Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D5.2

Specification and Set-up Demonstration case Phase 1

Document Identification	
Due date	30 April 2020
Submission date	15 May 2020
Revision	1.0

Related WP	WP5	Dissemination Level	PU
Lead Participant	NEC	Lead Author	Alessandro Sforzin (NEC)
Contributing Beneficiaries	ABI, AIT, ATOS, BBVA, CTI, DAWEX, ENG, ISGS, I-BP, NEC, SIE, TDL, UPRC, UPS-IRIT	Related Deliverables	D5.1

Abstract: This document presents deliverable "D5.2 – Specification and set-up Demonstration case Phase 1". For all the project demonstrators, we provide a detailed specification of all their respective use cases – which were introduced in deliverable D5.1 *Requirements Analysis of Demonstration case Phase 1* [1] – as well as an overview of the demonstrators' set-up once implemented and ready to be shown to the public. A demonstrator specification is a rigorous analysis of its components: for all its use cases, it lists their participants (e.g., stakeholders, actors) and their step-by-step workflows. We complement this information with diagrams giving a formal, graphic presentation of all use cases core functionalities. A demonstrator set-up shows how its use cases are assembled to bring the demonstrator to life. It also explains how the demonstrator will work from a user perspective, and how it will reach its intended audience. This document, therefore, provides detailed blueprints of all CyberSec4Europe's demonstrator cases and will guide their development and deployment stages.

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.

Executive Summary

CyberSec4Europe is an ambitious project addressing cybersecurity issues in the European 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 goal is to promote collaboration between industrial and academic participants to identify and analyse cybersecurity challenges in the selected sectors and develop innovative solutions to those challenges.

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. Over the course of the project's first year of activity, WP5 pinned down several use cases that serve as the basis of the demonstrators. Deliverable D5.1 [1] described them and analysed their requirements; it presents the results of many discussions with stakeholders and industry partners of each selected sector. The document served as input to the first version of the project's research roadmap [2], as well as to the initial set of research guidelines and technologies – also known as *assets* – that the demonstrators will integrate into their implementations [3, 4, 5, 6, 7, 8].

This document presents CyberSec4Europe's D5.2, titled "Specification and Set-up of Demonstration Case Phase 1". It builds upon the work reported in D5.1 [1] by further specifying the use cases of each demonstrator, and presenting a preliminary overview of what the demonstrators want to achieve to increase the cybersecurity resilience of their respective sectors. Whereas 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.

Jigsaw puzzles are a useful analogy to understand the relationship between a demonstrator and its use cases. In a jigsaw puzzle, interlocking pieces are put together to produce the complete picture. In WP5, the use cases are the interlocking pieces and the demonstrator is the picture we want to assemble. With this analogy in mind, D5.2 is the instruction manual that shows how to put the pieces together to compose the picture.

We structure the presentation of the demonstrators in two parts: specification and set-up. A demonstrator's specification formally analyses its use cases' workflow with step-by-step descriptions and diagrams. Its set-up shows how its use cases come together to implement its designed functionalities and describes how demonstrator will work once its development is complete.

Finally, D5.2 maps the demonstrators to WP3's assets. This is not a theoretical exercise; a demonstrator maps to only those assets that it will integrate into its prototype during the development cycle. WP3 and WP5 collaboration is mutually beneficial: one the one hand, WP3 produces assets (i.e., technologies) that satisfy WP5 demonstrators' requirements; on the other hand, WP5 ensures that these innovative technologies are integrated into the demonstrators, thus proving that CyberSec4Europe's research is not only relevant to the EU single market, but also effective in addressing cybersecurity issues in the relevant sectors.

