and visual reference to risk values. It then involves the identification of vulnerabilities that are exposed to various parts of the ports' supply chain. Relevant visual analysis functionalities are also specified to present all different patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures. These risk visualization services also include novel visual interfaces for scalable and efficient data management. This group of services addresses covers various aspects of two security domains, the Asset, Change, and Configuration Management and the Threat and Vulnerability Management and are in line with several security standards and specifications (e.g. ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 21827:2008, NIST SP800-40, NIST SP800-53, NIST SP800-64, NIST NVD and NISTIR 7628). These services provide the risk assessment and risk visualization functionalities required for the visual representation of a Maritime Transport infrastructure and in particular provide a visualization of the current state of the asset cartography.
4. ***Prediction, forecasting, social engineering and Open Intelligence Services:*** CS4E MT-RA gives emphasis on the identification of patterns/paths of (potential) vulnerabilities and attacks in the maritime transport sector. Focus is given on the identification of interdependencies between threats in different sectors and their cascading effects. This functionality is extended with forecasting procedures to estimate future impact, including metrics for the assessment of the probability of the various risks and of the overall resilience and reliability of the port infrastructure. This group of services addresses several aspects of three main security domains, the Situational Awareness, the Information Sharing and Communications and the Cybersecurity Program Management and are in line with several cybersecurity standards and approaches (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO 27005:2011, ISO/IEC 21827:2008, ISO 28001:2007, NIST Security Considerations in SDLC, NIST SP800-16, NIST SP800-37, NIST SP800-53, NIST SP800-61, NIST SP800-64, NIST SP800-128, NIST SP800-137, NIST NVD, NISTIR 7622, NISTIR 7628, NISTIR 7628, Key SEI CMM, SCADA AU RMF, Situation Awareness in Dynamic Systems and Supply Chain Risk Management Awareness).

6.1.4 Quality Indicators

In this section two types of questionnaires along with their feedback will be provided:

- **Technical User Questionnaire:** A demonstration of the functionality is realized for the technical users, then they are provided with specific instructions for a test scenario. Having completed the test scenario technical users are called to fill in the questionnaire
- **Stakeholder Questionnaire:** A questionnaire developed to gather information about the organization in the context of its compliance with various international standards

6.1.4.1 Questions

The questions posed for the non-technical users are presented below, on Table 23:

n.	Question	Possible answer	Answer	Comments
* Strongly Disagree:1, Disagree:2, Neutral:3, Agree:4, Strongly Agree:5				
1	Is the time required by using the CS4E MT-RA system reasonable?	*[1-5]		
2	The CS4E MT-RA system provides important decision support for improving the organizations risk situation.	*[1-5]		
3	How much money will your company save within the next five years and/or will be taken in additionally due to additional business if you would use the CS4E MT-RA system? (# [EUR])	*[1-5]		
4	Using the CS4E MT-RA system, my organization improves its compliance with security standards (e.g. ISO 27001).	*[1-5]		
5	Would you like to use the CS4E MT-RA system as a Service (SaaS)?	*[1-5]		
6	The CS4E MT-RA system provides convenient possibilities to exchange data with other software.	*[1-5]		

n.	Question	Possible answer	Answer	Comments
7	The CS4E MT-RA system enables a collaborative approach for supply chain participants to take care of their Critical Cyber Infrastructure.	*[1-5]		
8	The CS4E MT-RA system enables a collaborative approach for supply chain participants to take care of their Critical Cyber Infrastructure.	*[1-5]		
9	Have you tested the CS4E MT-RA system yourself?	["yes", "no"]		
OPTIONAL(requires yes on question 9)				
10	I was able to complete the tutorial's tasks and scenarios easy using the CS4E MT-RA system.	*[1-5]		
11	I felt comfortable using the CS4E MT-RA system.	*[1-5]		
12	It was easy to understand the structure and logic of the CS4E MT-RA system.	*[1-5]		
13	It was easy to learn how to use the CS4E MT-RA system.	*[1-5]		
14	I believe I could become more productive using the CS4E MT-RA system.	*[1-5]		
15	How many errors did you encounter during performing the task?	[number]		
16	The CS4E MT-RA system gave error messages that clearly told me how to fix problems.	*[1-5]		

n.	Question	Possible answer	Answer	Comments
17	Whenever I made a mistake using the CS4E MT-RA system, I could recover / undo easily and quickly.	*[1-5]		
18	The information (such as online help, on-screen messages and other documentation) provided with the CS4E MT-RA system was clear.	*[1-5]		
19	It was easy to find the information I needed.	*[1-5]		
20	The organization of information on the MITGATE software screens was clear and user-friendly.	*[1-5]		
21	The CS4E MT-RA system has all the functions and capabilities I expect it to have. If not, please comment what you are missing.	*[1-5]		
22	Overall, I am satisfied with the CS4E MT-RA system.	*[1-5]		
23	The CS4E MT-RA system provides helpful visualization and interactive control of the working process as well as the reports.	*[1-5]		
24	There are helpful shortcuts from one function to another.	*[1-5]		

Table 23: Stakeholder Questionnaire

6.1.4.2 Feedback

Results and observations were provided by PPA personnel that participated in the construction of the demonstration scenario. The most important observation is related to the assets management and how this is treated by the CS4E MT-RA system. In particular, the required information regarding the cyber assets of the organization are often already available and mapped in computer environments like Business Process Management Tools or existing inventory tools. Since the current version of the CS4E MT-RA system does not provide interfaces to such systems nor a standard-interface in the CS4E MT-RA platform is available this demands a duplicate data collection for the initial load of the system as well as during the data management. That requires lot of time to be originally created and difficulties are presented in maintaining it. This procedure is not advantageous, particularly keeping in mind security patches or hardware replacement.

The other significant observation had to do with the fact that a significant number of maritime users (e.g. port operators, maritime stakeholders) perform their everyday work-task using printed papers and not advanced ICT based solutions. This resulted a significant obstacle and difficulty in convincing them first to understand and then use the CS4E MT-RA Risk Assessment Toolkit.

Currently the majority of users working for the maritime industry either do not perform Risk Assessments on their infrastructures and if they do, they use a predefined, generic, non-cyber related, and short list of vulnerabilities (i.e. fire, lack of physical protection of the space, insufficient control of physical access to space, electricity instability, etc.). Consequently, such risk assessments do not adopt known and accepted methodologies, producing subjective results, which most of times do not depict the real image, in terms of security.

Analysis of the pilot user operations

These are our observations based on our experiences gained during the pilot operations:

- Many users were suspicious and provide unwillingness in using their real assets and infrastructures in the scenarios since they doubted that privacy issues and confidentiality is confirmed. The concept of participating in a supply chain risk assessment is new to most users.
- Users realized the potential value of the CS4E MT-RA system but they stated that the results generated from a supply chain risk assessment need to be reviewed by a security consultant, who has to create a risk treatment plan for their organization. Only in this case the CS4E MT-RA system has real value for them.
- Users suggested that CS4E MT-RA would probably gain more value by running at least once a day automatically and silently performing one and/or more risk assessments producing notifications to many recipients (i.e. security officers, IT departments, security consultants, etc).
- Many users also suggested that an open API should be implemented in order for other Security Systems in place to be able to communicate and automatically further process its results.
- To succeed on the aforementioned, the management console should be extended and provide many configurable and parameterizable options and services (i.e. generation of notifications if one new vulnerability appears and requires immediate actions).

Almost all maritime users participated in the pilot operations asked the following: “Who will undertake hosting and provision of the CS4E MT-RA tool and services respectively?”. Many of the users believe that such services should be provided by public trusted authorities in order to ensure the privacy and confidentiality level required for all participants. Other, however, suggested that the CS4E MT-RA system should be installed on their premises and only in order for them to be sure that privacy and confidentiality is applied.

6.1.5 Requirements Coverage

ID	Validated	Strategy	Result	Mandatory	Comments
MT-SP01	Partially	Test Case MT-TC1	Success	Yes	The functionality and security of the authentication mechanism was tested in MT-TC1.3 and MT-TC1.4

ID	Validated	Strategy	Result	Mandatory	Comments
MT-SP02	Partially	Test Case MT-TC1	Success	Yes	MT-TC1.3: In the Asset Management users cannot view or edit business partner assets without confirmation
MT-SP03	Partially	Document Analysis	Success	Yes	The risk assessment methodology as stated in the technology based analysis section analyzes risk for access control mechanisms
MT-SP04	Partially	Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section take network segregation under consideration
MT-SP13	Partially	Test Case MT-TC1	Success	Yes	The system produces logs that entail the required data.
MT-SP15	Partially	Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section take the availability of critical services under consideration.
MT-SP19	Partially	Questionnaire, Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section cover the compliance requirement
MT-SP20	Partially	Test Cast MT-TC1	Success	Yes	Covered through functionality
MT-U01	Partially	Questionnaire, Document Analysis	Success	Yes	Covered through the stakeholder evaluation
MT-OP01	Partially	Questionnaire, Document Analysis	Success	Yes	Covered through the stakeholder evaluation
MT-OP02	Partially	Document Analysis	Success	Yes	Covered through technology based analysis
MT-OP03	Partially	Document Analysis	Success	Yes	Covered through technology based analysis

ID	Validated	Strategy	Result	Mandatory	Comments
MT-SPL01	Fully	Questionnaire, Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section cover the compliance requirement
MT-LR01	Fully	Questionnaire, Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section cover the compliance requirement
MT-LR02	Fully	Questionnaire, Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section cover the compliance requirement
MT-LR03	Fully	Questionnaire, Document Analysis	Success	Yes	The Security Services as stated in the technology based analysis section cover the compliance requirement

Table 24: Maritime Transport –MT-UC1 Validation requirements' coverage.

6.1.6 Comments/Considerations

In this first validation phase, all of the requirements were assessed and validated, either partially or fully. The Legal and Regulatory Requirements, as well as the Social and Political Requirements were fully validated through document analysis, while the rest of the requirements were partially validated, based on all three validation strategies. However, as the full validation requires further integration of the relevant security services, this is expected at the next stage of the validation.

6.2 Use Case MT-UC2 – System Hardening

In this phase of the project we have validated a series of hardening tools that enable memory safety of in principle unsafe code (C/C++). In particular, we have validated hardening tools in terms of security and performance overhead. The tools are the following.

- **VTPin.** A pre-loader for protecting C++ binaries from VTable hijacking.
- **TypeArmor.** A binary-only CFI solution.

For the next phase, we plan to validate how these tools can be enabled in the maritime demonstrator; currently, all validation is executed with these tools operating standalone in instrumenting vulnerable *generic* software. Both tools are validated in terms of performance and security.

6.2.1 Actors

For this phase of the project the validation is demonstrated by researchers of UCY, that are part of the core teams that designed and implemented both VTPin and TypeArmor.

6.2.2 Test Case MT-TC2

6.2.2.1 MT-TC2.1 Validation of VTPin Deployment

6.2.2.1.1 Description

For the VTPin deployment, the following characteristics were tested and validated.

Performance: VTPin instruments a binary produced by a C++ compiler by pre-loading it and tracking all object deallocations. We thus evaluate VTPin with a selection of the C++ benchmarks (from the SPEC CPU2006 suite, Mozilla Firefox v47, and Chromium v50. All experiments are carried out on a host running Ubuntu Linux v14.04 (64-bit), armed with a 2GHz quad-core Intel Core i5-3320M CPU and 8GB RAM.

Security: We evaluated the effectiveness of VTPin by employing three publicly available exploits that target Firefox and rely on use-after-free vulnerabilities and VTable hijacking. The tests were performed on an Ubuntu Linux v14.04 (64-bit) virtual machine, with the latest version of Metasploit framework running on the host machine. Each corresponding Firefox version was compiled with GCC and the 'ac_add_options --enable-cpp-rtti' flag was added to the default configuration. The original exploits target Windows XP/SP3, so we had to port them to Linux; they match the following CVEs: CVE-2013-1690 (Firefox v17.0), CVE-2011-0065 (Firefox v3.5) and CVE-2013-0753 (Firefox v17.0.1).

6.2.2.1.2 Test Case Workflow

- Computational overhead. We summarize the results of the runtime overhead imposed by VTPin in Table 25. All SPEC CPU2006 benchmarks run to completion and each experiment was repeated 10 times. For Firefox and Chromium, we run typical JavaScript/HTML5 benchmarks. SunSpider and Kraken mainly stress JavaScript operations, and VTPin has an overhead of 4.1% and 1.2%, respectively on Firefox. The overhead for benchmarks that do not extensively use virtual objects is close to zero. xalanc, an XML parsing benchmark, massively allocates and deallocates memory and has an overhead of 4.9%.

Benchmark	Overhead
483.xalanc	1.049x
447.dealII	1.018x
450.soplex/1	1.015x
450.soplex/2	1.013x
462.libquantum	1.007x

444.namd	1.024x
453.povray	1.004x
473.astar	1.007x
Firefox	
SunSpider	1.041x
Kraken	1.012x
Peacekeeper	1.027x
Octane	1.003x
Chrome	
SunSpider	1.014x
Kraken	1.015x
Peacekeeper	1.036x
Octane	1.009x

Table 25: Results of Computational Overhead imposed by VTPin.

- Memory overhead.** VTPin preserves VTable pointers of virtual objects. The memory occupied by pinned objects is periodically reclaimed, however it is interesting to explore the amount of memory used before garbage collection. Table 26 summarizes the results for an instrumented Firefox running benchmarks and for a selection of SPEC CPU2006 programs. Notice that, when the glibc allocator is used, VTPin exhibits negligible memory overhead across all the benchmarks. When a slab allocator is used (and VTPin needs to retain entire virtual objects), the memory overhead is, as expected, more prominent. Nonetheless, only two benchmarks, Peacekeeper and xalanc, force VTPin's default configuration to garbage collect dead objects after hitting the 100 MB threshold. Max memory refers to the maximum cumulative allocation size observed during the execution of each benchmark. The VTPin/norealloc column (default on Firefox) depicts the amount of memory used by VTPin in absence of adequate realloc support from the underlying allocator (e.g., via a slab allocator). The VTPin/realloc column (default on SPEC) lists the amount of memory used by VTPin when adequate realloc support is available (e.g., via the glibc allocator). Note that VTPin's default configuration bounds memory leakage to 100 MB.

Benchmark	Max Memory	VTPin/norealloc	VTPin/realloc
<i>Firefox</i>			

SunSpider	131,309 KB	38,616 KB (29.4%)	3,462 KB (2.63%)
Octane	321,166 KB	16,740 KB (5.21%)	1,549 KB (0.48%)
Peacekeeper	624,546 KB	102,400 KB (16.4%)	21,632 KB (3.46%)
Kraken	1,240,534 KB	28,674 KB (2.31%)	2,559 KB (0.20%)
<i>SPEC CPU2006</i>			
483.xalanc	373,889 KB	102,400 KB (27.4%)	68,350 KB (18.2%)
447.dealII	107,035 KB	372 KB (0.34%)	272 KB (0.25%)
450.soplex/1	16,231 KB	496 B (0.00%)	24 B (0.00%)
450.soplex/2	15,758 KB	608 B (0.00%)	32 B (0.00%)
453.povray	3,278 KB	12 KB (0.36%)	552 B (0.01%)

Table 26: Memory Overhead Summary for VTPin

6.2.2.1.3 Test Case Results

Based on the results discussed above, we summarize the results of this test case.

Performance: The computational overhead for benchmarks that do not extensively use virtual objects is close to zero. xalanc, an XML parsing benchmark, massively allocates and deallocates memory and has an overhead of 4.9%. The same result holds for memory overhead, since based on the tests presented above, only two benchmarks, Peacekeeper and xalanc, force VTPin’s default configuration to garbage collect dead objects after hitting the 100 MB threshold.

Security: All exploits successfully triggered the respective vulnerabilities, which we cross-checked by inspecting their stacktraces, and they were all thwarted by VTPin.

6.2.2.2 MT-TC2.2 Validation of TypeArmor Deployment

6.2.2.2.1 Description

TypeArmor hardens binary for Linux/64-bit.

6.2.2.2.2 Test Case Workflow

Performance: The evaluation testbed runs on an Intel i5-2400 CPU 3.10GHz with 8GB of RAM, while the OS is Ubuntu 14.04 x86 64 running kernel 3.13. Performance evaluation is carried out on popular server applications, since they are fairly popular and often targets for attackers. The selection of software contains three FTP servers (namely, vsftpd v1.1.0, ProFTPD v1.3.3, and Pure-FTPd v1.0.36), two web servers (Nginx v0.8.54 and lighttpd v1.4.28), an SSH server (the OpenSSH Daemon v3.5), an email server (Exim v4.69), two SQL servers (MySQL v5.1.65 and PostgreSQL v9.0.10), a general-purpose distributed memory

caching system (Memcached v1.4.20), and a cross-platform runtime environment for server-side web applications (Node.js 0.12.5).

6.2.2.2.3 Test Case Results

The results are depicted in Table 27.

Application	Overhead
Exim	1.068
lighttpd	1.116
Memcached	1.014
Nginx	1.132
OpenSSH	1.021
ProFTPD	1.007
Pure-FTPd	1.02
vsftpd	1.025
PostgreSQL	1.16
MySQL	1.239
Node.js	1.061

Table 27: Overhead for tested Servers

6.2.2.2.4 Test Case Results

TypeArmor can cope with a vast amount of code-reuse attacks at the binary level. Additionally, TypeArmor can mitigate state-of-the-art code-reuse attacks that have not been seen in the wild. These attacks are commonly abbreviated as COOP (Counterfeit-Object Oriented Programming) attacks. We have evaluated our prototype with all published COOP exploits and they were all successfully prevented.

6.2.3 Technology Based Analysis

N/A

6.2.4 Quality Indicators

N/A

6.2.5 Requirements Coverage

The requirement coverage for MT-UC2 is illustrated in Table 28:

Req ID	Validated	Strategy	Result	Mandatory	Notes/Comments
MT-SP10	Partially	NA	NA	Yes	Components were validated successfully. Full validation requires integration.
MT-SP11	Partially	NA	NA	Yes	Components were validated successfully. Full validation requires integration.
MT-SP15	Partially	NA	NA	Yes	Components were validated successfully. Full validation requires integration.

Table 28: Requirements' coverage for MT-UC2.

6.2.6 Comments/Considerations

At this phase the security and privacy properties were tested in the underlying components, which were successfully validated. Full validation requires integration and is expected in the next phase of the validation.

6.3 Use Case MT-UC3 – Secure Maritime Communications

This use case will conclude in a demonstrator application. The implementation of the demonstrator is a work in progress, therefore, in Phase 1, we will look at the requirements that we can validate based on document analysis. These are the non-functional requirements that are connected with law and regulation (MT-SPL01, MT-LR01). However, note that we only validate based on the design of the application. In Phase 2, we will complete the demonstrator application. We will integrate with the PKI provided by SINTEF. At the end of Phase 2, we will validate the rest of the requirements and complete the validation started in this phase.

6.3.1 Actors

For Phase 1, the validation is carried out by document analysis. This analysis will be performed by researchers from CYBER.

6.3.2 Technology Based Analysis

For this use case we will use Technology Based Analysis for the initial validation. Analysis of the following documents and the implementation procedure was conducted:

1. The NATO Alliance Maritime Strategy (MT-SPL01);
2. Existing security standards: ISO/IEC 27001, IALA guideline 1082 (an Overview of AIS), IALA Guideline 1117 (VDES Overview) (MT-LR01).

6.3.2.1 MT-SPL01: Compliance with the NATO Alliance Maritime Strategy

The NATO Alliance Maritime Strategy states that “Allied maritime operations and activities can make vital contributions to Alliance security. Such contributions may include:

- Deterrence and collective defence;
- Crisis management;
- Cooperative security: Outreach through partnerships, dialogue and cooperation; and
- Maritime security.”

The design of the secure maritime communications application emphasizes the use of authentic and authorized ship-to-ship and ship-to-shore communications. This contributes to the maritime security aspect of the maritime strategy.

By equipping the VTS and vessels with means to securely communicate and authenticate themselves to each other and NATO forces, the secure communications application also supports the strategy requirement of “In support of these needs, NATO forces must be as agile, flexible and versatile as possible, well trained and equipped, rapidly deployable and sustainable at strategic distances, and fully interoperable with relevant military and non-military counterparts.”

The application also helps work towards another interoperability goal defined in the strategy “The Alliance, in accordance with the Comprehensive Approach Action Plan, will foster enduring relationships with relevant national and international actors in the maritime environment, such as the UN and EU, to contribute to our common goals of preventing conflict, building partner capacity, ensuring the freedom of the seas, upholding international maritime law and promoting Alliance values.” Namely, authenticated and authorized communications greatly contribute to upholding the international maritime law.

6.3.2.2 MT-LR01: Compliance with ISO/IEC 27001, IALA guideline 1082 (an Overview of AIS), IALA Guideline 1117 (VDES Overview)

The software development process of the developer of the secure maritime communications application (CYBER) has been ISO/IEC 27001 certified. The whole software development process (analysis, design, implementation, testing) follows the standard procedures.

The maritime communications application has been designed based on the IALA Guidelines 1082 and 1117, so the functional requirements are in compliance with these documents. In Phase 2, we will validate whether the implementation also complies to the requirements of these guidelines.

6.3.3 Quality Indicators

N/A

6.3.4 Requirements Coverage

Req ID	Validated	Strategy	Result	Mandatory	Notes/Comments
MT-SP01	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP02	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP03	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP05	No	Demonstrator	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP06	No	Demonstrator	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP09	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP12	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP16	No	Demonstrator	NA	Yes	Requires further integration. It will be validated in Phase 2

Req ID	Validated	Strategy	Result	Mandatory	Notes/Comments
MT-SP17	No	Demonstrator, penetration testing	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP19	No	Document analysis	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP20	No	Document analysis	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP21	No	Demonstrator	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SP23	No	Demonstrator	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-SPL01	Partially	Document analysis	Success	No	Will be completed in Phase 2
MT-LR01	Partially	Document analysis	Success	Yes	Will be completed in Phase 2
MT-LR02	No	Document analysis	NA	Yes	Requires further integration. It will be validated in Phase 2
MT-LR03	No	Document analysis	NA	Yes	Requires further integration. It will be validated in Phase 2

Table 29: Requirements Coverage for MT-UC3

6.3.5 Comments/Considerations

Since this use case is at an early implementation level, most of the requirements require further implementation and integration before they are tested and validated. Some of the requirements were partially tested based on document analysis. For the rest of the requirements validation will be performed at the next phase.

6.4 Use Case MT-UC4 - Trust infrastructure for secure maritime communication

In this phase of the project we have validated the setup and enrollment of the maritime PKI that enables secure maritime communication. This includes services for:

- Enrolment of new actors in the circle of trust.
- Issuing of cryptographic credentials that will allow the actors to communicate securely.

For the next phase, we aim to validate the integrated solution, which also includes the communication equipment and end users. In this context, we are able to validate services for:

- Checking the status of the cryptographic credentials.
- Exclusion of misbehaving or "expired" actors from the circle of trust.

The criteria for successful validation in this phase are either demonstrated through a functional prototype or documented.

6.4.1 Actors

For this phase of the project the validation is demonstrated by developers of the PKI technology owner (SINTEF).

6.4.2 Test Case MT-TC4

There are no test cases available for this phase of the validation in the current use case.

6.4.3 Technology Based Analysis

We have applied a technology-based validation inferred from a stand-alone prototype of the PKI. The prototype is based on OpenXPKI²², and adapted to the needs of a Maritime PKI. We have developed an interface, which allows ships to submit CSRs and to retrieve signed certificates programmatically. There is also an additional verification layer for the CSR used by the PKI Operators. Figure 58 shows how the PKI

²² The Open XPKI Project, <https://www.openxpki.org/>

is used in the enrollment process. From the ship point of view, Certificate Signing Requests are submitted using either a Web interface or a machine API on top of the Ship communication system. The PKI Operators use a Web interface for processing Certificate Signing Requests.

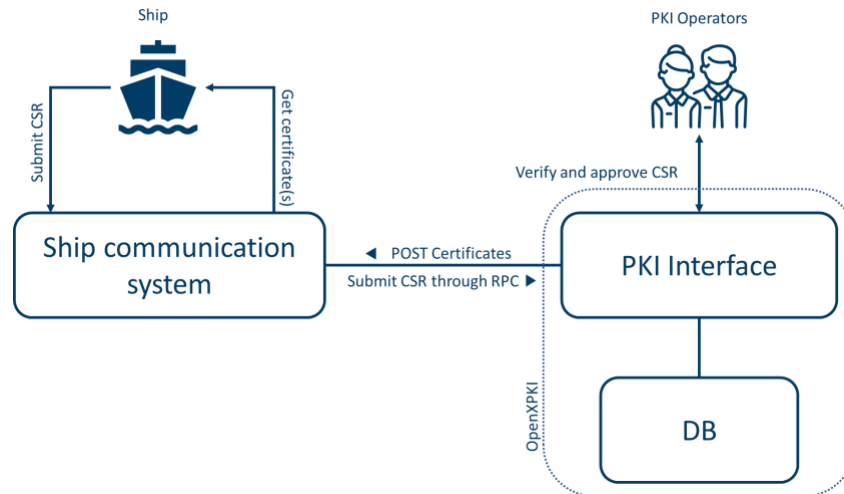
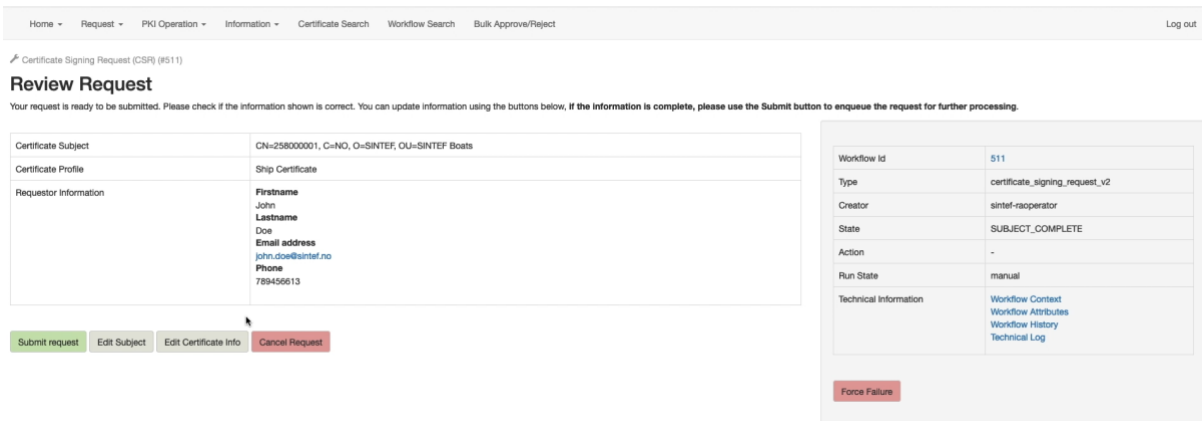


Figure 58. Layout of the PKI enrollment.

Validation evidence of the PKI Web interfaces and the resulting certificate are shown in the screenshots illustrated in Figure 59, Figure 60 and Figure 61.



Home - Request - PKI Operation - Information - Certificate Search Workflow Search Bulk Approve/Reject Log out

Certificate Signing Request (CSR) (#511)

Review Request

Your request is ready to be submitted. Please check if the information shown is correct. You can update information using the buttons below, if the information is complete, please use the Submit button to enqueue the request for further processing.

Certificate Subject	CN=25800001, C=NO, O=SINTEF, OU=SINTEF Boats
Certificate Profile	Ship Certificate
Requestor Information	Firstname John Lastname Doe Email address john.doe@sintef.no Phone 789456613

Submit request Edit Subject Edit Certificate Info Cancel Request

Workflow Id: 511

Type: certificate_signing_request_v2

Creator: sintef-raoperator

State: SUBJECT_COMPLETE

Action: -

Run State: manual

Technical Information: [Workflow Context](#), [Workflow Attributes](#), [Workflow History](#), [Technical Log](#)

Force Failure

Figure 59. User interface for creating and submitting a Certificate Signing Request.

[Home](#)
[Request](#)
[PKI Operation](#)
[Information](#)
[Certificate Search](#)
[Workflow Search](#)
[Bulk Approve/Reject](#)
[Log out](#)

Certificate Enrollment (#1023)

Certificate Enrollment

Error Code	Request was not approved
SCEP Endpoint	enroll
Server Interface	rpc
Certificate Subject	CN=258000003, C=NO, O=SINTEF, OU=SINTEF Boats
Comment	Original Comment: A comment from SINTEF / Fingerprint: 9028c4ae112ca1c19ae21814be9f73
Certificate Profile	Ship Certificate
Request Mode	Initial
Transaction ID	512707cda19574e7e061c7425c65ba9ca8f8e35

[Reject Request](#)
[Approve Request](#)

Workflow Id	1023
Type	certificate_enroll
Creator	anonymous
State	PENDING
Action	-
Run State	manual
Technical Information	Workflow Context Workflow Attributes Workflow History Technical Log

[Force Failure](#)

Figure 60. User interface for approving Certificate Signing Requests.

CKXZAWq6_SkKPNqzw9QiT_wl3lc

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      01:ff:02:f4:1b:c4:a6:3d:67:e8
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: CN=CysimsDemoIntermediateCA-0, O=NorwegianMaritimeAuthority, C=NO
    Validity
      Not Before: Oct  5 06:52:30 2020 GMT
      Not After : Oct  5 06:52:30 2023 GMT
    Subject: CN=258000001,C=NO,O=SINTEF,OU=SINTEF Boats
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:cf:0f:69:cc:e5:30:89:03:df:08:c7:3b:4e:2b:
        cf:28:9f:83:a4:5a:c1:9b:19:8d:51:7e:33:2a:65:
        0e:19:55:6b:6a:b5:7f:dd:23:f4:eb:d1:3c:9e:c3:
        7c:0f:5a:2c:82:7c:ba:cc:c9:94:6f:c6:19:09:0a:
        15:cb:a4:f3:9c
      ASN1 OID: prime256v1
      NIST CURVE: P-256
    X509v3 extensions:
      X509v3 Authority Key Identifier:
        keyid:9C:0C:E0:57:B1:13:DA:AD:3F:70:23:BB:C9:41:48:FD:B6:34:0B:E3
        DirName:/C=NO/O=NorwegianMaritimeAuthority/CN=CysimsDemoRootCA
        serial:01

      X509v3 Basic Constraints: critical
        CA:FALSE
      X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Agreement
      X509v3 Subject Key Identifier:
        44:43:03:CC:46:59:DE:29:09:C1:14:57:5E:DD:B4:19:A8:20:C9:39
    Signature Algorithm: ecdsa-with-SHA256
      30:65:02:31:00:f9:9c:08:1a:fc:b2:79:0e:c7:1d:1b:e4:96:
      3a:02:b4:9e:e5:ca:ea:4a:3d:ca:ec:36:1c:46:0c:b4:1d:00:
      1e:d7:23:e4:eb:c4:dc:89:01:6f:99:16:76:4b:eb:6d:04:02:
      30:04:7a:23:a8:95:63:ed:b0:1b:8f:b6:3b:e2:88:34:52:53:
      ab:98:d4:36:0e:4d:9f:7d:e2:b5:3e:f8:d2:57:79:7c:f1:9e:
      54:4b:62:4e:ed:62:5e:aa:d5:81:e8:3e:57
    -----BEGIN CERTIFICATE-----
    MIICDCCAfagAwIBAgIKAf8C9BvEpj1n6DAKBggqhkJOPQDAjBXMQswCQYDVQQG
    EwU1OTY7FIMFCA11IFCuaTmQuvUvnaWFiTWFvaYRnbnRydYRnbnR1n4HvY7ZkhRnNU
  
```

Figure 61. Generated certificate in PEM format.

6.4.4 Quality Indicators

N/A

6.4.5 Requirements Coverage

Table 30 shows coverage for the relevant requirements. The ones with comments "application specific" or "ship specific" are not subject for validation in this phase.

Req ID	Validated	Strategy	Result	Mandatory	Notes/Comments
MT-SP07	Yes	Technology based	Success	Yes	Part of the demonstrated enrollment process.
MT-SP08	No	Technology based	NA	Yes	Revocation not implemented yet. Will be implemented and tested in Phase 2.
MT-SP14	No	Technology based	NA	Yes	Revocation not implemented yet. Will be implemented and tested in Phase 2.
MT-SP22	No	Technology based	NA	Yes	Not implemented yet. Will be implemented and tested in Phase 2.
MT-OP05	Partially	Technology based	Success	Yes	The PKI has been configured for VDES bandwidth. Final validation requires integration.
MT-OP06	Partially	Technology based	Success	Yes	The PKI uses standardized English terminology.
MT-MP01	Partially	Technology based	Success	Yes	The PKI is designed to be operated by IMO (or similar organizations) as the trusted root, and

Req ID	Validated	Strategy	Result	Mandatory	Notes/Comments
					with flag states as subordinates.
MT-MP02	No	Technology based	NA	Yes	Not implemented yet. Will be implemented and tested in Phase 2.

Table 30: Requirements Coverage for MT-UC4

Comments/Considerations

As described above, in this phase we have validated the setup and enrollment of the maritime PKI, which includes the enrolment of new actors and the issuing of cryptographic credentials. The partial validation was successful, while for the next phase, we aim to fully validate the integrated solution.

6.5 Validation Summary

The validation summary for the Maritime Transport Sector is illustrated in Table 31:

ID	Validated	Result	Comments
MT-UC1	Partially	Success	According to the validation plan, the full validation of MT-UC01 will be performed in Phase 2 of the validation. Based on the results of the technical test cases the stakeholder evaluation and the technology analysis, several improvements will be realized and further tests will be implemented
MT-UC2	Partially	Success	According to the validation plan, the full validation of MT-UC02 will be performed in Phase 2 of the validation.
MT-UC3	Partially	Success	According to the validation plan, the requirements of MT-UC3 will be fully validated in Phase 2. This is because the communications application is developed in Phase 1 and will be completed in Phase 2. We have looked at the validation cases based on document analysis to the extent that they can be validated without having access to the implementation. Since MT-UC3 and MT-UC4 will provide a common demo, in phase 2 there will be common test cases.
MT-UC4	Partially	Success	According to the validation plan, the full validation of MT-UC04 will be performed in Phase 2 of the validation. Since MT-UC3 and MT-UC4 will provide a common demo, in

ID	Validated	Result	Comments
			phase 2 there will be common test cases.

Table 31: Maritime Transport demonstrator's use cases validation summary

6.6 Lessons Learned and Future Work

Concerning MT-UC1, in the current phase of the validation, we assessed multiple aspects of the Threat Modelling and Risk Analysis service. As the service evolves over the next deliverables further test cases will be required. Based on the results of the technical test cases the stakeholder evaluation and the technology analysis, several improvements will be realized, and further tests will be implemented. To move along with the roadmap provided in WP4, further research will be conducted on multiple directions:

- On the optimization of the attack path generation algorithm.
- Enhancements on existing risk assessment methodologies, utilizing evidence-based and scenario-based risk assessment approaches
- Improvements on the visual representation of vulnerable attack paths and attack scenarios.

Concerning MT-UC2, the underlying security testing tools have been set up and in the next phases these security hardening tools will be integrated with the risk mitigation component of the Risk Analysis service (MT-UC1). Furthermore, the MT-PKI service developed in MI-UC4 will be tested.

As the implementation of the maritime communications application derived from MT-UC3 was planned to be completed in Phase 2, we have not been able to validate most of the requirements for this use case. However, care has been taken that the non-functional requirements of the use-cases are considered and regarded with importance.

Finally, according to the validation plan, the full validation of MT-UC04 will be performed in Phase 2 of the validation. For this phase of the validation a basic outline of the prototype is illustrated along with its output.

7 Medical Data Exchange

The huge amount of data generated everyday by citizens, public administrations and companies is a valuable asset that need to be managed properly in terms of security and privacy. The digital economy boosts the use of these data by companies and organizations which must follow the regulatory framework (e.g. GDPR) and must assure the data are protected when stored or in transit. Special consideration must be considered when personal and sensitive data are shared between different actors. These challenges are tackling by the Medical Data Exchange demonstrator. Namely the use case MD-UC2 is devoted to protecting user data by using anonymization process when sensitive health records are shared between the data providers and data consumers, leveraging the infrastructures provided by the Covid-19 exchange platform. This platform was created for exchanging data generated during the Covid-19 pandemic, in the context of the Medical Data Exchange demonstrator.

Three use cases were already defined in D5.1 [1]:

- MD-UC1 - Sharing Sensitive Health Data through an API
- MD-UC2 - Sharing Sensitive Health Data through Files
- MD-UC3 – Enhancing the security of on-boarding and accessing the COVID-19 Exchange platform

Since the DANS asset was the unique one implemented and ready to be integrated in this Phase 1, only the MD-UC2 has been validated.

7.1 Use Case MD-UC2

- This use case is intended to share health data files stored in the data exchange platform in a privacy-preserving manner.
- The validation strategy followed by the medical data exchange demonstrator is mainly based on the use of test cases. These test cases are created based on the use case MD-UC2 covering how the DANS asset (anonymization tool) is being used during the anonymization process of a file containing health sensitive data. This process is performed by the end users (data providers) of the platform. In this context the running test cases help to validate the functional, the security and privacy requirements and the non-functional requirements described in D5.1 [1] and compiled in section 7.1.9 Requirements Coverage. At the end of this validation process conducted by the end users it is expected to conclude that the provided anonymization asset fulfils the end users expectations in terms of security, privacy and user experience, and accomplishes with the current regulation when sharing sensitive data. Also, by using the DANS asset, it facilitates to data providers the engagement to the exchange platform. Finally, valuable feedback from the end users has been received for improving the tools offered by the Covid-19 exchange platform, which helps to control and take decisions to overcome the pandemic challenges.
- The validation will be performed by running the following 6 test cases:
- Test Case MD-UC2-TC-001: validating the whole anonymization process, engaging end users;
- Test Case MD-UC2-TC-002: validating the anonymization functionality as a service, engaging development team;
- Test Case MD-UC2-TC-003: validating the anonymization functionality as a library to be integrated in an application, engaging development team;
- Test Case MD-UC2-TC-004: validating the anonymization report provided by the anonymization tool as a service, engaging development team;
- Test Case MD-UC2-TC-005: validating the anonymization report provided by the anonymization tool as a library to be integrated in an application, engaging development team;

- Test Case MD-UC2-TC-006: validating the anonymization service provides the right answers to the end users if the system is not working properly.

7.1.1 Actors

The initial plan for creating a trust, secure and privacy-preserving environment when sensitive data are shared were focused on the creation of a medical data exchange platform. This data exchange platform was intended to be used by different health actors such as hospitals, pharmaceutical companies or health tech companies D5.2 [18] provides detailed information on these actors). Due to the Covid-19 pandemic started on March 2020 in Europe the availability of the different actors was compromised as their main efforts were dedicated for the fighting the pandemic. In this context the initial planned data exchange platform was adapted to the new situation and a Covid-19 Exchange platform was launched, keeping the same functionalities planned at the beginning of the project and able to interact with the user data privacy-preserving tools developed during the demonstrator time life. In this way the actors engaged are basically research organizations aiming to share data retrieved from the Covid-19 pandemic which can help to understand the behaviour of the pandemic and to obtain data for coping the challenges arisen.

The test cases described in the following sections have been run by three different actors:

- The development team for validating the basic functionalities provided by the DANS asset.
- The data Covid-19 platform administrators for validating the functional requirements the Covid.19 Data Exchange platform must cover.
- The end users (data providers) of the Covid-19 platform for validating the functionalities provided by the DANS asset and the platform performing the anonymization process on health data files to be shared in a privacy-preserving manner.

7.1.2 Test Case MD-UC2-TC-001

7.1.2.1 Description

A data provider uploads a health data file with its metadata to Covid-19 DEP. The sensitive data file is anonymized by the DANS tool and encrypted by the platform. A data consumer consults the metadata, signs a contract with the data provider for retrieving the agreed data, and retrieves the anonymized health data file ready to be analysed.

7.1.2.2 Test Case Workflow

Preconditions:

- A data provider is logged in COVID-19 Exchange platform.
- The data provider is allowed to use the privacy-preserving services
- A data consumer is logged in COVID-19 platform.
- Privacy-preserving CS4EU services (e.g. anonymization service) are available at COVID-19 platform.
- The data provider creates a file with personal and sensitive health data from a specific source.

Steps:

1. The data providers go, on the COVID-19 platform, to the profile of the cybersec4europe pilot; the profile contains the link to the service.
2. The data provider goes to the service.

3. The *data provider* selects the anonymization service (DANS) from the list of CS4EU privacy-preserving services.
4. The *data provider* anonymizes the file data by using the DANS service.
5. She uploads to the COVID-19 platform the anonymized file using the DANS.
6. the COVID-19 platform encrypts the result file as additional protection measure.
7. The *data provider* provides the metadata to the DEP.
8. The *data consumer* browses the catalogue and the metadata already provided, which gives her information about how to manage the anonymized data file. An assessment tool is available for improving the user experience during the browsing process.
9. The *data consumer* contacts to the *data provider* through the DEP to settle terms and conditions on the management of the requested data. The DEP provides specific contract services for this purpose.
10. The *data consumer* requests the selected health data to the DEP data exchange marketplace.
11. The data exchange marketplace provides her the anonymized and encrypted file.
12. The data consumer decrypts the file containing the health data anonymized, and she is able to perform any analytics over the data.

7.1.2.3 Test Results

The data consumer receives the anonymized health data file.

7.1.3 Test Case MD-UC2-TC-002

7.1.3.1 Description

A user (data provider) wants to anonymize a csv/excel data file with medical data records by using the DANS as a service. She analyses the anonymized data by generating the related report.

7.1.3.2 Test Case Workflow

Preconditions:

- A user (data provider) has a data file in csv/excel format, containing a set of personal-sensitive health data. The first row of such a file contains the name of the data fields (attributes), and the data arranged in columns.
- The user (data provider) knows which attributes are sensitive, insensitive, quasi-identifying and identifying. If the user wants to apply a generalization as the transformation process for the anonymization, she needs to create hierarchies associated to the attributes of the input data. Therefore, the user could have several hierarchy data files in csv format, used in the transformation of the related data during the anonymization.
- A microaggregation method could be applied as additional transformation procedure. The user must decide among the available ones (Mode, Median, Arithmetic mean, Geometric mean or Interval).
- The user must specify the privacy models to be applied according to the attribute types, if she wants to preserve the privacy of these attributes:
 - o For the quasi-identifying attributes, K-anonymity and the K parameter.
 - o For the sensitive attributes, L-diversity and the L parameter.

Steps:

1. Upload the data file:

POST "<https://vm.project-cs4eu.eu:9083/dans/uploadFile>"

2. Upload the hierarchy files:

POST "<https://vm.project-cs4eu.eu:9083/dans/uploadFile>"

3. Choose to anonymize or to get an anonymization report:
 - a. If anonymizing the data file with the transformation input:

POST <https://vm.project-cs4eu.eu:9083/dans/file/{fileId}> & response content type = text/plain

- b. If getting the anonymization report with the transformation input:

POST <https://vm.project-cs4eu.eu:9083/dans/file/{fileId}> & response content type = application/pdf

7.1.3.3 Test Results

If the data provider selected the anonymization option, she got the **anonymized data set** in csv format, according to the transformation procedure applied.

If the data provider chose the report option, she got the **report** with some statistical data about the anonymization she specified to be applied to the source data.

7.1.4 Test Case MD-UC2-TC-003

7.1.4.1 Description

A user wants to anonymize a csv/excel data file using the DANS anonymization tool as a java library. She analyses the anonymized data by generating the related report.

7.1.4.2 Test Case Workflow

Preconditions:

- A user (data provider) has a data file in csv/excel format, containing a set of personal-sensitive health data on a local path at her computer. The first row of such a file contains the name of the data fields (attributes), and the data arranged in columns.
- The user (data provider) knows which attributes are sensitive, insensitive, quasi-identifying and identifying. If the user wants to apply a generalization as the transformation process for the anonymization, she needs hierarchies associated to the attributes of the input data. So, the user has several hierarchy data files in csv format, used in the transformation of the related data during the anonymization, on a local path at her computer.
- A microaggregation method could be applied as another transformation procedure. The user must decide among the available ones (Mode, Median, Arithmetic mean, Geometric mean, Interval).
- The user has to specify the privacy models to be applied according to the attribute types, if she wants to preserve the privacy of these attributes:
 - o For the quasi-identifying attributes, K-anonymity and the K parameter.
 - o For the sensitive attributes, L-diversity and the L parameter.

Steps:

1. Invoke the following method belonging to the class *DansSimpleService*, specifying to true if anonymizing or generating an anonymization report:

Resource dansData (DANSinput dansInput,

boolean isAnonymFileReturned,
boolean isStatisticDataReturned,
String myPath)

7.1.4.3 Test Results

If the data provider selected the anonymization option, she got the **anonymized data set** in csv format, according to the transformation procedure applied, in the specified path.

If the data provider chose the report option, she got the **report** pdf file with some statistical data in the path just specified, according to the anonymization she specified to be applied to the source data.

7.1.5 Test Case MD-UC2-TC-004

7.1.5.1 Description

A user wants to anonymize a csv/excel data file, or to study the statistics data which would describe the anonymization process for a transformation input data provided for the former data file

The data source or any given hierarchy file have not been uploaded.

7.1.5.2 Test Case Workflow

Preconditions:

- A user (data provider) has a data file in csv/excel format, containing a set of personal-sensitive health data. The first row of such a file contains the name of the data fields (attributes), and the data arranged in columns.
- The user (data provider) knows which attributes are sensitive, insensitive, quasi-identifying and identifying. If the user wants to apply a generalization as the transformation process for the anonymization, she needs hierarchies associated to the attributes of the input data. So, the user has several hierarchy data files in csv format, used in the transformation of the related data during the anonymization.
- A microaggregation method could be applied as another transformation procedure. The user must decide among the available ones (Mode, Median, Arithmetic mean, Geometric mean, Interval).
- The user must specify the privacy models to be applied according to the attribute types, if she wants to preserve the privacy of these attributes:
 - o For the quasi-identifying attributes, K-anonymity and the K parameter.
 - o For the sensitive attributes, L-diversity and the L parameter.

Steps:

1. Upload the data file:

POST "<https://vm.project-cs4eu.eu:9083/dans/uploadFile>"

2. Upload the hierarchy files:

POST "<https://vm.project-cs4eu.eu:9083/dans/uploadFile>"

3. Anonymize the data file or generate the report with a transformation input, but this input does not contain the specified file identifiers got in the above steps:

POST <https://vm.project-cs4eu.eu:9083/dans/file/{fileId}> & response content type = text/plain or application/json

7.1.5.3 Test Results

The user gets an error message showing there is no data file/hierarchy file.

7.1.6 Test Case MD-UC2-TC-005

7.1.6.1 Description

A user wants to anonymize a csv/excel data file or to generate the anonymization report using the DANS as a java library, but the path to the files is wrong.

7.1.6.2 Test Case Workflow

Preconditions:

- A user (data provider) has a data file in csv/excel format, containing a set of personal-sensitive health data on a local path at her computer. The first row of such a file contains the name of the data fields (attributes), and the data arranged in columns.
- The user (data provider) knows which attributes are sensitive, insensitive, quasi-identifying and identifying. If the user wants to apply a generalization as the transformation process for the anonymization, she needs hierarchies associated to the attributes of the input data. So, the user has several hierarchy data files in csv format, used in the transformation of the related data during the anonymization, on a local path at her computer.
- A microaggregation method could be applied as another transformation procedure. The user must decide among the available ones (Mode, Median, Arithmetic mean, Geometric mean, Interval).
- The user must specify the privacy models to be applied according to the attribute types, if she wants to preserve the privacy of these attributes:
 - o For the quasi-identifying attributes, K-anonymity and the K parameter.
 - o For the sensitive attributes, L-diversity and the L parameter.

Steps:

1. Invoke the following method belonging to the class *DansSimpleService* with a wrong path or a non-existent one:

```
Resource dansData (DANSInput dansInput,  
boolean isAnonymFileReturned,  
boolean isStatisticDataReturned,  
String myPath) // Specify a wrong path here
```

7.1.6.3 Test Results

The user gets an error message since the files have not been found in the path just specified.

7.1.7 Test Case MD-UC2-TC-006

7.1.7.1 Description

A user wants to analyse the anonymization/or to anonymize the source data. During the anonymization process something unexpected event happens, and an error is returned to the end user.

The unexpected events tested were:

- The transformation input data are not correct.
- The format of the files to be uploaded is not one of the allowed ones (csv/excel).
- The hierarchy files/data source files are not found.
- The certificate of the machine expired.
- The DANS was not running.

7.1.7.2 Test Case Workflow

Preconditions:

- A user (data provider) has a data file in a given format, containing a set of personal-sensitive health data. The first row of such a file contains the name of the data fields (attributes), and the data arranged in columns. *(Suppose that the file format is neither cvs nor excel. An error occurs.)*
- The user (data provider) knows which attributes are sensitive, insensitive, quasi-identifying and identifying. If the user wants to apply a generalization as the transformation process for the anonymization, she needs to create hierarchies associated to the attributes of the input data. Therefore, the user could have several hierarchy data files in csv format, used in the transformation of the related data during the anonymization. *(Suppose not all the expected hierarchy files are uploaded. An error occurs.)*
- A microaggregation method could be applied as additional transformation procedure. The user must decide among the available ones (Mode, Median, Arithmetic mean, Geometric mean or Interval).
- The user must specify the privacy models to be applied according to the attribute types, if she wants to preserve the privacy of these attributes:
 - o For the quasi-identifying attributes, K-anonymity and the K parameter.
 - o For the sensitive attributes, L-diversity and the L parameter.

Steps:

(If the DANS is not running, or the certificates expired or the server is down, the swagger API will not work.)

1. Upload the data file:

POST <https://vm.project-cs4eu.eu:9083/dans/uploadFile>

(If the format file is not allowed, an error will be returned.)

2. Upload the hierarchy files:

POST <https://vm.project-cs4eu.eu:9083/dans/uploadFile>

(If the format files are not allowed, an error will be returned.)

3. Choose to anonymize or to get an anonymization report:

(If the transformation string is not syntactically correct, an error will be returned.)

(If the transformation string is correct but the specified files are not found, an error will be returned.)

- a. If anonymizing the data file with the transformation input:

POST <https://vm.project-cs4eu.eu:9083/dans/file/{fileId}> & response content type = text/plain

- b. If getting the anonymization report with the transformation input:

POST <https://vm.project-cs4eu.eu:9083/dans/file/{fileId}> & response content type = application/pdf

7.1.7.3 Test Results

No anonymization takes place. The user gets an error message showing what is happened.

7.1.8 Quality Indicators

This section provides the quality indicators based on the effectiveness and efficiency of the solution.

7.1.8.1 Effectiveness and efficiency of the solution

In the Medical Data Exchange demonstrator, the following indicators have been covered:

- **Integration and interoperability:** DANS APIs are publicly exposed on the developer partner premises. The Swagger APIs (generated with the OpenAPI Specification²³) of the DANS asset provides a direct access to the service and their functionalities (e.g. anonymize files, manage hierarchy files or retrieve statistic report of the anonymization process), providing examples of the type of every parameter used. Since the anonymization service is running as a service, the operations can be invoked from other systems;
- **Documentation:** A user guide documentation is provided to the end users for validation. This guide contains examples, tutorials for easing the use of the anonymization tool, APIs provided by the DANS tool are specified and documented. During this phase 1 the anonymization service (DANS) has been deployed only on the developer partner infrastructure for an easy management. The documentation related with installation, configuration and integration of the anonymization service will be provided to the end users in phase 2. README files providing information on the anonymization tool is already prepared, and information on installation, configuration and integration will be included in phase 2;
- **Usability:** Based on the feedback provided by the end-users is foresee to provide a basic user interface during the phase 2 for facilitating the use of the DANS as a service. The DANS asset is provided in two flavours. DANS as a service to be deployed on the data provider infrastructure or on third-party premises, and as a java library to be integrated into legacy applications developed by the data provider;
- **Source code management and automated CI testing:** The DANS asset java code (DANS as a service and as a java library), are managed through GitLab at ATOS premises. As any repository in this software development platform, the version control, issue and merge request tracking, make easier the code maintenance;

²³ <https://swagger.io/specification/>

- **Deployment:** DANS (as a service) code is ready to be dockerized and is deployed on the developer partner premises as a docker container. On the other hand, DANS library (a jar library) can be integrated in modules or applications implemented by the end users (data providers).

7.1.9 Requirements Coverage

The following table shows how each MD requirement has been validated. The descriptions of the requirements come from the deliverable D5.1 [1]. Notice the modal verbs in the description column indicate the mandatory nature of each requirement, according to the RFC 2119 - IETF [16].

ID	Description	Validated	Strategy	Result	Comments
MD-SP01	<i>When personal and sensitive data are shared, data providers MUST preserve the data subjects' privacy by using privacy-preserving techniques</i>	Yes	Test Case MD-UC2-TC-002 Test Case MD-UC2-TC-003	Success	k-anonymity and l-diversity privacy models are available to be used in the DANS asset.
MD-SP02	<i>When personal and sensitive data are shared, data providers MUST preserve the data subjects' privacy by using anonymization tools</i>	Yes	Test Case MD-UC2-TC-002 Test Case MD-UC2-TC-003	Success	k-anonymity and l-diversity privacy models are available to be used in the DANS asset.
MD-SP03	<i>Communications between data providers and data consumers through the platform to exchange health data MUST be</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security police ^[1]

ID	Description	Validated	Strategy	Result	Comments
	<i>protected by security associations, in order to avoid leaks of sensitive information</i>				
MD-SP04	<i>Communications between data providers and data consumers through the platform to exchange health data MUST be protected by security associations, preserving data integrity</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹
MD-SP05	<i>Data subject's health data MUST be protected at any time by using an encryption scheme that allows to ensure their confidentiality</i>	-	N/A		Not apply to this UC
MD-SP06	<i>Data subject's health data MUST be protected at any time by using an encryption scheme that allows to</i>	-	N/A		Not apply to this UC

ID	Description	Validated	Strategy	Result	Comments
	<i>ensure their integrity</i>				
MD-SP07	<i>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</i>	-	N/A		Not apply to this UC
MD-SP08	<i>The marketplace MUST provide sharing contracts between data providers and data consumers</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹
MD-LF01	<i>A schema for metadata MUST be defined and provided by Dawex marketplace. The schema MUST use a well-known standard (such as XSD).</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹

ID	Description	Validated	Strategy	Result	Comments
MD-LF02	<i>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</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹
MD-OP01	<i>All the legal conditions for the exchange of sensitive health data MUST be provided by the marketplace</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex compliance police ¹²¹
MD-OP02	<i>Definition of the taxonomy related to medical data MUST be provided</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹
MD-MP01	<i>Marketplace SHOULD consider the final user feedback for updating the platform</i>	Yes	Test Case MD-UC2-TC-001	Success	Feedback from end users has been collected (see section 2.3)
MD-SPL01	<i>Data subjects' personal data MUST be protected at</i>	No	Test Case MD-UC2-TC-001	No case yet	We are not using personal data as the data

ID	Description	Validated	Strategy	Result	Comments
	<i>any moment avoiding third parties can learn from the data</i>				are anonymized.
MD-SPL02	<i>Data providers MUST be able to provide data from multiple sources in an adequate form to data consumers for analytics</i>	Partially	Test Case MD-UC2-TC-002 Test Case MD-UC2-TC-003	Success	The allowed formats of the data files from the data providers are csv and excel. The available formats for the anonymized data files to be consumed by the data consumers are csv and pdf (this one with report data.)
MD-SPL03	<i>The data exchange marketplace SHOULD allow shared data monetization. The data owner can be remunerated when its health data are used.</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹
MD-LR01	<i>The data subjects' privacy MUST be preserved at any time. Towards this end, data providers and data consumers MUST fulfil</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex compliance police ²

ID	Description	Validated	Strategy	Result	Comments
	<i>the GDPR regulation and accomplish the data subjects' rights.</i>				
MD-LR02	<i>The marketplace MUST provide sharing smart contracts between data providers and data consumers</i>	Yes	Test Case MD-UC2-TC-001	Success	See Dawex security and privacy police ¹

Table 32: Medical Data Exchange – MD-UC2 Validation requirements' coverage.

^[1] <https://www.dawex.com/en/security-privacy/>

^[2] <https://www.dawex.com/en/compliance/>

7.2 Validation Summary

The Medical Data exchange pilot has been validated by passing the test cases specified in the former section. Some of those test cases were performed by the end users, and the most technical ones were passed by the development team.

The following table provides the validation summary:

ID	Validated	Result	Comments
Test Case MD-UC2-TC-001	Partially	Success	<p>This test validates the COVID-19 Exchange platform with the DANS asset.</p> <p>Two requirements are not completely covered yet: MD-SPL01 and MD-SPL02 (see Table 1: T5.6 – IDMD-UC2 Validation requirements' coverage.)</p>

ID	Validated	Result	Comments
Test Case MD-UC2-TC-002	Yes	Success	This an asset test, without integration in the COVID-19platform.
Test Case MD-UC2-TC-003	Yes	Success	This an asset test, without integration in the COVID-19 platform.
Test Case MD-UC2-TC-004	Yes	Success	This an asset test, without integration in the COVID-19 platform.
Test Case MD-UC2-TC-005	Yes	Success	This an asset test, without integration in the COVID-19 platform.
Test Case MD-UC2-TC-006	Yes	Success	This an asset test, without integration in the COVID-19 platform.

Table 33: Medical Data Exchange demonstrator's use cases validation summary.

7.3 Lessons Learned and Future Work

The validation of the requirements indicated in Table 25 demonstrates that the initial goals planned for MD-UC2 has been reached. According to the summary of the validation shown in Table 26, only one of the Test cases has been covered partially as not all the protected tools has been developed in phase 1 (crypto tool for end-to-end encryption will be completed in phase 2).

Additionally, a highly valuable feedback has been provided by the end users (team of data scientist working for a French health corporation (pharmaceutical sector)). The main aspects to be considered in the future releases of the DANS asset are related to the next points:

- **Returned codes:** Provide more returning codes, in order to give more detailed information of the results to the user.
- **Graphical user interface:** Substitute the swagger API into a more user-friendly interface, not so much technical.
- **Ease of Use:** The guide that represents the usage of a tool to anonymize sensitive data, on a theoretical level, the idea is clear and well represented. On the other hand, the technical representation is insufficient especially for inexperienced users (non-technical users). The structure of the file that specifies the hierarchy of quasi-sensitive attributes is superficially explained. The JSON input for the metadata will vary according to the file to be anonymized. For this reason, inexperienced users will be unable to test or benefit from such a tool.
- **Importance of the tool:** The concept of anonymization of sensitive data through either the generalization and fitting attributes into higher-level classes. The micro-aggregation procedure or

the privacy models like quasi-identifying attributes (K-anonymity) and the sensitive attributes (L-diversity) remain very important methods. When they deal with sensitive data and information, they facilitate the transferability of data and information yet keep high-level compliance with the privacy issue, especially in sectors tackling personal data.

Based on this feedback the future work planed for the following versions of the DANS assets will be the following:

- Develop a basic user interface that can help the end users to work with this asset in a friendly way;
- Add new code messages providing more useful information to the end users. The information provided will be enough to be informed on the process but keeping security, not giving information can compromise the service.
- Update DANS user guide with additional explanations.

8 Smart Cities

Smart cities demonstrator cases have been focused on two main goal:

- Setup and put in operation a user centric infrastructure to support sensor and other urban data platform and infrastructure for identity and personal data exchange and their reuse in public services, in compliance with GDPR;
- Setup an Open Innovation cycle that will drive city stakeholders from cyber security risks and needs assessment to the identification of the related solutions for cyber security and privacy.

In order to address Smart Cities security and privacy objectives a set of challenges have been identified in line with the results of WP4 activities. In this context the demonstrators of Murcia, Porto and Genova have been focused on implementing and putting on operation, some of the use cases identified and described in D5.1 and D5.2 by deploying, testing and validating a set of solution prototypes, scouted from WP3 activities, mainly in this first stage individually, to address the identified challenges.

The main outcome of Smart Cities demonstrator activities is 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 cyber security risks and regulations compliance based on trust 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 Cities.

Specifically the contexts of use cases validated in this first stage in Murcia, Genova and Porto are the following:

- Murcia: extending the security and privacy aspects in smart city data platform;
- Genova: user centric privacy consent management, assessment and prevention of cyber security attacks and estimating attacks impact;
- Porto: anonymization and privacy-preserving models for sensor network platform.

For each use case a set of validation test cases have been planned and performed to validate the security and privacy requirements identified in D5.2. Some requirements have been (or partially) covered through the adoption of specific solution adopted in the defined validation scenarios. The selection and adoption of the identified solutions have been validated also from a quality point of view by analyzing in first phase only indicators on their effectiveness and efficiency.

Although in general only internal actors have been involved in this first phase, some questionnaires have been presented in order to make a first evaluation on the quality of the solutions.

8.1 Use Case SMC-UC2

For the first phase, we have planned to validate subcases related to data consumption from the Smart City platform. For this phase, only internal validation (using a lab test) is planned, analysing the technology involved in the test cases. As no end-user questionnaires will be made, the success of the validation will depend on the correct execution of the test cases and the evaluation of the technologies used, along with internal (but non-members of the project) questionnaires/feedback about the quality.

In this evaluation, three of the assets identified in WP3 for the Smart City challenges will play a key role :

- ppIdM : It is used to perform the authentication and authorization of users against the smart-city platform in a privacy-preserving way. In the demonstrator, it corresponds to the specific deployment of an OLYMPUS virtual IdP composed of three individual IdPs.

- **Mobile p-ABC** : As the tool to gain privacy in authentication/authorization. This demonstrator is based in a new p-ABC approach evolving from previous solutions like Idemix. Issuance and presentation processes are those of novel *PS-MS* crypto that increase the efficiency.
- **eIDAS browser** : It is key for performing id-proofing of the users against the ppIdM, achieving strong linkage with physical identity. In the demonstrator, it is integrated in the Android app for eIDAS authentication via NFC using Spanish ID card (DNIe), and also for using digital certificates based on *CI@ve* Spanish system. It relies on the Keyrock component as a bridge to eIDAS.

8.1.1 Actors

For the first phase, the only actors involved in the evaluation will be developers, which will carry out technical tests, and researchers/experts that will complete a questionnaire for feedback. Other actors (and stakeholders) that have been identified as potential participants of the use case, like citizens or service providers (as per D5.2), will be included in subsequent evaluations.

8.1.2 Test Case SMC-UC2-TC01

This section describes a technical test case to validate some of functional and non-functional requirements related to security and privacy aspects covered by the use case.

8.1.2.1 Description

The test case is based on an application that uses the services offered by the MiMurcia Smart City platform. It has to follow the necessary steps for authentication/authorization, and we can test that they are correctly integrated, secure and privacy-preserving. For the test case three services will be used, which present the user with a map that contains specific information:

- **Public transport**: The user does not need any special characteristic to use this service.
- **Parking availability**: The user needs to be over 18 to use this service.
- **Water consumption**: The user needs to be from Murcia to use this service.

Multiple components are involved in this test. Figure 62 shows them, as well as a simplified flow of the test. In the following, we include a brief description of the components and their role:

OLYMPUS vIdP: OLYMPUS virtual identity provider comprised of multiple individual IdPs. Leverages distributed p-ABCs to offer privacy-preserving (minimal disclosure and unlinkability) authentication (presentation of attributes).

Keyrock: Identity management system used as a bridge to eIDAS (i.e., handles SAML communication flow with eIDAS node to obtain certified attributes).

eIDAS node: Handles authentication (of a natural person in the first pilot) with an electronic certificate or national eID following the eIDAS specification.

MiMurcia: Smart city platform that offers services for Murcia city.

- **Services**: Public transport, parking availability... Information.
- **PEP**: Controls access to the services, checking that the request includes a valid capability token (i.e., the request is authorized).
- **Capability Manager**: Generates capability tokens that bestow authorization to use specific services. Relies on the PDP for the decision (using XACML).

PDP: Checks if an authorization request should be conceded, using the OLYMPUS verification library to validate the presentation token against the policy.

8.1.2.2 Test Case Workflow

The following figure summarizes the test case workflow:

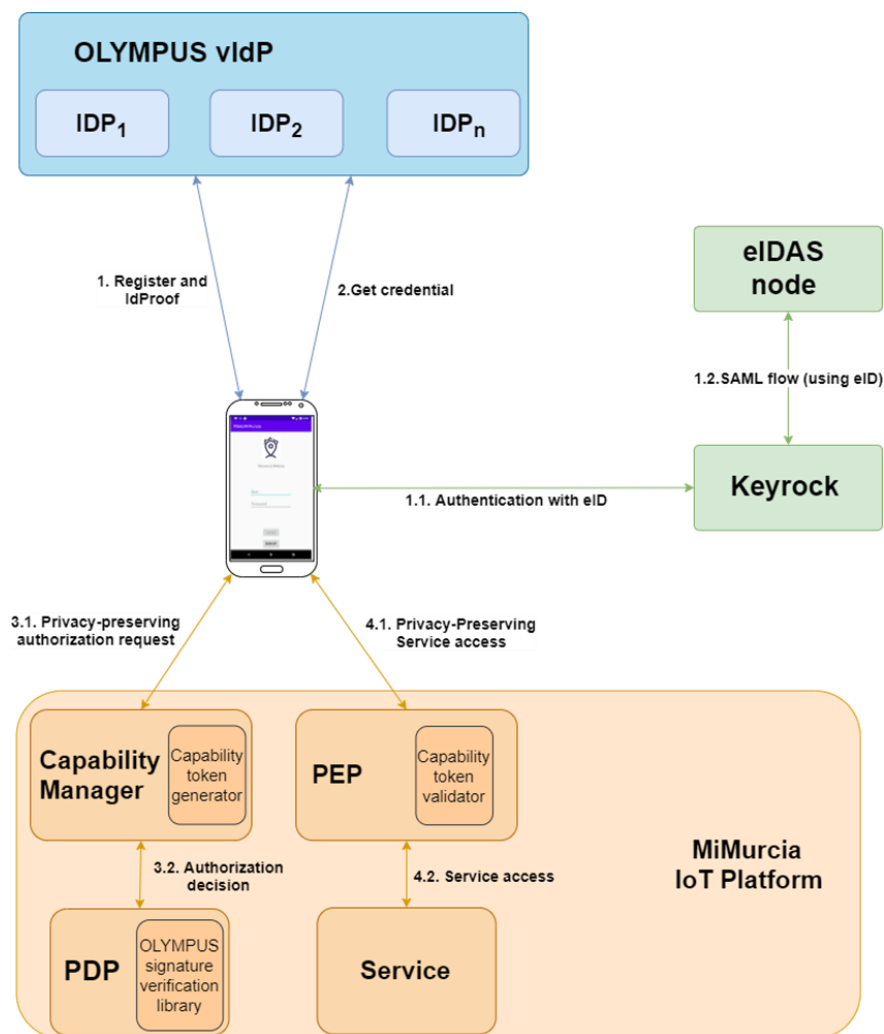


Figure 62: Test case SMC-UC02-TC01 summary