Document Information

Contributors

Name	Partner
Antonio Marrone	ABI
Roberto Tordi	ABI
Mario Trinchera	ABI
Stephan Krenn	AIT
Juan Carlos Perez Baun	ATOS
Susana Gonzalez Zarzosa	ATOS
Miryam Villegas Jimenez	ATOS
Laura Chinellato	BBVA
Vasia Liagkou	CTI
Jérémy Decis	DAWEX
Marco Angelini	ENG
Vincenzo Savarino	ENG
Andrei Cheta Florica	ISGS
Laura Colombini	ISGS
Mederic Collas	I-BP
Paul Marty	I-BP
Victor Poyet	I-BP
Rahul Bobba	NEC
Alessandro Sforzin	NEC
Jorge Cuellar	SIE
Prabhakaran Kasinathan	SIE
Martin Wimmer	SIE
David Goodman	TDL
Christos Grigoriadis	UPRC
Eleni Maria Kalogeraki	UPRC
Panagiotis Kotzanikolaou	UPRC
Spyros Papastergiou	UPRC
Abdelmalek Benzekri	UPS-IRIT

Reviewers

Name	Partner
Marco Angelini	ENG
Ahad Niknia	GUF
Antonio Lioy	POLITO
Jozef Vyskoc	VAF

History

0.01	2019-11-18	NEC	Added ToC
0.02	2020-03-09	NEC	Added abstract, executive summary, and introduction.
0.03	2020-03-12	NEC, SIE	Added Section 3
0.04	2020-03-13	ATOS	Added Section 5
0.05	2020-03-13	ENG	Added Section 8
0.06	2020-03-13	TDL	Added Section 2
0.07	2020-03-13	UPRC	Added Section 6
0.08	2020-03-13	NEC	Added conclusions
0.09	2020-03-16	ATOS, DAWEX	Added Section 7
0.10	2020-03-23	AIT	Added Section 4
0.11	2020-03-23	NEC	Quality check. Submitted for high-level review to PC.
0.12	2020-03-27	ENG	Updated Section 8
0.13	2020-04-03	UPRC	Updated Section 6
0.14	2020-04-06	NEC	Submitted to internal reviewers.
0.15	2020-04-24	ENG	Addressed internal reviewers' comments about section 8.
0.16	2020-04-24	SIE, NEC	Addressed internal reviewers' comments about section 3.
0.17	2020-04-24	AIT	Addressed internal reviewers' comments about section 4.
0.18	2020-04-24	ATOS	Addressed internal reviewers' comments about sections 5.
0.19	2020-04-24	UPRC	Addressed internal reviewers' comments about section 6.
0.20	2020-04-24	TDL	Addressed internal reviewers' comments about section 2.
0.21	2020-04-24	ATOS	Addressed internal reviewers' comments about sections 7.
0.22	2020-04-24	NEC	Rewrote Executive Summary

0.23	2020-04-27	NEC	Fixed references to Figures throughout the document.
0.3	2020-04-28	NEC	Additional check. Version submitted to internal reviewers for 2nd round of review.
0.31	2020-04-29	NEC	Changed section 5 title to "Incident Reporting in the Financial Sector"
0.32	2020-05-08	TDL	Updated section 2
0.33	2020-05-08	NEC	Fixed broken figure links and figures numbering. Version ready for submission.
1.0	2020-05-12	GUF	Layout and graphical improvements, and preparation for submission

Table of Contents

1 Introduction 1

1.1 Structure of the Document 1

2 Open Banking 3

2.1 Use Cases Specification 4
2.1.1 Use Case OB-UC1: Sharing of Identity Verification and Fraudulent Activity 4
2.1.2 Use Case OB-UC4: Open Banking API Architecture 12

2.2 Demonstrator Set-up 21
2.2.1 Use Case OB-UC1: Sharing of Identity Verification and Fraudulent Activity 21
2.2.2 Use Case OB-UC4: Open Banking API Architecture 26

3 Supply Chain Security Assurance 32

3.1 Use Cases Specification 32
3.1.1 Use Case SCH-UC1: Supply Chain for Retail 32
3.1.2 Use Case SCH-UC2: Compliance and Accountability in Distributed Manufacturing 35

3.2 Demonstrators Set-up 44
3.2.1 Use Case SCH-UC1: Supply Chain for Retail 44
3.2.2 Use Case SCH-UC2: Compliance and Accountability in Distributed Manufacturing 47

4 Privacy-Preserving Identity Management 54

4.1 Use Cases Specification 54
4.1.1 Use case IDM-UC1: Registration 54
4.1.2 Use case IDM-UC2: Issuance 57
4.1.3 Use case IDM-UC3: Presentation 60
4.1.4 Use case IDM-UC4: Revocation 62
4.1.5 Use case IDM-UC5: Inspection 65
4.1.6 Use case IDM-UC6: Certificate Renewal 67
4.1.7 Use case IDM-UC7: De-registration 69

4.2 Demonstrator Set-up 71
4.2.1 Relation to Use Cases 72
4.2.2 Relation to WP3 Assets 72
4.2.3 Description and Workflow 72
4.2.4 Target Group 75

5 Incident Reporting in the Financial Sector 76

5.1 Use Cases Specification 76
5.1.1 Use case IR-UC1: Data Collection, Enrichment, and Classification 76
5.1.2 Use Case IR-UC2: Managerial Judgement 84
5.1.3 Use Case IR-UC3: Data Conversion and reporting preparation 88

5.2 Demonstrator Set-up 91
5.2.1 Relation to Use Cases 91
5.2.2 Relation to WP3 Assets 91
5.2.3 Description and Workflow 94
5.2.4 Target Group 97

6 Maritime Transport 98

6.1 Use Cases Specification 98
6.1.1 Use Case MT-UC1: Threat Modelling and Risk Analysis for Maritime Transport Services 98
6.1.2 Use Case MT-UC2: Maritime System Software Hardening 127
6.1.3 Use Case MT-UC3: Secure Maritime Communications 128
6.1.4 Use Case MT-UC4: Trust Infrastructure for Secure Maritime Communication 134

6.2 Demonstrator Set-up 139
6.2.1 Demonstrator MT- D1: Threat Modeling and Risk Analysis for Maritime Transport Services 140
6.2.2 Demonstrator MT- D2: Maritime System Software Hardening 145
6.2.3 Demonstrator MT- D3: Secure Maritime Communications and Trust Infrastructure for Secure Maritime Communication 147

7 Medical Data Exchange 150

7.1 Use Cases Specification 150
7.1.1 Use case MD-UC1: Sharing Sensitive Health Data through an API 151
7.1.2 Use case MD-UC2: Sharing Sensitive Health Data through Files 155
7.1.3 Use case MD-UC3: Enhancing the Security of On-Boarding and Accessing the Dawex Platform 158

7.2 Demonstrator Set-up 162
7.2.1 Relation to Use Cases 163
7.2.2 Relation to WP3 Assets 164
7.2.3 Description and Workflow 165
7.2.4 Target Group 169

8 Smart Cities 170

8.1 Use Cases Specification 170
8.1.1 Use Case SMC-UC1: Register Data Consumer and Manage Services 170
8.1.2 Use Case SMC-UC2: Discover and Consume City Data 173
8.1.3 Use Case SMC-UC3: Personal Data Sharing 178
8.1.4 Use Case SMC-UC4: Sensor Data Sharing and Processing 185
8.1.5 Use Case SMC-UC5: Assess Social Engineering Exposure by Simulating Phishing Attacks on Service Provider's Target Groups 189
8.1.6 Use Case SMC-UC6: Cyber Risk Assessment 192
8.1.7 Use Case SMC-UC7: Cybersecurity Needs and Solution Elicitation and Selection 194