The user, not registered, clicks the button **New Credential** and selects sign up to create a new user to generate the credential. After writing the needed information (user and password), the user clicks on the confirm button and is redirected to Keyrock to login (*step 1.1*). The user selects to login with eID, is redirected to the Spanish eIDAS node and chooses between using electronic certificate, national eID, or login as a European citizen (*step 1.2*). Finally, the eIDAS node and the IdM respond with the assertion which contains the certified attributes, so the user can perform Id Proving and her OLYMPUS account will have the information needed to generate credentials (*step 1*). Before going back to the main menu, the app transparently retrieves a credential for the user (*step 2*). Now, the user can click to use a service. The application will retrieve the policy associated to the service from the Smart City Platform and ask if the user wants to share the requested attributes from her credential. If she accepts, the app will use the credential to perform a Zero-Knowledge presentation and obtain an authorization token (*steps 3.1 and 3.2*). The user is then redirected to the service (*steps 4.1 and 4.2*). In future interactions, the user will be able to reuse the stored credential to access services and also obtain new credentials (e.g., when the stored one expires) simply by login with the username and password she chose.

8.1.2.3 Test Results

The application allows users to register in the Smart City platform using strong identity from eIDAS and to perform the task of accessing the services offered by the platform, performing the necessary authentication/authorization steps while preserving their privacy.

8.1.3 Technology Based Analysis

Some requirements have been demonstrated and validated by the intrinsic features of the component of the system integrated in the use case and not explicitly described in the above test case.

8.1.3.1 SMC-SP01- Solution ensures that authentication is implemented

Yes. The Smart City platform must be accessed through PEP using Capability Tokens, and the user must authenticate (based on ppIdM) to obtain them from the Capability Manager.

8.1.3.2 SMC-SP02- Keep sensitive information secured and accessible only to authorized users

Partially. Services are protected by specific access policies, and users must prove they fulfil them in order to access. Credentials are stored in an encrypted wallet on user side. User data in vIdP (ppIdM) can be securely stored (e.g., encrypted database) but for first test a simple unsecure implementation is used.

8.1.3.3 SMC-SP04- 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

Partially. All communications can be protected using SSL (they are all HTTP/S based), and they are, excepting test services (communication between PEP and test data services is currently HTTP).

8.1.3.4 SMC-SP06- Solution provides data provenance, so that it allows for auditing of data access and update on secured data

Partially. User data for registration against the ppIdM comes from eIDAS assertions (linked to an eIDAS node public certificate). For the Smart City platform, data access is completely anonymized.

8.1.3.5 SMC-SP10- 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

Partially. It is supported, and communications are indeed protected using SSL except in the case of the test services.

8.1.3.6 SMC-SP11- Solution should have a secure store for keys and be able to integrate with key stores.

Yes. Server keys are protected in keystores, and user credentials are currently stored using Android secure storage (could be any kind of wallet).

8.1.3.7 SMC-SP16- Personal data has to be stored in a protected way (e.g. encryption, hashing);

Partially. It is encrypted on user side. In the ppIdM encrypted storage is simple to integrate but for testing it is not yet implemented.

8.1.3.8 SMC-SP19- 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

Yes, as the ppIdM used for authentication and authorization offers minimal disclosure/anonymization by design (based on p-ABC technology).

8.1.3.9 SMC-SP22- Demonstration case solutions should prevent the possibility of creating central surveillance on users or groups of users.

Yes, thanks to the decentralized ppIdM+dp-ABC approach, the ppIdM cannot spy users, and the Smart City platform (acting as service provider) will not be able to either (unless users explicitly decide to show identifying information).

8.1.3.10 SMC-SP23- The establishment of technological practices for security and privacy should be based on open architectures and standards

Yes. All architectural and cryptographic tools used are public.

8.1.4 Quality Indicators

For this first phase, only internal validation (using a lab test/pilot) is planned, analysing the technology involved in the test cases, so no questionnaires for end-users/stakeholders will be used, although internal questionnaires for feedback will be considered.

8.1.4.1 Effectiveness and efficiency of the solution

This category comprises the following subcategories:

- integration and interoperability (KPI_QAI)
- documentation (KPI_QAD)
- usability (KPI_QAU)
- source code management (KPI_QASCM)
- testing (KPI_QAT)
- deployment (KPI_QADPY)

KPI_QAI_01: Integration and interoperability. The functionality of the components is exposed for example via JSON REST/RPC APIs for the integration with other systems. The functionality in this way is made available for the server-side components and for the UI components.

Indicator	Description	Evaluation
API exposure	Solution client and server exposure both as code library and REST interface. Authorization API exposed as REST	Yes.
Level of simplicity, adaptability and functionality of the	Service is readily adoptable and applicable in at least 50% of cases	Not completely evaluated, but questionnaires show that the API of the ppIdM offers enough functionality (87.5% strongly agree, 12.5%) and

Indicator	Description	Evaluation
API perceived by developers.		integration of the ppIdM client is easy to understand (50% strongly agree, 50% agree)
Support Single Sign-On to allow for using single credentials across different applications.	Solution should support ≥ 1 SSO systems	Yes, using the ppIdM.

KPI_QAD_01: Installation, configuration, and integration documentation. For each component README file providing i) the component installation instructions; ii) the component configuration instructions; and iii) component integration instructions defining the necessary steps to set up the integration with other components.

We provided readme with installation/configuration instructions for the ppIdM server, and documentation for integration of client side. In surveys, 62.5% strongly agreed and 37.5% agreed that the readme was easy to follow, and 50% strongly agreed and 50% agreed that the client integration steps were easy to understand.

KPI_QAD_02: Specification and documentation for the APIs.

Indicator	Description	Evaluation
Level of completeness on the API documentation perceived by developers.	Surveys should reveal that the service has adequate documentation in at least 50% of cases	Documentation of ppIdM API, installation and integration guides have received good evaluations in surveys (at least 3,5 score in the related questions, where 2 would be a 50-50 split between favourable and unfavourable answers).
Level of understandability on the API documentation perceived by developers.	Surveys should reveal that the service has clear documentation in at least 50% of cases	First survey shows 75% strongly agree and 25% agree that the ppIDM API documentation is clear and understandable

KPI_QAD_03: Additional documentation (examples, tutorials, etc). the documentation should provide the description of the usage scenarios of the component, examples (e.g., API call inputs and outputs, testing instructions, tutorials, howto, etc). (Not really)

KPI_QAU_01: Usability and UX. Usability and User experience.

Indicator	Description	Evaluation
User perceived level of trust in the solution	>75% of user high or very high trust in surveys	62.5% <i>strongly agreed</i> and 37.5% <i>agreed to high level of trust</i>
App user friendliness, look and feel perceived by the user (simple to install, easy to navigate, provides use guidelines and information about problems, easy to remove)	Surveys should reveal that the service is perceived as reliable in at least 50% of cases	Reliability study was broken down for the three main processes: Enrolment: 62.5% Strong Agree, 25% Agree, 12.5% Strong disagree Login: 75% Strong Agree, 25% Agree Service access: 75% Strong Agree, 25% Agree
User consent is prompted to the user for user data sharing	>75% of users think that consent is clearly accomplished	62.5% Strongly agreed, 25% Agreed and 12.5% Disagreed
Consent Form is usable and user friendly	>75% users satisfied with the solution	62.5% Strongly agreed, 25% Agreed and 12.5% Disagreed (though some good feedback about more readable text)
General level of satisfaction with the solution (enrolment, authentication, authorization and usage processes, consent lifecycle management)	>75% users satisfied with the solution	50% show really high and 50% high level of satisfaction.

KPI_QASCM_01: Use of SCM and issue tracking. Any use of source code management repository and related issue tracking (**target:**1) *Using Git repositories for all components, and CI-Code coverage check for the ppIdM.*

KPI_QADPY_01: Docker containers provided. To further improve the deployment procedure allowing for targeting different Cloud environments. *Not yet*

KPI_QAT_01: Percentage of issues resolved. The issues reported during the process of the component development, integration, evaluation should be appropriately managed and resolved by the component owners. (**target:** >50% for the first stage) *Yes*

8.1.4.2 User and stakeholder engagement and impact evaluation

Although these KPIs will not be really considered in this phase, we can obtain a first ***rough approximation*** for some specific efficiency and effectiveness indicators through technical tests (with some light support from the questionnaire).

Indicator	Description	Target	Evaluation
Internal efficiency	Time to perform enrolment in the smart city pp-IdM	<3 seconds	668 ms * (combined with IdProof)
	Mobile IdProof through eIDAS	<4 seconds (subject to eIDAS performance)	668 ms * (combined with ppIdM enrolment). eIDAS auth process is not really measurable because it requires constant user input
	Throughput of enrolments (no. enrolments in some timeslot)	> 5000 / hour	Not measured yet
	Time to perform authorization in the smart city platform	<3 seconds	3240 ms*
	Throughput of authentications (no. authentications in some timeslot)	> 5000 / hour	Not measured yet
Internal effectiveness	Percentage of enrolment requests successfully completed	>95%	10 out of 10 tests completed. (3.375 score for the relevant question in the survey)
	Percentage of authentication requests successfully completed	>95%	10 out of 10 tests completed. (3.750 score for the relevant question in the survey)
	Percentage of authorization requests successfully completed	>95%	Needed 12 tries to complete 10 tests (83% succesful). (3.375 score for the relevant question in the survey)

*Time values obtained using a Poco X3 NFC, averaging between 10 measurements (taking these measurements was also considered for estimating reliability). The averages for the processes were:

Login: 1532 ms, Register and IdProof (with the ppIdM): 668 ms, Authorization: 3240ms, Get Policy: 373 ms

8.1.4.2.1 Questions

Following, a list of the questions asked in the internal questionnaire for feedback are listed, explaining the reasoning behind including each of them.

1. Do you think the content of the provided ppIdM API documentation is clear and understandable?

The ppIdM is a key component in this demo, and the quality of its documentation is a key indicator.

2. Has it been easy for you to follow the installation and configuration documentation of the ppIdM server?

The ppIdM is a key component in this demo, and the quality of its documentation is a key indicator.

3. Has it been easy for you to understand how to integrate the ppIdM client side in an application?

The ppIdM is a key component in this demo, and integration of the client in any app should be as simple as possible per the defined quality indicators.

4. Does the set of functionalities provided by the ppIdM cover the frequent needs about IdM?

The ppIdM is a key component in this demo, and feedback about its functionality is interesting for future development/features.

5. Please, add any additional comment regarding the ppIdM (e.g., proposal of new API functionalities...)

This question collects general feedback about the ppIdM if the respondent wishes to.

6. Is the enrolment (correct SignUp plus IdProof with eIDAS) process reliable?

This question aims to expand on the reliability study of the solution, apart from technical tests on this.

7. Is the credential obtention (correct login) process reliable?

This question aims to expand on the reliability study of the solution, apart from technical tests on this.

8. Is the service access (after the policy is accepted, getting a service or unauthorized message) process reliable?

This question aims to expand on the reliability study of the solution, apart from technical tests on this.

9. Please, briefly explain what scenario caused the most common error (e.g., after pressing service CapManger does not correctly answer)

Extra information about reliability/error cases on the pilot if the respondent wishes to.

10. Were the computations sufficiently efficient for...

10.1 The login process (from pressing the button until you are back to main menu)?

10.2 The enrolment process (from correct read of eID/certificate to being back to main menu)?

10.3. Service access process (from accepting policy until the service starts loading)?

Simple question about user “feel” on efficiency (to add extra context to first efficiency technical evaluations)

11. Please add any comment regarding time consumption and responsiveness of the different processes (e.g., a process takes a specially long time under specific circumstances)

Extra information on the efficiency topic, if the respondent wishes to.

12. Was the application informative enough about user data sharing, including asking consent in relevant steps?

Feedback about consent request and how informative is the solution, as it is a key quality indicator.

13. If not, please explain how the application fails to do so:

Feedback about consent request and how informative is the solution, as it is a key quality indicator.

14. Do you feel a high level of trust on the security and privacy offered by the solution?

Feedback about user trust, as needed by the correspondent quality indicator.

15. Please, point out what would be missing for an increased trust on the solution:

Extra feedback about user trust, for future development.

16. Do you trust technologically enforced privacy-guarantees more than those based on contracts and policies?

Some general feedback about privacy in digital interactions.

17. Do you think that maintaining privacy is important in everyday digital life?

Some general feedback about privacy in digital interactions.

18. General level of satisfaction with the app (please focus on user friendliness, functionality provided and trust)?

Feedback about the pilot solution in general.

19. Please, explain any suggestion you have to improve the application:

Feedback about the pilot solution in general, with possible future features/changes in mind.

8.1.4.2.2 Feedback

The following tables show the per unit representation of answers for the “option choosing” questions from the 16 completed surveys. Also, the score is a weighted average considering the following “score” values:

- Strongly agree: 4, Agree: 3, Disagree:2, Strongly Disagree: 1
- Really High: 5, High:4, Medium: 3, Low:2, Really low: 1

Question	Strongly Agree	Agree	Disagree	Strongly disagree	Score
1	0,750	0,250	0,000	0,000	3,750
2	0,625	0,375	0,000	0,000	3,625
3	0,500	0,500	0,000	0,000	3,500
4	0,875	0,125	0,000	0,000	3,875
5					
6	0,625	0,250	0,000	0,125	3,375

Question	Strongly Agree	Agree	Disagree	Strongly disagree	Score
7	0,750	0,250	0,000	0,000	3,750
8	0,750	0,250	0,000	0,000	3,750
9					
10.1	0,625	0,375	0,000	0,000	3,625
10.2	0,375	0,625	0,000	0,000	3,375
10.3	0,500	0,500	0,000	0,000	3,500
11					
12	0,625	0,250	0,125	0,000	3,500
13					
14	0,625	0,375	0,000	0,000	3,625
15					
16	0,500	0,500	0,000	0,000	3,500
17	1,000	0,000	0,000	0,000	4,000

Question	Really high	High	Medium	Low	Really low	Total
18	0,50	0,50	0,00	0,00	0,00	4,50
19						

As the “written answer” questions were optional, in the following we simply show the non-empty answers received for each of the relevant questions:

Question 5.

Answer 1. Two factor authentication would be welcome.

Answer 2. More technical examples of ppIdM API usage (JSON payload/response)

Question 9.

Answer 1. Used FNMT certificate and all went OK.

Answer 2. Connectivity issues, bad position of eID card

Answer 3. Reading eID through NFC is usually difficult

Answer 4. Sometimes PEP does not respond

Question 11.

Answer 1. Keypad OK should do a submit (eID CAN)

Answer 2. Service access usually takes some time

Question 13.

Answer 1. There should be a button/checkbox that ensures that the user read what is being asked.

Answer 2. The "attribute" requested text could be improved (more user-friendly)

Question 15.

Answer 1. Even if you know it is not, it feels a little "insecure" having to access using your password, as you are authorizing the app to access all your information (although, as I have already said, you know it only accesses to certain data).

Question 19.

Answer 1. Add the exit app when going back in Main Screen.

Answer 2. There should be an option to create an account on a computer, so Id be able to use a chip card reader to verify my id

Answer 3. Provide a way of seeing passwords when they are being written. Sometimes, the confirmation or enter buttons are hidden by the keyboard

Answer 4. Improve user experience in small screens.

Answer 5. The graphical interface could be improved.

Answer 6. Maybe a little of work with the interface (more visually "beautiful"), and improve loading times between sections.

Answer 7. n/a

8.1.5 Requirements Coverage

This section summarize the security and privacy coverage and results of the performed validation.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP01	Yes	Test Case SMC-UC2_TC01 Technology based	Success	Yes	The Smart City platform must be accessed through PEP using Capability

ID	Validated	Strategy	Result	Mandatory	Comments
					Tokens, and the user must authenticate (based on ppIdM) to obtain them from the Capability Manager.
SMC-SP02	Partially	Test Case SMC-UC2_TC01 Technology based	Success	Yes	Services are protected by specific access policies, and users must prove they fulfil them in order to access. Credentials are stored in an encrypted wallet on user side. User data in vIdP (ppIdM) can be securely stored (e.g., encrypted database) but for first test a simple unsecure implementation is used.
SMC-SP03	No	Test Case SMC-UC2_TC01		Yes	
SMC-SP04	Partially	Test Case SMC-UC2_TC01 Technology based	Success	Yes	All communications can be protected using SSL (they are all HTTP/S based), and they are, excepting test services (communication between PEP and test data services is currently HTTP).
SMC-SP05	Partially	Test Case SMC-UC2_TC01	Success	NO	Custom approach. p-ABC. Other technologies (SAML, XACML) are integrated
SMC-SP06	Partially	Test Case SMC-UC2_TC01 Technology based	Success	Yes	User data for registration against the ppIdM comes from eIDAS assertions (linked to an eIDAS node public certificate). For the Smart City platform, data access is completely anonymized.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP07	Partially	Technology based	Success	Yes	Not for all parties this requirement is covered byt the used technology
SMC-SP08	Partially	Technology based	Success	Yes	Not for all parties this requirement is covered byt the used technology
SMC-SP09	Partially	Technology based	Success	Yes	Not for all parties this requirement is covered byt the used technology
SMC-SP10	Partially	Test Case SMC-UC2_TC01 Technology based	Success	Yes	It is supported, and communications are indeed protected using SSL except in the case of the test services.
SMC-SP11	Yes	Test Case SMC-UC2_TC01 Technology based	Success	Yes	Server keys are protected in keystores, and user credentials are currently stored using Android secure storage (could be any kind of wallet).
SMC-SP12	Partially	Test Case SMC-UC2_TC01	Success	Yes	Some GDPR contemplated actions are not yet fully implemented
SMC-SP13	Partially	Test Case SMC-UC2_TC01	Success	Yes	Some "questions" are implicitly answered (e.g., why: to be able to access the service)