8.2 Demonstrators Set-up 200
8.2.1 City of Murcia 200
8.2.2 City of Porto 204
8.2.3 City of Genova 205

9 Conclusions 214

10 Bibliography 215

List of Figures

Figure 1: Open Banking - General Open Banking Architecture 3
Figure 2: Open Banking - A fraudulent transaction takes place and a complaint is eventually lodged 9
Figure 3: Open Banking - : A reported fraudster is blocked from carrying out further fraudulent transactions 10
Figure 4: Open Banking - The credit renegotiation scam 11
Figure 5: Open Banking - A spoofing attack and the implications for legitimate users 14
Figure 6: Open Banking - An undetected spoofing attack 14
Figure 7: Open Banking - : A prevented spoofing attack 15
Figure 8: Open Banking - An undetected tampering attack 15
Figure 9: Open Banking - A prevented tampering attack 16
Figure 10: Open Banking - An undetected privilege escalation 16
Figure 11: Open Banking - A prevented privilege escalation 17
Figure 12: Open Banking - Attacker targets multiple endpoints to develop an exploitation strategy 18
Figure 13: Open Banking - Attacker finds a vulnerability to inject malicious code into API 19
Figure 14: Open Banking - Attacker compromises a service through getting access to an internal API 20
Figure 15: Open Banking - Payment fraud scenario's timeline 22
Figure 16: Open Banking - Monitoring and reporting a fraud report 23
Figure 17: Open Banking - Sharing payment fraud information 23
Figure 18: Open Banking – Verifying a suspected fraudulent request 24
Figure 19: Open Banking - A tampering attack and its consequences for the victims 28
Figure 20: Open Banking - Schema representing an attacker exploiting a vulnerability to realize a privilege escalation with the relative consequences for the victims 30
Figure 21: Supply Chain Security Assurance - SCH-UC1 Use case diagram showing the steps involved in a dispute resolution between a warehouse and a retailer store. 35
Figure 22: Supply Chain Security Assurance - Initial phase where T_Design and T_FeasibilityStudy as input tokens exist. 40
Figure 23: Supply Chain Security Assurance - Transition PublishDesign consumes both tokens and creates a new token T_DesignPublished. 41
Figure 24: Supply Chain Security Assurance - Tokens T_DesignPublished and T_NoBoAcceptance are available. 42
Figure 25: Supply Chain Security Assurance - End of the basic demonstration flow where the Design has been accepted via T_DesignAccepted. 43
Figure 26: Supply Chain Security Assurance – SCH-UC1 Demonstrator's main view. 46
Figure 27: Supply Chain Security Assurance - Illustration of a typical retail supply chain. 47
Figure 28: Supply Chain Security Assurance - Workflow GUI: Step 1 (login) 47
Figure 29: Supply Chain Security Assurance - Workflow GUI: Step 2 (workflow selection) 48
Figure 30: Supply Chain Security Assurance - Workflow GUI: Step 3 (Petri Net view) 49
Figure 31: Supply Chain Security Assurance - Workflow GUI: Step 4 (Places view) 50
Figure 32: Workflow GUI: Step 5 (Transition view) 50
Figure 33: Supply Chain Security Assurance - Different layers of the proposed DEMO architecture. 51
Figure 34: Privacy-Preserving Identity Management - Relations among use cases of the identity management demonstrator 54
Figure 35: Privacy-Preserving Identity Management - IDM-UC1 Diagram 55
Figure 36: Privacy-Preserving Identity Management - IDM-UC1 Basic Flow 57
Figure 37: Privacy-Preserving Identity Management - IDM-UC2 Diagram 58
Figure 38: Privacy-Preserving Identity Management - IDM-UC2 Basic Flow 59
Figure 39: Privacy-Preserving Identity Management - IDM-UC3 Diagram 60