SMC-SP14	Yes	Test Case SMC-UC2_TC01	Success	Yes	User has to accept sharing data with the ppIdM (using certificate/eID) and with the Smart City platform (explicit ok message).
SMC-SP15	No			Yes	

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP16	Partially	Test Case SMC-UC2_TC01	Success	Yes	It is encrypted on user side. In the ppIdM encrypted storage is simple to integrate but for testing it is not yet implemented.
SMC-SP17	No			Yes	
SMC-SP18	Partially	Test Case SMC-UC2_TC01	Success	Yes	No unnecessary data (minimal disclosure)
SMC-SP19	Yes	Test Case SMC-UC2_TC01 Technology based	Success	Yes	The ppIdM used for authentication and authorization offers minimal disclosure/anonymization by design (based on p-ABC technology).
SMC-SP20	Yes	Test Case SMC-UC2_TC01	Success	Yes	Requested data (policies) are shown to the user (who has to consent) before sending them.
SMC-SP21	Yes	Test Case SMC-UC2_TC01	Success	Yes	
SMC-SP22	Yes	Test Case SMC-UC2_TC01 Technology based	Success	Yes	Thanks to the decentralized ppIdM+dp-ABC approach, the ppIdM cannot track users, and the Smart City platform (acting as service provider) will not be able to either (unless users explicitly decide to show identifying information).
SMC-SP23	Yes	Test Case SMC-UC2_TC01 Technology based	Success	Yes	All architectural and cryptographic tools used are public.
SMC-SP24	No	Test Case SMC-UC2_TC01	Success/Fail	Yes	No third-party reuse

Table 34: Smart Cities - SMC-UC02 Validation requirements' coverage.

8.2 Use Case SMC-UC3

The Municipality of Genova is currently redesigning both system architectures and administration processes, aiming at improving both efficiency and security of internal and external services.

Among the several tasks that such an activity can require, a set of mechanisms for improving a) the security of the stored data and b) the privacy management has to be adopted.

For what concerns privacy management, these mechanisms should help in managing both the record of data processing activities and the conservation of privacy consents given by each user.

This use case validates a user centric management of citizen personal data in compliance with the new GDPR and at the same time provide in an integrated manner tools for citizen to have more control on own privacy and more transparency on the use of own data (self-service transparency dashboard).

For this use case, we firstly analyzed the processes of collection and conservation of privacy consent. As previously mentioned, the Municipality offers multiple services to the citizens, sharing the need of compliance with the same requirements – as collecting user consents before actually providing the service.

The Municipality of Genoa decided to adopt the CaPe platform as a central mechanism for managing privacy consents and as means to manage privacy disclaimers. This means that CaPe will be integrated in the its global IT architecture, becoming a fundamental service to be employed by any service requiring the user to provide the confirmation of privacy disclaimer view and if any a privacy consent. Moreover, the role of CaPe in the whole architecture would enable – both to users and back office operators – to obtain an overview of the given consent forms for every service.

In this first phase of test and validation a lab replication (sandbox) of a set of identified online services have been performed in order to test, from and technical and operation point of view, the workflow of services provision with the introduction and interaction of the adopted solution by means of its APIs and dashboards.

In this use case and its related test the following main components have been adopted:

Consent based Personal Data Suite (CaPe) . A “consent based” and open source platform with the goal to manage and control “personal data” during the interaction among data subjects and public and private services as Data Controller and processors (PA, Social, IoT, B2C). It provides tools for lawful data sharing processes, with the ability to grant and withdraw consent to third parties for accessing own personal data. It follows the MyData principles to exploit the potential of personal data, facilitates its control and new business opportunities in compliance with the GDPR.

SPID test server. The Public Digital Identity System (SPID), is the solution that allows you to access the online services of the Public Administration and private companies with a single Digital Identity (username and password) that can be used by computers, tablets and smartphones.

Keyrock: Identity management system, one of GE of FIWARE platform, used as a bridge to SPID in order to implement a Service Provider module responsible for protecting an online resource and consuming information from the Identity Provider (SPID), namely handling SAML communication flow.

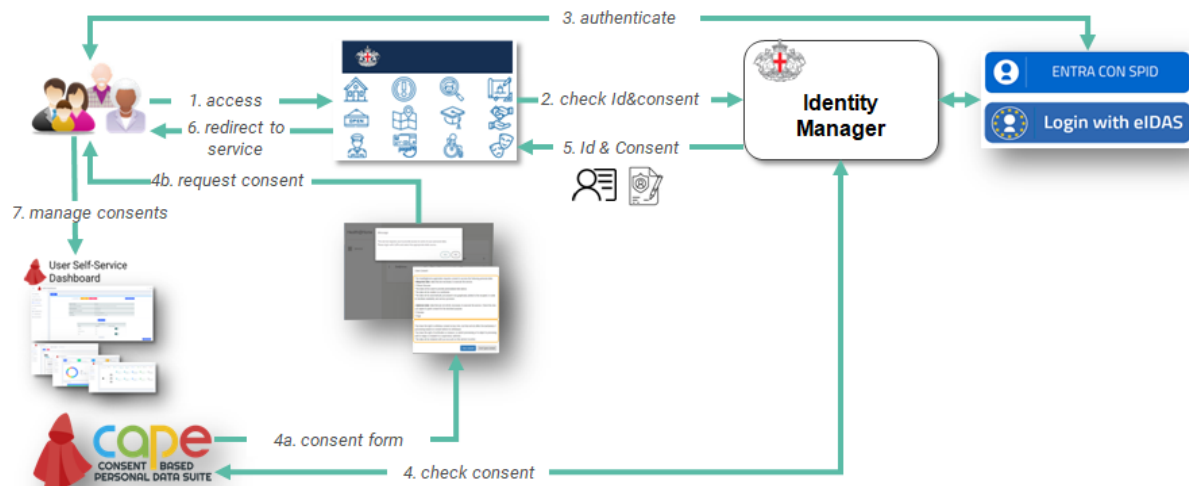


Figure 64 - Test case SMC-UC03-TC01 summary

1. A citizen wants to access one of the online services provided by the municipality. The enter point is the online service portal. Each service involved in the test case have been described previously according to the service model adopted by the CaPe solution and supported by a front end editor tool provided by the Data Controller Dashboard.
2. If citizen is not already authenticated the online service portal redirects to the service authentication system, in the specific case with SPID the Italian eIDAS scheme,
3. The authentication platform identifies the user and it checks if he/she has provided consent or privacy disclaimer acceptance. If not the authentication systems redirects to CaPe, (step 4)
4. CaPe shows the consent form, according to the related service description, and collects the opt-in opt-out answers contained in the consent form,
5. Identity and in case usage rules (from consent) are provided,
6. The user is redirected to the service, being able to use it.
7. Each citizen can control and manage consents through the "self-service" dashboard. The citizen can modify of consent, for example modify third parties disclosure or which personal data is allowed for the specified purpose or definitely withdraw the consent. The modifications are forwarded to the service on line portal by means of the CaPe SDK client. By means of the s Data Controller can view the status of each consent by means of the Data Controller Dashboard connected to the CaPe SDK client.

8.2.2.3 Test Results

The test case has successfully demonstrated the coverage of requirements related to the support of the end-to-end process of consent management. The solution adopted has been integrated in a current flow of online service provision of the municipality, the consent check have been performed by the online portal and a consent collection have been performed by mean of a dynamic consent form generated from the service description. Finally the citizen as data subject can manage the consents and check which data is used, how and for what purpose.

8.2.3 Technology Based Analysis

Some requirements have been demonstrated and validated by the intrinsic features of the component of the system integrated in the use case and not explicitly described in the above test case.

8.2.3.1 SMC-SP01- Solution ensures that authentication is implemented / SMC-SP05 Solution can be integrated with existing authentication mechanisms;

The solution adopted (CaPe) for a use centric consent management and its integration with Keyrock allow the integration with multiple SSO systems. At this phase only Keyrock embedded SSO solution and Online SPID test server have been tested.

8.2.3.2 SMC-SP02- Keep sensitive information secured and accessible only to authorized users

All the modules integrated in the scenario support Auth2.0 with multiple profile and also multi key encryption of any sensitive information stored in the solution adopted in the demonstrator keep sensitive information accessible only to authorized users and application.

8.2.3.3 SMC-SP04- 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-SP10- 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

All communication among modules, internally and externally, are protected using HTTPS. Only for lab test services that replicates the production ones in this first phase do not use HTTPS for their access.

8.2.3.4 SMC-SP06- Solution provides data provenance, so that it allows for auditing of data access and update on secured data

Audit Logging are assured only for consent managements and events related to interaction with CaPe and Keyrock solution and only data provenance metadata related to consent are managed and stored.

8.2.3.5 SMC-SP07- Solution is easy to protect and isolate parts from vulnerabilities;

The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator and it is compatible with the WSO2 ESB adopted by the municipality for its interoperability layer. This combination assures an adequate level protection and isolation.

8.2.3.6 SMC-SP11- Solution should have a secure store for keys and be able to integrate with key stores.

The multi key encryption of any sensitive information adopted in the demonstrator adopts server keystores and its isolation in each docker container with docker trust keystore.

8.2.3.7 SMC-SP16- Personal data has to be stored in a protected way (e.g. encryption, hashing);

Personal data used in the solution adopted in the demonstrator , namely consents and user authentications, are both encrypted and hashed by means of the multi key encryption provided by the solution.

8.2.4 Quality Indicators

For this first phase, only internal validation (using a lab test/pilot) is planned, analysing the technology involved in the test cases, so no questionnaires for end-users/stakeholders will be used, focusing mainly in the effectiveness and efficiency of the solutions adopted and integrated in flow of service online provision.

8.2.4.1 Effectiveness and efficiency of the solution

This category comprises the following subcategories:

- integration and interoperability (KPI_QAI)
- documentation (KPI_QAD)
- usability (KPI_QAU)
- source code management (KPI_QASCM)
- testing (KPI_QAT)
- deployment (KPI_QADPY)

KPI_QAI_01: Integration and interoperability. The functionality of the components is exposed for example via JSON REST/RPC APIs for the integration with other systems. The functionality in this way is made available for the server-side components and for the UI components.

Indicator	Description	Evaluation
API exposure	Solution client and server exposure both as code library and REST interface. Authorization API exposed as REST	YES, internal and external API exposed as REST
Level of simplicity, adaptability and functionality of the API perceived by developers.	Service is readily adoptable and applicable in at least 50% of cases	Quite completely adoptable and applicable to the use case performed for online service provision in the municipality. The API provided by the solution have been adapted and extended to the specific flow of online service provision, in particular regarding the automatic flow of service linking and consent check and related association to self service dashboard for personal data control
Support Single Sign-On to allow for using single credentials across different applications.	Solution should support ≥ 1 SSO systems	Support to SPID bridged by Keyrock solution. OAUTH2.0 Supported

KPI_QAD_01: Installation, configuration, and integration documentation. For each component README file providing i) the component installation instructions; ii) the component configuration instructions; and iii) component integration instructions defining the necessary steps to set up the integration with other components.

Yes. Each CaPe component provides a readme file listing the systems requirements and installation steps and configuration files to interact with the other components.

KPI_QAD_02: Specification and documentation for the APIs.

Indicator	Description	Evaluation
Level of completeness on the API documentation perceived by developers.	Surveys should reveal that the service has adequate documentation in at least 50% of cases	All APIs have Swagger documentation
Level of understandability on the API documentation perceived by developers.	Surveys should reveal that the service has clear documentation in at least 50% of cases	>75% of swagger API clearly described

- **KPI_QAD_03: Additional documentation (examples, tutorials, etc).** the documentation should provide the description of the usage scenarios of the component, examples (e.g., API call inputs and outputs, testing instructions, tutorials, howto, etc).

Yes. An additional document have been provided about the usage of the solution. Some example demos are provided how to use the components and some code snippets to use with the SDK provided by the CaPe solution.

- **KPI_QAU_01: Usability and UX.** Usability and User experience.

Indicator	Description	Evaluation
Minimal browser support. The component user interface (where available e.g. dashboards, forms, ect..) should provide support for the wide range of widely used browsers.	>1	Chrome and Firefox supported. Some graphical issues in mobile phone browser.
User perceived level of trust in the solution	>75% of user high or very high trust in surveys	n/a
App user friendliness, look and feel perceived by the user (simple to install, easy to navigate, provides use guidelines and information about problems, easy to remove)	Surveys should reveal that the service is perceived as reliable in at least 50% of cases	n/a
User consent is prompted to the user for user data sharing	>75% of users think that consent is clearly accomplished	n/a

Indicator	Description	Evaluation
Consent Form is usable and user friendly	>75% users satisfied with the solution	n/a
General level of satisfaction with the solution (enrolment, authentication, authorization and usage processes, consent lifecycle management)	>75% users satisfied with the solution	n/a

- **KPI_QASCM_01: Use of SCM and issue tracking.** Any use of source code management repository and related issue tracking (**target:1**)

GitLab and Github used for the all components adopted in the use case

- **KPI_QAD_01: Docker containers provided.** To further improve the deployment procedure allowing for targeting different Cloud environments.

Fine grained dockerization of all the components adopted in the use case

- **KPI_QAT_01: Percentage of issues resolved.** The issues reported during the process of the component development, integration, evaluation should be appropriately managed and resolved by the component owners. (**target: >50%** for the first stage)

>80% issued solved for the adaptation and adoption of the solutions in the use case

8.2.4.2 User and stakeholder engagement and impact evaluation

In this first phase no engagement and impact evaluation have been performed.

8.2.5 Requirements Coverage

This section summarize the security and privacy coverage and results of the performed validation.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP01	Yes	Test Case UC3_1	Success	Yes	At this first phase only solution embedded SSO and SPID test server have been tested
SMC-SP02	Yes	Technology based	Success	Yes	Multi key encryption of any sensitive information stored in the solution adopted in the demonstrator

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP03	Partially	Test Case UC3_1, Technology based	Success	Yes	Only related to consent management and events related to interaction with CaPe
SMC-SP04	Yes	Technology based	Success	Yes	All communications can be protected using SSL (they are all HTTP/S based), and they are except from test services
SMC-SP05	Partially	Test Case UC3_1, Technology based	Success	NO	Solution adopted in the use case provides bridge for SAML profile consumption. Only SPID test server tested
SMC-SP06	Partially	Test Case UC3_1, Technology based	Success	Yes	Only data provenance metadata related to consent are managed and stored. For the specific test case no metadata stored for data access
SMC-SP07	Yes	Technology based	Success	Yes	Fine modularity, Dockerization and isolation
SMC-SP08	Partially	Technology based	Success/Fail	Yes	Requirements full addressed from backend point of view according to the deployment and configuration adopted
SMC-SP09	Partially	Technology based	Success/Fail	Yes	Only log records
SMC-SP10	Partially	Test Case UC3_1, Technology based	Success/Fail	Yes	It is partially supported, messages and communications are protected using SSL
SMC-SP11	Yes	Test Case UC3_1, Technology based	Success	Yes	
SMC-SP12	Yes	Test Case UC3_1,	Success	Yes	

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP13	Yes	Test Case UC3_1,	Success	Yes	
SMC-SP14	Yes	Test Case UC3_1	Success	Yes	The consent manager supported by the solution adopted allow a double sign of the consent (Data Subject and Data Controller)
SMC-SP15	No				Supported by the solution adopted by not covered in the setup of the performed test case.
SMC-SP16	Yes	Test Case UC3_1, Technology based	Success	Yes	Personal data used in the solution adopted in the demonstrator are both encrypted and hashed by means of the multi key encryption provided by the solution
SMC-SP17	No				
SMC-SP18	Partially	Test Case UC3_1	Success	Yes	Requirements tested and addressed from the adopted tool point of view according to the usage rules related to the privacy disclaimer and collected consents supported by the adopted tools
SMC-SP19	Yes	Test Case UC3_1	Success	Yes	Data minimization applied according to the privacy rules
SMC-SP20	Yes	Test Case UC3_1	Success	Yes	Any comments here.
SMC-SP21	Partially	Test Case UC3_1	Success	Yes	Consent rules not enforced and tested in the data consuming

ID	Validated	Strategy	Result	Mandatory	Comments
					service selected for the validation
SMC-SP22	Partially	Test Case UC3_1,	Success	Yes	Requirements tested and addressed from the adopted tool point of view.
SMC-SP23	Yes	Test Case UC3_1	Success	Yes	The solution adopted in the demonstrator are open.
SMC-SP24	Yes	Test Case UC3_1	Success	Yes	The solution adopted in the demonstrator allow the data subject to manage consents by means of a self service dashboard.

Table 35: Smart Cities - SMC-UC03 Validation requirements' coverage.

8.3 Use Case SMC-UC4

For the first phase, we have planned to validate the exchanging and processing of information between the integration of pTASC and ARGUS for the marketplace use case. For this phase, only a lab test is planned, analysing the privacy-preserving techniques and API's for the integration involved in the test cases. As no end-user questionnaires will be made, the success of the validation will depend on the correct execution of the test cases and the evaluation of the technologies used, along with internal C3P feedback about the quality.

The laboratory testbed includes a FIWARE platform that integrates physical sensors and multiple computing devices with heterogeneous capabilities. Its purpose is to map a wide range of application scenarios and use cases, noise, humidity, temperature, luminosity and motion detection, to name a few. While many of our experiments are focused on security aspects of the physical sensors and respective computing platforms, in this demonstrator we also address device provisioning and privacy preserving middleware, including data storage and computation.

The architecture is based on FIWARE platform, which allows to evaluate and scale the demonstrator for the real world validation of Porto in the future and allows to study additional security and privacy concerns created by these ecosystems. The IoT device provisioning is usually an arduous task that encompasses device configuration, including identity and key provisioning. Given the potentially large number of devices in Smart-city contexts, this process must be scalable and semi-autonomous, at least.

In this evaluation, three of the assets identified in WP3 for the Smart City challenges will play a key role :

- **PTASC:** A privacy preserving tool for allow users to control the data to be shared for the marketplace;
- **ARGUS:** A cloud-of-clouds tool to store the information remotely in the cloud, that allow a classification and processing of the data

- **Briareos:** A distributed HIDS that allow to detect zero-days using ML

8.3.1 Actors

For the first phase, the only actors involved in the evaluation will be developers, which will carry out technical tests, and researchers/experts that will complete a questionnaire for feedback. Other actors (and stakeholders) that have been identified as potential participants of the use case, like citizens or service providers, will be included in subsequent evaluations.

8.3.2 Test Case SMC-UC04-TC01

This section describes a technical test case to validate some of functional and non-functional requirements related to security and privacy aspects covered by the use case.

8.3.2.1 Description