Figure 40: Privacy-Preserving Identity Management - IDM-UC3 Basic Flow 62
Figure 41: Privacy-Preserving Identity Management - IDM-UC4 Diagram 63
Figure 42: Privacy-Preserving Identity Management - IDM-UC4 basic flow 64
Figure 43: Privacy-Preserving Identity Management - IDM-UC5 diagram 65
Figure 44: Privacy-Preserving Identity Management - IDM-UC5 basic flow 66
Figure 45: Privacy-Preserving Identity Management - IDM-UC6 diagram 67
Figure 46: Privacy-Preserving Identity Management - IDM-UC6 basic flow 68
Figure 47: Privacy-Preserving Identity Management - IDM-UC7 diagram 69
Figure 48: Privacy-Preserving Identity Management - IDM-UC7 basic flow 71
Figure 49: Privacy-Preserving Identity Management - Demonstrator's high-level architecture 73
Figure 50: Privacy-Preserving Identity Management - Overview of the demonstrator's software layers 74
Figure 51: Privacy-Preserving Identity Management - Application overview of the IdM provider 75
Figure 52: Incident Reporting – IR-UC1 Data Collection, Enrichment, and Classification Use Case Diagram 77
Figure 53: Incident Reporting - Actors involved in use case IR-UC1 79
Figure 64: Incident Reporting - IR-UC1 Basic Flow 84
Figure 55: Incident Reporting – IR-UC2 Managerial Judgement Use Case Diagram 85
Figure 56: Incident Reporting - Actors involved in use case IR-UC2 85
Figure 57: Incident Reporting - IR-UC2 Basic Flow 87
Figure 58: Incident Reporting - IR-UC3 Data Conversion and Reporting Use Case Diagram 88
Figure 59: Incident Reporting - Actors involved in use case IR-UC3 89
Figure 60: Incident Reporting - IR-UC3 Basic Flow 90
Figure 61: Incident Reporting - Demonstrator's Architecture 94
Figure 62: Incident Reporting - Flowchart foreseen in the use cases of the Mandatory Incident Reporting demonstrator 96
Figure 63: Maritime Transport - Basic Flow of the Asset Declaration Process 101
Figure 64: Maritime Transport - Basic Flow of the Networks Management/Association of Assets with Networks Process 101
Figure 65: Maritime Transport - Basic Flow of the Assets Customization Process 102
Figure 66: Maritime Transport - Basic Flow of the Maritime Service Initiation and the Service Process Declaration Processes 105
Figure 67: Maritime Transport - Basic Flow of the Vulnerabilities Declaration Process 108
Figure 68: Maritime Transport - Basic Flow of the Vulnerabilities Synchronization and Management Process 109
Figure 69: Maritime Transport - Basic Flow of the Threats Declaration Process 111
Figure 70: Maritime Transport - Basic Flow of the Threats Synchronization and Management Process 111
Figure 71: Maritime Transport - Basic Flow of the Security Controls Declaration Process. 112
Figure 72: Maritime Transport - Basic Flow of the Attack Scenario Declaration Process 114
Figure 73: Maritime Transport - Basic Flow of the Risk Assessment Initiation Process 117
Figure 74: Maritime Transport - Basic Flow of the Involved Assets Preview Process 118
Figure 75: Maritime Transport - Basic Flow of the RA Summary Preview Process 119
Figure 76: Maritime Transport - Basic Flow of the RA Involved Assets Preview Process 121
Figure 77: Maritime Transport - Basic Flow of the Attack Paths Generation and Visualization Process 122
Figure 78: Maritime Transport - Basic Flow of the Review Risk Assessment Results Process 124
Figure 79: Maritime Transport - Basic Flow of the Attack Path Analysis Scenarios Execution Process 125
Figure 80: Maritime Transport - Basic Flow of the Mitigation Strategy Selection Process 126
Figure 81: Maritime Transport – Use case MT-UC3.1: VTS transmits to Vessels. 131