The test case is based on a marketplace that acts as a middleware based on the information provided by the city and the users that interact with sensors to generate data.

The city or users sensors can gather additional data that may be of interest to marketers to reinforce marketing strategies in a region, creating accurate and personalized ads contextualized to a person or region's interests. The information generated in a smart city allows to sell data allowing businesses and enterprises, that depend on city users, to acquire and process ML models to predict user behaviour. Our structure allows users to choose a set of data collected by the IoT sensors and stored in the Orion/ARGUS database to be shared with external entities (also selected by the data owner) in exchange for monetary compensation, offering users the possibility to monetize their data. For example, users can choose to sell data about temperature but not about lighting and air conditioning because they know that a machine learning algorithm can combine data to determine the presence in a given local. Note that this sell data option is valid for white-box devices or devices with data APIs.

As private information is involved, we must comply with the best practices to ensure the GDPR compliance. It needs to ensure that a user can control the information that we decide to upload to the cloud and we can test that they are correctly integrated, secure and privacy-preserving.

For the test case three services will be used:

- Porto Data Hub, a middleware that is based on FIWARE to store and monitor the data being exchanged.
- An IoT device that uploads information to the Porto Data Hub
- Android App that allows users to navigate on the web and control/share information being exchanged

Multiple components are involved in this test case. Figure 65 shows them, as well as a simplified flow of the test. In the following, we include a brief description of the components and their role:

- **PTASC:** A privacy preserving tool for data-sharing control mechanisms that allows users control their data's privacy and their respective Internet of Things (IoT) devices. The platform places the user as an active participant in the data market, behaving as its own data intermediary for potential consumers by monitoring, controlling, and negotiating the usage of their data;
- **ARGUS:** A cloud-of-clouds tool to store the information remotely in the cloud. The broker (ARGUS) acts as a proxy to the existing public cloud infrastructures by performing all the necessary authentication, cryptography and erasure coding. ARGUS uses erasure code as a way to provide

efficient redundancy (opposite to standard replication) while adding an extra layer to data protection in which data is broken into fragments, expanded and encoded with redundant data pieces that are stored across a set of different storage providers (public or private). The key characteristics of ARGUS are confidentiality, integrity and availability of data stored in public cloud systems.

- **Briareos:** A distributed HIDS that allows to detect zero-days using ML. Briareos is a module extensible framework. The Briareos Host Component is composed of pipelines for traffic processing, whose nodes contain modules. It supports multiple processing modes: inline, parallel and distributed. It is implemented as a distributed system capable of performing heavy tasks, which can be a plus for detecting unknown attack vectors.
- **Porto data hub:** Smart city platform that offers storage and marketplace for the Porto city users.
 - Orion fiware
 - Android App
 - KeyRock

In this use case, a user can control their data, in order to guarantee the privacy and security of them. The integration between the concepts pTASC and ARGUS allows to create a marketplace that has the control of the users' data on their side. This way, the data is always entitled on the decision of the user. For usability purposes, we use a smartphone with a webapp that gives to the user the way to control their data. Users can create the account and link their devices to them. Then, they can select different policies for their data. Also, they can access the marketplace to sell their data and select specific data to be sell.

Note that, pTASC concept focuses on the control of data sharing on the user side, not necessarily on the market itself. For this reason, and as users can use sensitive information, we need to integrate GDPR compliance methods to guarantee the pseudo-anonymity of the data. One way, will be the integration of Homomorphic Encryption (HE) concepts or Multiparty Computation, that allows the computation over the data without necessarily access them (raw).

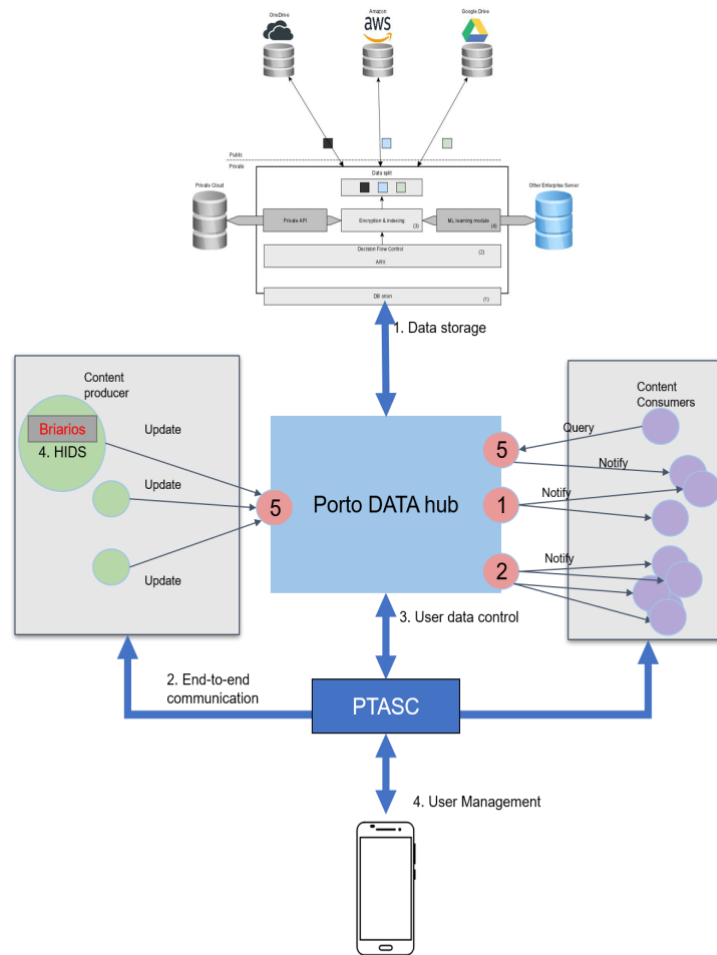


Figure 65 - Overview of the Porto Data Hub with integration and components

ARGUS is the component that includes the marketplace, which has the capability to store and share data among the users. Here, will be the component that implements the concepts of HE for the computation over the data.

Regarding the security component of devices, we have the Briareos that takes an active role on intrusion detection directly on the device, and focuses on the security issues of the devices itself. It allows the detection of abnormal behaviours of devices. This is an important component to guarantee the security of all the infrastructure.

The Figure 65 summarizes the components and communications among each asset expected to be deployed in the demonstrator. The current version is missing the communication component (PTASC).

8.3.2.2 Test Case Workflow

The test case workflow is depicted in the Figure 66:

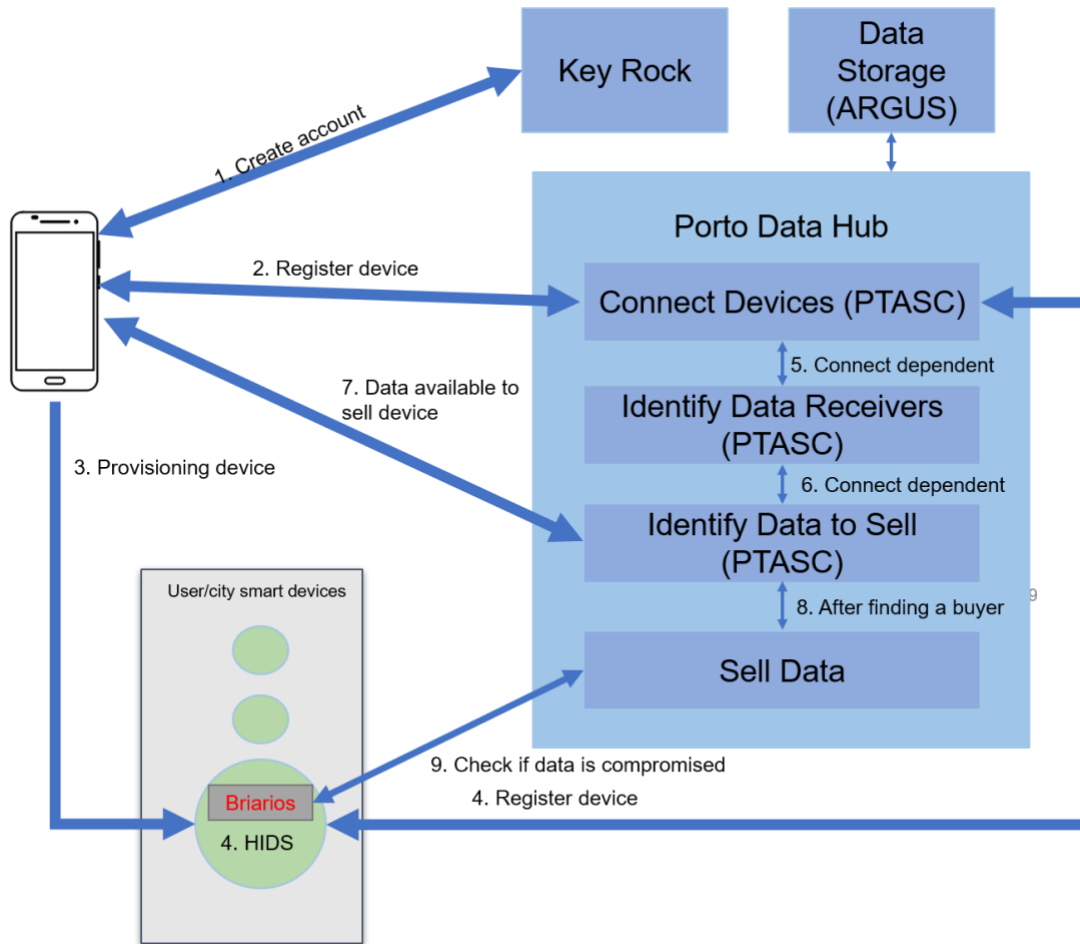


Figure 66 - Overview of the Porto Data Hub workflow

1. A citizen wants to access sensors and share information in the Porto Data Hub, which is one of the online services provided by the municipality. The entry point is the online service portal implemented using KeyRock;
2. In a smart city context, the user has a humidity sensor on his home. It desires to know the difference between the in-house temperature and the outside collected by the city, so it connects both sensors (from the city and home) using PTASC;
3. The citizen needs to perform the authentication from the client-side in the device;
4. After this request, the Porto Data Hub can add the sensor in the database (ARGUS);
5. Then, the user must specify the device that needs the information (the smartphone);
6. During this process, the user must choose if he want to sell the information available. This data can include other sources of information such as geolocations that may allow to re-identify the user.
7. The user can choose to share the temperature data without a specific location on the city or aggregated.

8.3.2.3 Test Results

The test case has successfully demonstrated the coverage of requirements related to the user's support and empowerment to control their data in the smart cities ecosystem and the possibility to extract and extend the mechanism for sharing sensor data from the platforms.

The solutions adopted have been integrated into a laboratory environment (this is mainly motivated by the assets low TRL).

8.3.3 Technology Based Analysis

This section provides a description of how each requirement has been validated by the intrinsic features of the components of our demonstrator case, namely pTASC, ARGUS and BRIAREOS.

8.3.3.1 SMC-SP01- Solution ensures that authentication is implemented

The Porto Data Hub platform is only accessed after the user or device authenticates through keyrock or PTASC.

8.3.3.2 SMC-SP02- Keep sensitive information secured and accessible only to authorized users

Persistent data is stored on ARGUS and it is protected by specific access policies, and users must ensure that are the owners of the information. Credentials and public keys are stored in an encrypted SGX to ensure an extra layer of security.

8.3.3.3 SMC-SP04- 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

All API for the communication uses SSL, and they are implemented using accepted standards protocols, e.g., TLS 1.3.

8.3.3.4 SMC-SP06 - Solution provides data provenance, so that it allows for auditing of data access and update on secured data

All the information uploaded to the Porto Data Hub is recording with a timestamp and a specific owner to ensure that the information can be audited. Also the marketplace will allow and store any query computations performed over the data.

8.3.3.5 SMC-SP7 - Solution is easy to protect and isolate parts from vulnerabilities;

Briareos allows to detect vulnerabilities in an early stage, allowing for understanding the system's vulnerabilities and reducing and isolating the environment.

8.3.3.6 SMC-SP10- 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

Communications using SSL allow us to integrate any end-to-end solutions available. PTASC implements a end-to-end solutions using Yubikeys.

8.3.3.7 SMC-SP11- Solution should have a secure store for keys and be able to integrate with key stores.

Private keys in the Porto Data Hub are protected using intel SGX.

8.3.3.8 SMC-SP16- Personal data has to be stored in a protected way (e.g. encryption, hashing);

It is encrypted, Porto Data Hub only maintains a local copy (in clear text) of information that do not contain personal information.

8.3.3.9 SMC-SP22- Demonstration case solutions should prevent the possibility of creating central surveillance on users or groups of users.

The marketplace will allow users to sell the information but it collects and allows them to explicitly decide whether to sell or not a specific type of information.

8.3.3.10 SMC-SP23- The establishment of technological practices for security and privacy should be based on open architectures and standards

All architectural and cryptographic tools used are public standards.

8.3.4 Quality Indicators

8.3.4.1 Effectiveness and efficiency of the solution

This category comprises the following subcategories:

- integration and interoperability (KPI_QAI)
- documentation (KPI_QAD)
- usability (KPI_QAU)
- source code management (KPI_QASCM)
- testing (KPI_QAT)
- deployment (KPI_QADPY)

Below the indicators we plan to consider according the above-mentioned multi stage test and validation

KPI_QAI_01: Integration and interoperability. The functionality of the components is exposed for example via JSON REST/RPC APIs for the integration with other systems. The functionality in this way is made available for the server-side components and for the UI components.

Indicator	Description	Evaluation
API exposure	Solution client and server exposure both as code library and REST interface. Authorization API exposed as REST	Yes, internal and external API exposed as REST.
Level of simplicity, adaptability and functionality of the API perceived by developers.	Service is readily adoptable and applicable in at least 50% of cases	The API provided by the solution is adapted and extended to the specific use case. It also have API's to extend and produce dashboards.
Support Single Sign-On to allow for using single credentials across different	Solution should support ≥ 1 SSO systems	Not enabled, but it is possible to include.

applications.		
---------------	--	--

KPI_QAD_01: Installation, configuration, and integration documentation. For each component README file providing i) the component installation instructions; ii) the component configuration instructions; and iii) component integration instructions defining the necessary steps to set up the integration with other components.

We provided a README with installation/configuration instructions for deploy in a docker environment, and documentation to integration of assets with PTASC.

KPI_QAD_02: Specification and documentation for the APIs.

Indicator	Description	Evaluation
Level of completeness on the API documentation perceived by developers.	Surveys should reveal that the service has adequate documentation in at least 50% of cases	All APIs are built and documented using FastAPI.
Level of understandability on the API documentation perceived by developers.	Surveys should reveal that the service has clear documentation in at least 50% of cases	>60% of FastAPI produce clear documentation.

- **KPI_QAD_03: Additional documentation (examples, tutorials, etc).** the documentation should provide the description of the usage scenarios of the component, examples (e.g., API call inputs and outputs, testing instructions, tutorials, howto, etc).

An additional document can be provided about the usage of the solution. Some demos are provided to integrate the Manager Yubikey in the system with a tutorial (step-by-step) available.

- **KPI_QAU_01: Usability and UX.** Usability and User experience.

Indicator	Description	Evaluation
Minimal browser support. The component user interface (where available e.g. dashboards, forms, ect..) should provide support for the wide range of widely used browsers.	>1	Mobile Phone support, Android APP.
User perceived level of trust in the solution	>75% of user high or very high trust in surveys	The manual enrolment provided by PTASC ensures

		that users understand the behavior, accordingly with previous test.
App user friendliness, look and feel perceived by the user (simple to install, easy to navigate, provides use guidelines and information about problems, easy to remove)	Surveys should reveal that the service is perceived as reliable in at least 50% of cases	To be evaluated in Phase 2.
User consent is prompted to the user for user data sharing	>75% of users think that consent is clearly accomplished	To be evaluated in a real environment.
Consent Form is usable and user friendly	>75% users satisfied with the solution	To be evaluated in a real environment.
General level of satisfaction with the solution (enrolment, authentication, authorization and usage processes, consent lifecycle management)	>75% users satisfied with the solution	Previous test with PTASC demonstrate satisfaction with the mechanism implemented.

- **KPI_QASCM_01: Use of SCM and issue tracking.** Any use of source code management repository and related issue tracking (**target:1**)

Github is used for all components adopted in the use case.

- **KPI_QAD_01: Docker containers provided.** To further improve the deployment procedure allowing for targeting different Cloud environments.

The integration with docker allows to adapt to any new cloud environments.

- **KPI_QAT_01: Percentage of issues resolved.** The issues reported during the process of the component development, integration, evaluation should be appropriately managed and resolved by the component owners. (**target: >50%** for the first stage)

>50% issued solved for the adaptation and adoption of the solutions in the use case.

8.3.4.2 User and stakeholder engagement and impact evaluation

Indicator	Description	Target	Evaluation
Internal efficiency	Time to perform enrolment in the Porto Data Hub	<3 seconds	Less than 1.34 seconds.
	Detecting an intrusion in the system	<5 minutes (subject to Briareos)	Not measured in a real environment, but with the lab test in less than a minute.

	Throughput of upload to the Porto Data Hub	> 2 MB/S	Throughput in the ARGUS is higher than 2MB/S evaluated using previous test of ARGUS.
	Time to send request to buy request (excluding time for users to agree)	<1 minute	2 seconds.
Internal effectiveness	Percentage of enrolment requests successfully completed	>95%	10 out of 10 tests completed.
	Percentage of authentication requests successfully completed	>95%	10 out of 10 tests completed.
	Percentage of authorization requests successfully completed	>95%	10 out of 10 tests completed.

8.3.5 Requirements Coverage

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP01	Partially	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	The Porto Data Hub platform is only accessed after the user or device authenticates through keyrock or PTASC.
SMC-SP02	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	Persistent data is stored on ARGUS and it is protected by specific access policies, and users must ensure that are the owners of the information. Credentials and public keys are stored in an encrypted SGX to ensure an extra layer of security.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP03	NO	SMC-UC04-TC01 <i>Technology based</i>		Yes	
SMC-SP04	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	All API for the communication uses SSL, and they are implemented using accepted standards protocols.
SMC-SP05		SMC-UC04-TC01 <i>Technology based</i>		NO	
SMC-SP06	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	All the information uploaded to the Porto Data Hub is recording with a timestamp and a specific owner to ensure that the information can be audited. Also the marketplace will allow and store any query computations performed over the data.
SMC-SP07	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	Briareos allows to detect vulnerabilities in an early stage, allowing for understanding the system's vulnerabilities and reducing and isolating the environment.
SMC-SP10	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	Communications using SSL allow us to integrate any end-to-end solutions available. PTASC implements a end-to-end solutions using Yubikeys.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP11	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	Private keys in the Porto Data Hub are protected using intel SGX.
SMC-SP16	Partially	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	It is encrypted, Porto Data Hub only maintains a local copy (in clear text) of information that do not contain personal information.
SMC-SP22	Partially	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	The marketplace will allow users to sell the information but it collects and allows them to explicitly decide to sell identifying information.
SMC-SP23	Yes	SMC-UC04-TC01 <i>Technology based</i>	Success	Yes	All architectural and cryptographic tools used are public.

Table 36: Smart Cities - SMC-UC04 Validation requirements' coverage plan.

8.4 Use Case SMC-UC5

As reported in the last Threat Landscape by ENISA²⁴, the phishing attack is one of the top15 cyber threats nowadays, and the simulated phishing campaigns for testing is one of the best mitigation actions they suggest, therefore we are on the right way.

The UC5 *Assess Social Engineering exposure by simulating phishing attacks on Service Provider's target-groups* has been fully validated within the Genoa demonstrator environment. A combination of the validation methods has been used to validate this UC. The requirements that allow to be validated by test cases, have followed this way. The non-functional requirements have been validated through questionnaire or technology based analysis.

²⁴ ENISA Threat Landscape – 2020: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

The criteria to establish test successful was the passing of test case, a positive answer to the question or a good result of the technology based analysis.

8.4.1 Actors

The test cases were executed by the penetration tester, who acts as user of the platform: in this case, ENG was the user to validate the demonstrator on phishing attack simulation.

Questionnaire and technology based analysis were used by the technology owner: in this case, ENG is the owner of the tool used to perform the attack simulation.

8.4.2 Test Case SMC-UC5-TC01

This section describes a technical test case to validate some of functional and non-functional requirements related to security and privacy aspects covered by the use case.

8.4.2.1 Description

This test case aims to validate the features of the tool for social driven vulnerability assessments (SDVA), in order to check the achievement of requirements addressed by UC5. In this Test Case the CISO (or managers) of Genoa municipality orders a penetration tester to perform a social driven vulnerability assessment (e.g. phishing simulation) within pseudo-anonymized target groups (employees, department, specific team, etc...). All the Genoa civil servants have been grouped and hitted as targets. The test expects that the CISO has previously defined the assessment plan (white box vs black box approach) and shared characteristics of the plan with the pen tester, that is in charge to define, execute and monitor the phishing attack, as well as to create the final reporting.

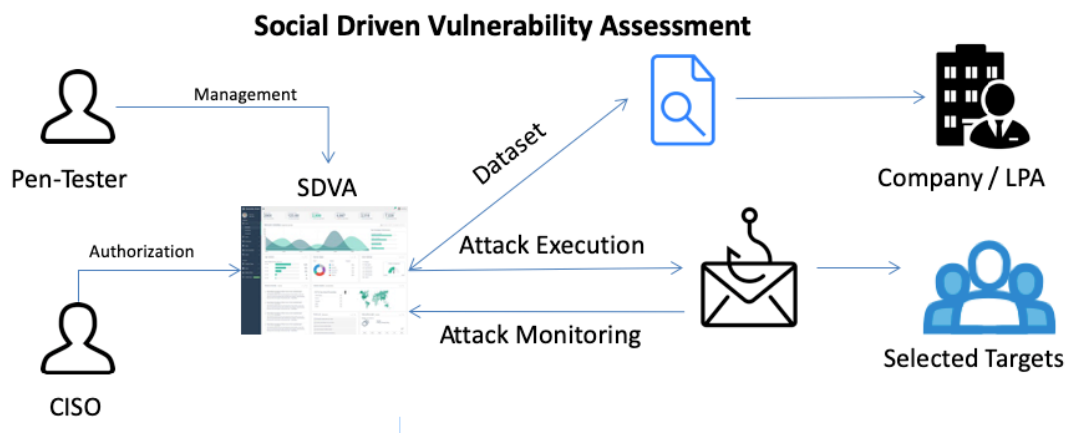


Figure 67 - Test case SMC-UC05-TC01 summary

8.4.2.2 Test Case Workflow

1. System Administrator deploys the solution and creates the CISO account, passing credentials to the CISO of the organization;
2. CISO accesses to the web application home page;
3. The system asks for credential;
4. CISO inserts the username and password;

5. The system grants access to the user;
6. CISO accesses to the SDVA Management GUI, initializes the assessment
7. CISO set pen-tester (PT) account, filling the “Create user” form with fullname, company, email address, username and password;
8. The system notifies the user about the successful creation of new user;
9. CISO logs out;
10. PT accesses to the web application home page and inserts the username and password;
11. The system grants access to the user;
12. PT accesses to the SDVA Management GUI and performs the “hook preparation”:
 - a. Create the hook of the attack;
 - b. Web Site Configuration - PT creates the landing page of the fake web site;
 - c. Email Configuration - PT creates the email content of the hook.
13. PT accesses to the “execution of the attack” stage:
 - a. Set up of the attack: attack schedule and parameters (blocks of emails and delay among them,...)
 - b. Launches the attack;
 - c. Monitors the attack;
 - d. Closes the Attack.
14. PT accesses to the “Information Aggregation and Reporting” stage:
 - a. Accesses to the Aggregation and Reporting Module;
 - b. Performs by-default aggregation rules;
 - c. Defines new aggregation rules and have custom reports;
 - d. Accesses to the statistical representation of the outcomes (percentage of people that have fall into the attack,...);
 - e. Discovers technological vulnerabilities;
 - f. PT collect the report for C-Level.
15. CISO reviews the report;
16. The CISO asks for deleting the targets database;
17. The system performs the deleting action and notifies the user.

8.4.2.3 Test Results

The test was successfully passed: all the activities described above were performed as planned. Genova was the Smart City who tested the solution and the CISO found the final report very interesting to identify and address effectively the lack of knowledge within his organization.

8.4.3 Technology Based Analysis

Some requirements have been demonstrated and validated by the intrinsic features of the component of the system integrated in the use case and not explicitly described in the above test case.

8.4.3.1 SMC-SP02 Keep sensitive information secured and accessible only to authorized users;

The authentication mechanism of the solution allows keeping all the targets’ sensitive information secured and accessible only to CISO and PTs listed in the users to the platform.

- 8.4.3.2 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;

All internal communications among modules are protected using HTTPS and JWT authentication.

- 8.4.3.3 SMC-SP05 Solution can be integrated with existing authentication mechanisms;

This requirement cannot be addressed by SDVA solution, because the authentication is embedded in this prototype and does not allow to integrate with other systems.

- 8.4.3.4 SMC-SP07 Solution is easy to protect and isolate parts from vulnerabilities;

The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator. This assures an adequate level of protection and isolation.

- 8.4.3.5 SMC-SP08 Solution allows for monitoring access and changes;

Monitoring feature is provided by Json Web Token (JWT) technology. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token.

- 8.4.3.6 SMC-SP09 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;

Despite the fact that the component is not able to prevent any breaches, logs are stored for each module of the solution to track actions and requests.

- 8.4.3.7 SMC-SP12 Solution must implement privacy rules as stated by the European Union, in particular the new GDPR, national law, ECHR[19] (Article 8), EU Charter[21] (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;

The solution respects all the rules requested by regulations at European and National level.

- 8.4.3.8 SMC-SP17 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.

Storage is anonymized and data is aggregated to ensure high security readiness.

- 8.4.3.9 SMC-SP19 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;

The SDVA solution hides personal data to the user by aggregation before he/she can access it through the attack report.

- 8.4.3.10 SMC-SP20 Whenever personal information is visible to others, this should clearly be indicated to users;

No personal data is accessible outside the platform users

- 8.4.3.11 SMC-SP21 No automated decision should be done when processing personal data.

There is no automated decision into this solution

8.4.3.12 SMC-SP22 Demonstration case solutions should prevent the possibility of creating central surveillance on users or groups of users.

The collected personal data set is designed with specific rules in order to avoid central surveillance mechanism.

8.4.3.13 SMC-SP23 SDLC The establishment of technological practices for security and privacy should be based on open architectures and standards

The solution adopts an open architecture allowing to add/remove modules as needed.

8.4.4 Quality Indicators

8.4.4.1 Effectiveness and efficiency of the solution

This category comprises the following subcategories:

- integration and interoperability (KPI_QAI)
- documentation (KPI_QAD)
- usability (KPI_QAU)
- source code management (KPI_QASCM)
- testing (KPI_QAT)
- deployment (KPI_QADPY)

KPI_QAI_01: Integration and interoperability. The functionality of the components is exposed for example via JSON REST/RPC APIs for the integration with other systems. The functionality in this way is made available for the server-side components and for the UI components.

Indicator	Description	Evaluation
API exposure	Solution client and server exposure both as code library and REST interface. Authorization API exposed as REST	Yes
Level of simplicity, adaptability and functionality of the API perceived by developers.	Service is readily adoptable and applicable in at least 50% of cases	Yes. Ready at 100%

KPI_QAD_01: Installation, configuration, and integration documentation in README. Component README file providing i) the component installation instructions; ii) the component configuration instructions; and iii) component integration instructions defining the necessary steps to set up the integration with other components.

The solution provides users and sysadmins with a set of README files to help the installation, configuration and integration.

KPI_QAD_03: Additional documentation (examples, tutorials, etc). the documentation should provide the description of the usage scenarios of the component, examples (e.g., API call inputs and outputs, testing instructions, tutorials, howto, etc).

Additional documentation is provided in each section and steps of the solution. In particular it provides help feature through a tooltip advice about the usage of the tool.

KPI_QAU_01: Usability and UX. Usability and User experience.

Indicator	Description/Target	Evaluation
Minimal browser support. The component user interface (where available e.g. dashboards, forms, ect..) should provide support for the wide range of widely used browsers.	>1	2 (Chrome, Firefox)
General level of satisfaction with the solution (enrolment, authentication, authorization and usage processes, consent lifecycle management)	>75% users satisfied with the solution	100% users satisfied

KPI_QASCM_01: Use of SCM and issue tracking. Any use of source code management repository and related issue tracking (**target:1**)

The solution uses GitLab as source repository

KPI_QAD_01: Docker containers provided. To further improve the deployment procedure allowing for targeting different Cloud environments.

Yes

KPI_QAT_01: Percentage of issues resolved. The issues reported during the process of the component development, integration, evaluation should be appropriately managed and resolved by the component owners. (**target: >50%** for the first stage)

80%

8.4.4.2 User and stakeholder engagement and impact evaluation

Indicator	Description	Target	Evaluation
Number of engaged	Business (SME, Corporate, etc)	1 (ENG)	1

Indicator	Description	Target	Evaluation
stakeholders for each type (target groups identified in D5.2)	Organizations (public organizations, non-profit organizations)	1 (Genova)	1
	Individuals (Consumers, Citizen, other)	100+ (SDVA Targets)	4125
Internal efficiency	Percentage of time saved in the specific process/activity supported in the demonstrator	>70% of time saved x Target User	80% of time saved for sending emails and analysing the result of the attack
	Time to perform the specific process/activity supported in the demonstrator	3 seconds for report generation	3
Tools adoptions	Number of procedures supported by the adopted tools	4	4
	Number of demonstrator/tools users	1 (Pen tester)	1
Changing behaviours	Number of activities developed with the aim of changing behaviours of the involved actors	1 live lesson	1
	Success rate of the activities developed to improve behavioural change processes	>10-20% Phishing URL click rate reduction (with & without training)	Not available after this first round of trial
Impact on human capital	Number of activities supporting the acquisition of digital competences, eSkills and the reduction of digital divide	1 course about phishing awareness	0
Process/service and organisational innovation	Number of new organisational methods implemented	2 (Victim communication stack, Attack Simulation)	2

8.4.4.2.1 Questions

Following, a list of the questions asked in the internal questionnaire for feedback.

1. User profile:

- ☐ Chief Executive Officer (CEO)
- ☒ Chief Information Security Officer (CISO)
- ☐ Chief Financial Officer (CFO)
- ☐ Other, specify _____

2. General Feedback about the adopted tool:

#	ITEM	Strongly disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly agree (5)	Add a comment
1	Please rank the following statement: "the Social Engineering cyber-risk reduction achieved in the TO4SEE trials justify the costs sustained for implementing it on the basis of the results"					X	
2	Is the achieved Social Engineering cyber-risk reduction high compared with your expectations					X	
3	The achieved results can lead to long-lasting Social Engineering cyber-risk reduction					X	

3. SWOT Analysis

a. Strengths - please identify the strengths of the tool in reducing cyber-risk.

The tool allows us to better focus the economic resources to be used in infrastructure and training within the LPA

b. Weaknesses - please identify the factors that detract from the tool's ability to reduce cyber-risk

Data anonymization

c. Opportunities - please consider the opportunities generated by the application of the framework in your organisation (e.g. new business opportunity thanks to an increased cyber-maturity, etc.)

Greater cyber-maturity leads to greater efficiency of office operations

- d. *Threats - please describe the external factors which negatively affect the tool in reducing cyber-risk (e.g. entry into force of GDPR, insufficient background cyber-maturity of your employees, EU legal framework, ineffectiveness of training programs, etc.)*

The anonymization system prevents you from being able to focus training on specific users. This leads to generalized training with a potential increase in training costs (both economic and time)

4. *Do you recommend to use SDVA at your workplace permanently?*

Yes, for the following reason: It is a good tool to use periodically

No, for the following reason: _____

8.4.5 Requirements Coverage

This section summarize the security and privacy coverage and results of the performed validation.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP01	Yes	SMC-UC5-TC1	Success	Yes	
SMC-SP02	Yes	Technology based	Success	Yes	The authentication mechanism of the solution allows keeping all the targets' sensitive information secured and accessible only to CISO and PTs listed in the users to the platform.
SMC-SP03	Yes	SMC-UC5-TC1	Success	Yes	
SMC-SP04	Yes	Technology based	Success	Yes	All internal communications among modules are protected using HTTPS and JWT authentication.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP05	No	Technology based	Success	NO	The authentication is embedded in this prototype and does not allow to integrate with other systems
SMC-SP06	N.A.				
SMC-SP07	Yes	Technology based	Success	Yes	The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator.
SMC-SP08	Yes	Technology based	Success	Yes	Monitoring feature is provided by Jason Web Token (JWT) technology
SMC-SP09	Yes	Technology based	Success	Yes	Logs are recorder in order to track requests and actions of the component.
SMC-SP10	N.A.				
SMC-SP11	N.A.				
SMC-SP12	Yes	Technology based	Success	Yes	The solution respects all the rules requested by regulations at European and National level.
SMC-SP13	N.A.				
SMC-SP14	N.A.				
SMC-SP15	N.A.				
SMC-SP16	N.A.				

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP17	Yes	Technology based	Success	Yes	Storage is anonymized and data is aggregated to ensure high security readiness.
SMC-SP18	Yes	SMC-UC5-TC1	Success	Yes	
SMC-SP19	Yes	Technology based	Success	Yes	The SDVA solution hides personal data to the user by aggregation before he/she can access it through the attack report
SMC-SP20	Yes	Technology based	Success	Yes	No personal data is accessible outside the platform users
SMC-SP21	Yes	Technology based	Success	Yes	There is no automated decision into this solution
SMC-SP22	Yes	Technology based	Success	Yes	The collected personal data set is designed with specific rules in order to avoid central surveillance mechanism.
SMC-SP23	Yes	Technology based	Success	Yes	The solution adopts an open architecture allowing to add/remove modules as needed.
SMC-SP24	N.A.				

Table 37: Smart Cities - SMC-UC05 Validation requirements' coverage.

8.5 Use Case SMC-UC6

The UC06 *Cyber Risk Assessment, evaluate the Service Provider's cyber maturity level and estimate probability and impacts of cyber attacks* has been fully validated by the usage of the RATING tool. A combination of the validation methods has been used to validate this UC. The requirements that allow to be validated by test cases, have followed this way. The non-functional requirements have been validated through questionnaire or technology based analysis.

The criteria to establish test successful was the passing of test case, a positive answer to the question or a good result of the technology based analysis.

8.5.1 Actors

The test cases were executed by the CISO (acting also as CRO) and CFO, who act as users of the platform: in this case, Genova was the user to validate the demonstrator on cyber risk assessment.

Questionnaire and technology based analysis were used by the technology owner: in this case, ENG is the owner of the tool used to assess the cyber-posture of the Genova organisation.

8.5.2 Test Case SMC-UC6-TC01

This section describes a technical test case to validate some of functional and non-functional requirements related to security and privacy aspects covered by the use case.

8.5.2.1 Description

This test case aims to validate the features of the tool RATING, in order to check the achievement of requirements addressed by UC6. This test allows C-Levels (managers as well) to profile cyber risks scenarios based on (both tangible and intangible) asset's cyber vulnerabilities exposure and relationships between direct and indirect losses. The process steps are (i) a Company Profiling, focused on the identification of the main assets of the service provider, (ii) a Cyber Vulnerability Assessment, to evaluate the cyber maturity model of the service-provider, (iii) a Qualitative Impact Analysis, to identify cascading effects scenarios on assets, evaluate the capital at risk, simulate the losses and prioritize main key assets, (iv) a Risk Modelling through the aggregation of the likelihood, vulnerability and impact scores produced by previous analysis.

8.5.2.2 Test Case Workflow

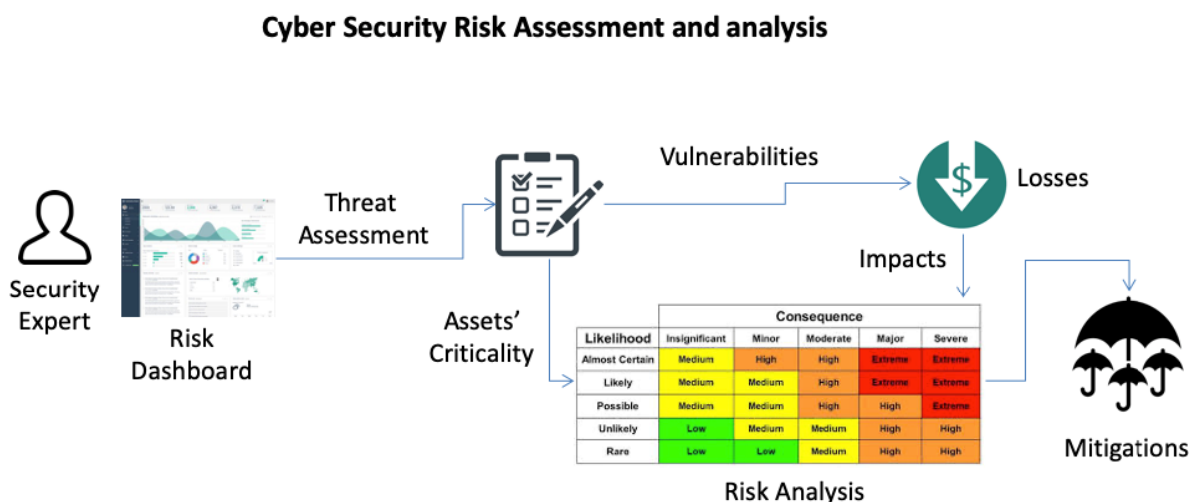


Figure 68 - Test case SMC-UC06-TC01 summary

1. The CISO initializes the risk assessment, providing information about the title of the assessment;
2. CISO (in create-mode), identifies the assets involved in the assessment (Asset Clustering). They can be tangible and intangible;
3. CISO start the vulnerability assessment. It concerns in the identification and measurement of the current countermeasures implemented by the organization. In order to evaluate the likelihood of the attacks and company's cyber posture, measurement process is grouped by human, IT and physical characteristics, which can be calculated using holistic procedures;
4. Based on vulnerability scores, the CFO can make the impact analysis. CFO basically identify the cascading effects of a probable attack, defining direct and indirect consequences and identifying the costs related to the cyber-attacks;
5. Based on estimated cascading effects and vulnerability exposures, the CFO can perform qualitative analysis to prioritize the assets at risk;
6. Once estimated, the CFO performs a simulation of losses taking in consideration cascading effects identified previously. Finally, the system returns the impact reports on the critical assets;
7. The CRO, performs the risk analysis. based on discovered impacts and vulnerabilities, the user get evidence of the asset at risk and starts to think how to protect the business;
8. The CRO, defines the risk priority and its tolerance in order to let the system to aggregate data and make the risk matrix. Finally, CRO can exports results as human readable formats, in order to share such information as internal audits;

8.5.2.3 Test Results

The test was successfully passed: all the activities described above were performed as planned. GEN was the Smart City who tested the solution and the CISO found the final report very interesting to identify the risks and address effectively the cyber threats within his organization.

8.5.3 Technology Based Analysis

Some requirements have been demonstrated and validated by the intrinsic features of the component of the system integrated in the use case and not explicitly described in the above test case.

8.5.3.1 SMC-SP02 Keep sensitive information secured and accessible only to authorized users;

The authentication mechanism of the solution allows keeping all the organization's sensitive information secured and accessible only to CISO.

8.5.3.2 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;

All internal communications among modules, are protected using HTTPS and JWT authentication.

8.5.3.3 SMC-SP05 Solution can be integrated with existing authentication mechanisms;

The SingleSign-on (SSO) feature allows to integrate the authentication mechanism with other compliant solutions.

8.5.3.4 SMC-SP07 Solution is easy to protect and isolate parts from vulnerabilities;

The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator. This assures an adequate level of protection and isolation.

8.5.3.5 SMC-SP08 Solution allows for monitoring access and changes;

Monitoring feature is provided by Jason Web Token (JWT) technology. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token.

8.5.3.6 SMC-SP09 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;

Despite the fact that the component is not able to prevent any data breach, logs are recorder in order to track requests and actions of the component.

8.5.3.7 SMC-SP12 Solution must implement privacy rules as stated by the European Union, in particular the new GDPR, national law, ECHR[19] (Article 8), EU Charter[21] (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;

The solution respects all the rules requested by regulations at European and National level.

8.5.3.8 SMC-SP17 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.

No personal data is handled. Evaluated assets are categorized following ISO27001 security measures.

8.5.3.9 SMC-SP19 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;

The solution does not use any personal data.

8.5.3.10 SMC-SP20 Whenever personal information is visible to others, this should clearly be indicated to users;

The solution does not use any personal data.

8.5.3.11 SMC-SP21 No automated decision should be done when processing personal data.

There is no automated decision into this solution

8.5.3.12 SMC-SP22 Demonstration case solutions should prevent the possibility of creating central surveillance on users or groups of users.

The solution does not use any personal data.

8.5.3.13 SMC-SP23 SDLC The establishment of technological practices for security and privacy should based on open architectures and standards

The solution adopts an open architecture allowing to add/remove modules as needed.

8.5.4 Quality Indicators

8.5.4.1 Effectiveness and efficiency of the solution

This category comprises the following subcategories:

- integration and interoperability (KPI_QAI)
- documentation (KPI_QAD)
- usability (KPI_QAU)
- source code management (KPI_QASCM)
- testing (KPI_QAT)
- deployment (KPI_QADPY)

KPI_QAI_01: Integration and interoperability. The functionality of the components is exposed for example via JSON REST/RPC APIs for the integration with other systems. The functionality in this way is made available for the server-side components and for the UI components.

Indicator	Description	Evaluation
API exposure	Solution client and server exposure both as code library and REST interface. Authorization API exposed as REST	Yes
Level of simplicity, adaptability and functionality of the API perceived by developers.	Service is readily adoptable and applicable in at least 50% of cases	Yes. Ready at 100%
Support Single Sign-On to allow for using single credentials across different applications.	Solution should support ≥ 1 SSO systems	Yes. SSO is available with JWT technology

KPI_QAD_01: Installation, configuration, and integration documentation in README. Component README file providing i) the component installation instructions; ii) the component configuration instructions; and iii) component integration instructions defining the necessary steps to set up the integration with other components.

YEs. The solution provides users and sysadmins with a set of README files to help the installation, configuration and integration.

KPI_QAD_03: Additional documentation (examples, tutorials, etc). the documentation should provide the description of the usage scenarios of the component, examples (e.g., API call inputs and outputs, testing instructions, tutorials, howto, etc).

Yes. additional document is provided describing risk assessment steps

KPI_QAU_01: Usability and UX. Usability and User experience.

Indicator	Description	Evaluation
Minimal browser support. The component user interface (where available e.g. dashboards, forms, ect..) should provide support for the wide range of widely used browsers.	>1	2 (Chrome, Firefox)
General level of satisfaction with the solution (enrolment, authentication, authorization and usage processes, consent lifecycle management)	>75% users satisfied with the solution	100% users satisfied

KPI_QASCM_01: Use of SCM and issue tracking. Any use of source code management repository and related issue tracking (**target:1**)

The solution uses GitLab as source repository

KPI_QAD_01: Docker containers provided. To further improve the deployment procedure allowing for targeting different Cloud environments.

Yes

KPI_QAT_01: Percentage of issues resolved. The issues reported during the process of the component development, integration, evaluation should be appropriately managed and resolved by the component owners. (**target: >50%** for the first stage)

100%

8.5.4.2 User and stakeholder engagement and impact evaluation

Indicator	Description	Target	Evaluation
Number of engaged stakeholders for each type (target groups identified in D5.2)	Business (SME, Corporate, etc)	1 (ENG)	Yes
	Organizations (public organizations, non-profit organizations)	1 (Genova Municipality)	Yes
	Individuals (Consumers, Citizen, other)	Genova's CISO	Yes

Indicator	Description	Target	Evaluation
Internal efficiency	Percentage of time saved in the specific process/activity supported in the demonstrator	>50% (avoiding manual analysis)	80%
	Time to perform the specific process/activity supported in the demonstrator	<3 seconds	2,5s
Tools adoptions	Number of procedures supported by the adopted tools	>=4	4
	Number of demonstrator/tools users	1-4 (CISO Finacial Risk Expert)	1
Changing behaviours	Number of activities developed with the aim of changing behaviours of the involved actors	>=1 live lesson	Yes
Impact on human capital	Percentage of improvement of skills of actors employed	10-50% of CISO's awareness about Organization Cyber Posture	50%
Process/service and organisational innovation	Number of new organisational methods implemented	>=2	4

8.5.4.2.1 Questions

Following, a list of the questions asked in the internal questionnaire for feedback.

1. User profile

☐ Chief Executive Officer (CEO)

☒ Chief Information Security Officer (CISO)

☐ Chief Financial Officer (CFO)

☐ Other, specify _____

2. Do you think that a self-assessment is a relevant instrument to map cybersecurity status in your LPA?

Yes

in particular

#	ITEM	Strongly disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly agree (5)	Add a comment
2.1	RATING helps LPAs to implement business continuity and risk assessment (according to ISO 27001:2005:A.14.1.2)					X	
2.2	RATING supports security LPA staff to understand if a risk related to a specific threat exceeds a set threshold					X	
2.3	If a new asset will be introduced in LPA infrastructure, RATING will easily identify it to perform the risk assessment					X	
2.4	RATING easily identifies residual risks					X	
2.5	RATING supports to monitor the risk profile evolution of LPAs over time					X	
2.6	It is easy to edit part of existing self-assessment					X	
2.7	RATING allow security LPA staff to see the results of the self-assessment in relation to the values obtained from the monitoring tools and the results of the individual assessments of employees					X	
2.8	The most suitable mitigation actions are displayed in RATING for the risky attack strategies					X	
2.9	RATING help completing a self-assessment for a single LPA's				X		Only qualitative because quantitative

#	ITEM	Strongly disagree (1)	Disagree (2)	Neither agree nor disagree (3)	Agree (4)	Strongly agree (5)	Add a comment
	service, using a quantitative or a qualitative approach						approach isn't tailored for LPA
2.10	RATING's user guide helps to complete a self-assessment					X	
2.11	How much clear and easy is to access RATING functionalities?					X	
2.12	Do you think that RATING returns an attack strategies' matrix that is easy to read and useful?					X	
2.13	Do you think that RATING is easy to be adopted?				X		Some questions must be filled in based on the perception of the manager of the area as it can be difficult to have precise data.
2.14	Do you think that RATING allows you to identify any errors of assessment?				X		The value is perceived as good or not based on the evaluator's experience.

3. Did you miss certain functionalities when using RATING?

Yes, namely the quantitative impact analysis

4. Using RATING, why do you think that your LPA can save a lot of money?

The resulting assessment allows the leadership to better evaluate the economic and strategic plan to ensure cyber security.

5. Using *RATING*, do you think that you will better manage cyber security attacks?

With *RATING* it is possible to have a greater perception of the prevailing risk and act accordingly to mitigate it.

6. What is, in your opinion, the greatest advantage of using *RATING* and what is the functionality you think could be the most useful for an LPA?

RATING provides well-detailed reporting and adopts, for the assessment, safety standards that make it certifying. Reporting should refer to the security standards used in cybersecurity.

7. What are, in your opinion, the greatest disadvantages or problems with using *RATING*?

It adopt only EBITDA in quantitative impact analysis approach. This isn't used in LPA. It is very difficult to enter economic information in order to assess its impact in the event of a cyber-attack.

8. Do you recommend to use *RATING* at your workplace permanently?

- a) Yes, for the following reason: but the adoption of the tool depends on the acceptance of the reports at manager level
- b) No, for the following reason: _____

8.5.5 Requirements Coverage

This section summarize the security and privacy coverage and results of the performed validation.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP01	Yes	SMC-UC6-TC1	Success	Yes	
SMC-SP02	Yes	Technology based	Success	Yes	The authentication mechanism of the solution allows keeping all the organization's sensitive information

ID	Validated	Strategy	Result	Mandatory	Comments
					secured and accessible only to CISO.
SMC-SP03	Yes	SMC-UC6-TC1	Success	Yes	
SMC-SP04	Yes	Technology based	Success	Yes	All internal communications among modules, are protected using HTTPS and JWT authentication.
SMC-SP05	Yes	Technology based	Success	NO	The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator. This assures an adequate level of protection and isolation.
SMC-SP06	Yes	SMC-UC6-TC1	Success	Yes	
SMC-SP07	Yes	Technology based	Success	Yes	The deployment configuration uses a docker isolation of the modules of the solution adopted in the demonstrator. This assures an adequate level of protection and isolation.
SMC-SP08	Yes	Technology based	Success	Yes	Monitoring feature is provided by Jason Web Token (JWT) technology
SMC-SP09	Yes	Technology based	Success	Yes	Logs are recorder in order to track requests and actions of the component.
SMC-SP10	N.A.				

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP11	N.A.				
SMC-SP12	Yes	Technology based	Success	Yes	The solution respects all the rules requested by regulations at European and National level.
SMC-SP13	N.A.				
SMC-SP14	N.A.				
SMC-SP15	N.A.				
SMC-SP16	N.A.				
SMC-SP17	Yes	Technology based	Success	Yes	No personal data is handled. Evaluated assets are categorized following ISO27001 security measures.
SMC-SP18	Yes	SMC-UC6-TC1	Success	Yes	
SMC-SP19	Yes	Technology based	Success	Yes	The solution does not use any personal data.
SMC-SP20	Yes	Technology based	Success	Yes	The solution does not use any personal data.
SMC-SP21	Yes	Technology based	Success	Yes	There is no automated decision into this solution
SMC-SP22	Yes	Technology based	Success	Yes	The solution does not use any personal data.
SMC-SP23	Yes	Technology based	Success	Yes	The solution adopts an open architecture allowing to add/remove modules as needed.

ID	Validated	Strategy	Result	Mandatory	Comments
SMC-SP24	N.A.				

Table 38: Smart Cities - SMC-UC06 Validation requirements' coverage.

8.6 Validation Summary

The following table gives a summary of the above validated use cases.

ID	Validated	Result	Comments
SMC-UC01	Partially	Success	The use case for this first phase have been included as preliminary steps for UC02 test. Not all necessary steps have been tested in line with the followed internal validation (using a lab test) approach.
SMC-UC02	Yes	Success	A complete test case have been performed according a defined scenario. Almost all requirements have been completely or partially addressed
SMC-UC03	Yes	Success	A complete test case have been performed according a defined scenario. Almost all requirements have been completely or partially addressed
SMC-UC04	Yes	Success	A complete test case have been performed according a defined scenario. Almost all requirements have been completely or partially addressed
SMC-UC05	Yes	Success	A complete test case have been performed according a defined scenario. Almost all applicable requirements have been addressed
SMC-UC06	Yes	Success	A complete test case have been performed according a defined scenario. All applicable requirements have been addressed

SMC-UC07	No	-	As documented in 5.2 this UC have been postponed in the second phase.
----------	----	---	---

Table 39: Smart Cities demonstrator's use cases validation summary.

8.7 Lessons Learned and Future Work

The sandbox replication of Genova online service to validate a user centric management of citizen personal data in compliance with the GDPR have highlighted some aspects of interoperability and use of the CaPe platform within the access flow to the services of the municipality, confirming that aspects of user experience and integration with legacy systems are two of the security and privacy challenges that must be addressed within smart city contexts. However, this has led to some extensions of the functionalities provided, in as-a-service mode, by the adopted solution (CaPe). The performed validation and shared results also put the basis of some extension and interaction with other solutions from WP3, in particular GENERAL_D of CNR, to analyse how to translate the legal basis of processing into enforceable access rules or how the collected consents and privacy disclaimers acceptance can be stored as hash certificate in DLT based solutions going to be analyzed in WP3 activities.

In order to support cross border scenarios we are going to enable the interaction with the Italian eIDAS node, in collaboration with Politecnico di Torino also involved in the project, in order to extend the use of online services also to European Union citizens, who can thus access them through the eIDs (digital identities) of the countries of origin. At the same time that integration will allow each European citizen as data subject to manage and control the legal basis of personal data processing during his/her interaction with the various services, by managing the given consents and checking which data is used, how and for what purpose. This integration is not completed in this first phase and not included in the test case for SMC-UC03. We plan to include it in the second phase.

From the cyber risk assessment carried out in Genoa, the need for specific training on cyber security emerged from the analysis of the result. In fact, the specific question " *Has the use case experience led to changes to your internal IT security policies/best practices/procedures?*" received a positive response, for its tangible feedback, towards leadership, of the problems arising from a lack of attention to cyber-security issues. Also the further lesson learned is the cyber risk assessment use case allowed to review individual internal processes and improve procedures. Where the improvement cannot be immediate, it still allows to plan the need to think and adopt new solutions.

The cyber risk assessment demonstrator case also highlighted another aspect. The LPA has a difficulty in retrieving financial information (like EBIT data) to fill the quantitative analysis questionnaire. This due to the lack of profit behind their activities.

Another interesting result came from the phishing simulation: the worst performance has been obtained by people with a high level of education, meaning that the cyber security awareness does not follow the usual education path, but it needs specific training courses to cover the gap.

From the test case executed in Murcia, multiple fronts that need to be improved have been identified. We noted the importance of taking advantage of the results in the privacy preserving identity management area to protect the Smart City resources. This will require efforts in integrating current and new identity management features, adapting them to the needs of the Smart City platform. At least, this will involve integration of new types of zero-knowledge predicates (range proofs), complete integration of p-ABC presentations into the XACML authorization framework of the platform and integration of DLT to improve reliability and trust in the identity management solution.

Another key point is the need to facilitate the protection of the diverse components of the architecture. In that vein, the pilot will include cyber threat intelligence and analysis platforms, taking special account in automation and sharing knowledge. In particular, we plan to integrate a MISP instance that retrieves Cyber threat information from compromised situations, with the goal that it will be possible to share information among the devices involved in the pilot, and even with other instances from the project.

In the Porto demonstrator, it is possible to showcase the value of data in a smart city. The user must have control over the information exchanged with the city. In this sense, this Porto Data Hub prototype will showcase the needs in a lab environment. This lab environment allows us to define a set of challenges that must be addressed in the future regarding user privacy/consent and especially identity.

As future work, it is also relevant to extend the search for tools available in the WP3 that allow to demonstrate and join synergies in a real environment to produce a safer environment. An example of this is the integration of the software development life cycle tools (WP3 T3.3) to increase the system's security using SOBEK.

All the identified solutions, ideas and lessons learned will constitute the first basis of the innovation area to put in operation in the second phase, by leveraging the CityXCity Catalogue²⁵ provided by OASC and planned to go live in December 2020. The catalogue allows cities and communities to browse solutions that are operational in cities already. The catalogue enables to exchange, among others, cyber security solutions that work, and for cities to get ideas and inspiration to ease the identification, uptake, collaboration and deployment of cyber security services for smart cities.

²⁵ <http://catalogue.city/>

9 Conclusions

In this document we present the Deliverable D5.3 – Validation Demonstration Case Phase 1. This deliverable builds upon the previous deliverable D5.2 [18]. We introduced seven demonstrators in our first deliverable D5.1 [1] and this deliverable marks the end of phase 1. This document provided a detailed validation strategy of the demonstrator's use cases, featuring test cases and technology based analysis. The validation approach consists of test case or technology based analysis. In some case both approaches are chosen. In both these approaches, a detailed description of the functionalities and aspects of the use case which will be validated is provided. This is followed by quality indicators covering the efficiency and efficacy of the solution. For each use case, we provide a validation summary. All the validation approaches

We concluded each demonstrator use case with a discussion of the lessons learned and future work. Here we took the opportunity to identify assets from WP3 that can be transferred and play a crucial role in future deliverables. During the second cycle of the project, we will define the requirements and specifications of each of the demonstrator use cases in greater depth and in the final deliverable of phase 2, we will describe the validation strategy in its final form.

10 References

- [1] [Sforzin 2019] CyberSec4Europe Deliverable D5.1: Requirements Analysis of Demonstration Cases Phase1. EU H2020-SU-ICT-03-2018 project. Editor Alessandro Sforzin 2019
<https://cybersec4europe.eu/wp-content/uploads/2020/06/D5.1-Requirements-Analysis-of-Demonstration-Cases-Phase-1-v3.0.pdf>
- [2] E. Androulaki, S. Cocco und C. Ferris, „Private and confidential transactions with Hyperledger Fabric,“ IBM, 11 May 2018. [Online]. Available: <https://developer.ibm.com/technologies/blockchain/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/>
- [3] J. Liu, W. Li, G. Karame und N. Asokan, „Scalable Byzantine Consensus via Hardware-assisted Secret Sharing,“ in IEEE Transactions on Computers, 2019.
- [4] L. Lamport, R. Shostak und M. Pease, „The Byzantine Generals Problem,“ ACM Transactions on Programming Languages and Systems, Bd. 4, Nr. 3, pp. 382-401, 1982.
- [5] M. Castro und B. Liskov, „Practical Byzantine fault tolerance,“ in 3rd Symposium on Operating Systems Design and Implementation, 1999.
- [6] G. S. Veronese, M. Correia, A. N. Bessani und L. C. Lung, „Efficient Byzantine Fault-Tolerance,“ IEEE Transactions on Computers, Bd. 62, Nr. 1, 2013.
- [7] T. Distler, C. Cachin und R. Kapitza, „Resource-Efficient Byzantine Fault Tolerance,“ IEEE Transactions on Computers, Bd. 65, Nr. 9, pp. 2807-2819, 2015.
- [8] D. Chaum: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM 24: 84–88 (1981)
- [9] D. Chaum: Security without identification: Transaction systems to make big brother obsolete. Commun.ACM 28: 1030–1044 (1985)
- [10] J. Camenisch, A. Lysyanskaya: A Signature Scheme with Efficient Protocols. SCN 2002: 268-289
- [11] J. Camenisch, E. Van Herreweghen: Design and implementation of the idemix anonymous credential system. CCS 2002: 21-30
- [12] S. Krenn, T. Lorünser, A. Salzer, C. Striecks: Towards Attribute-Based Credentials in the Cloud. CANS 2017: 179-202
- [13] U. Haböck, S. Krenn: Breaking and Fixing Anonymous Credentials for the Cloud. CANS 2019: 249-269

-
- [14] C. Paquin, G. Zaverucha: U-Prove Cryptographic Specification V1.1 (Revision 3). 2013
 - [15] Tor Project | Anonymity Online. <https://www.torproject.org/>
 - [16] RFC 2119 – IETF: Key words for use in RFCs to Indicate Requirement Levels, 1997, <https://www.ietf.org/rfc/rfc2119.txt>
 - [17] ARX: ARX introduction <https://arx.deidentifier.org/> , ARX github <https://github.com/arx-deidentifier/arx>
 - [18] [Sforzin 2020] CyberSec4Europe Deliverable D5.2: Specification and Set-up Demonstration case Phase 1. EU H2020-SU-ICT-03-2018 project. Editor Alessandro Sforzin 2020.
 - [19] European Convention on Human Rights https://www.echr.coe.int/documents/convention_eng.pdf
 - [20] Information Commissioner’s Office, Data protection impact assessments, (n.d.). <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/?q=DPIA>
 - [21] European Union Agency for Cybersecurity, Online tool for the security of personal data processing, (2019). <https://www.enisa.europa.eu/risk-level-tool/> (accessed 8 July 2020)
 - [22] CNIL, The open source PIA software helps to carry out data protection impact assesment, (2019). <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment> (accessed 8 July 2020).