Figure 82: Maritime Transport - Use case MT-UC3.2: Vessels broadcast to vessels. 132
Figure 83: Maritime Transport - Use case MT-UC3.3: Vessel transmits vessel voyage information to VTS 133
Figure 84: Maritime Transport - Use case MT-UC3.4: Maritime Single Window Reporting 134
Figure 85: Maritime Transport - The Public Key Infrastructure (PKI) to be used in the demonstrations. 135
Figure 86: Maritime Transport - Use case MT-UC4.1: Establishing the PKI – Root CA establishment (Process 1) 137
Figure 87: Maritime Transport - Use case MT-UC4.1: Establishing the PKI – Intermediate CA etsablishment (Process 2) 137
Figure 88: Maritime Transport - Use case MT-UC4.2: Operating the PKI – Enrolment of new end entities into the PKI (Process 1 and 2) 138
Figure 89: Maritime Transport - Use case MT-UC4.2: Operating the PKI – Revocation of end entities from the PKI (Process 3) 139
Figure 90: The Risk Assessment Services of the CyberSec4Europe Maritime Transport System .. 142
Figure 91: Maritime Transport - Overview of the demonstrator's first round. 148
Figure 92: Maritime Transport - An overview over the physical realisation of the demonstrator's second round. 148
Figure 93: Medical Data Exchange - Services general view 150
Figure 94: Medical Data Exchange - UML diagram for MD-UC1 sharing sensitive health data through an API 151
Figure 95: Medical Data Exchange - MD-UC1 Basic flow diagram 154
Figure 96: Medical Data Exchange - MD-UC2 UML diagram 156
Figure 97: Medical Data Exchange - MD-UC2 Basic flow diagram 158
Figure 98: Medical Data Exchange - MD-UC3 UML diagram 159
Figure 99: Medical Data Exchange - MD-UC3 Basic flow diagram 161
Figure 100: Medical Data Exchange - MD-UC3.1 basic flow diagram 162
Figure 101: Medical Data Exchange - MD-UC3.2 basic flow diagram 162
Figure 102: Medical Data Exchange – Dawex DEP architecture high-level view 165
Figure 103: Medical Data Exchange – Task T5.6 demonstrator high-level view architecture 166
Figure 104: Medical Data Exchange - High-level view of services interaction with the Dawex DEP 167
Figure 105: Medical Data Exchange - Crypto service, DEP and stakeholder’s interaction in use case MD-UC1 167
Figure 106: Medical Data Exchange - Anonymization service, DEP and stakeholder’s interaction in use case MD-UC2. 168
Figure 107: Medical Data Exchange - Anonymization service and DEP detailed interaction in use case MD-UC2. 168
Figure 108: Medical Data Exchange - SPeIDI and DEP interaction in use case MD-UC3 169
Figure 109: Medical Data Exchange - SPeIDI and DEP detailed interaction in use case MD-UC3. 169
Figure 110: Smart Cities - SMC-UC1 use case diagram 171
Figure 111: Smart Cities - SMC-UC2 data discovery use case diagram 175
Figure 112: Smart Cities - SMC-UC2 discover and consume city data use case flow diagram 176
Figure 113: Smart Cities - SMC-UC3 Service description and registration use case flow diagram 181
Figure 114: Smart Cities - SMC-UC3 Service linking use case flow diagram 182
Figure 115: Smart Cities - SMC-UC3 Consent request use case flow diagram 183
Figure 116: Smart Cities - SMC-UC3 Data request use case flow diagram 184
Figure 117: Smart Cities - SMC-UC3 Usage control use case flow diagram 185
Figure 118: Smart Cities - SMC-UC4 Sensor data sharing and processing use case flow diagram 187
Figure 119: Smart Cities - SMC-UC4 use case alternate flow diagram 188

Figure 120: Smart Cities - SMC-UC5 Social driven vulnerability assessment use case flow diagram 191
Figure 121: Smart Cities - SCM-UC6 Cybersecurity risk assessment use case flow diagram 194
Figure 122: Smart Cities - SCM-UC7 Problem Definition flow diagram 195
Figure 123: Smart Cities - SCM-UC7 Idea Generation flow diagram 196
Figure 124: Smart Cities - SCM-UC7 Idea Selection and Refinement flow diagram 196
Figure 125: Smart Cities - SCM-UC7 Solution Selection flow diagram 197
Figure 126: Smart Cities - Fiware architecture implemented in Murcia 201
Figure 127: Smart Cities - Secure data-access infrastructure 203
Figure 128: Smart Cities - CaPe in the Municipality architecture 208
Figure 129: Smart Cities - Usage of CaPe 208
Figure 130: Smart Cities - LPA phishing campaign attack - phase 1 209
Figure 131: Smart Cities - LPA phishing campaign attack - phase 2 210
Figure 132: Smart Cities - LPA TO4SEE Awareness and mitigation 210
Figure 133: Smart Cities - LPA Phishing Recognition 211
Figure 134: Smart Cities - LPA clerks, services and assets 212
Figure 135: Smart Cities - LPA clerks, services and assets evaluated 212
Figure 136: Smart Cities - RATING reports and possible mitigation solutions 213
Figure 137: Smart Cities - LPA adopted mitigation solutions 213

List of Tables

Table 1: Incident Reporting - Criteria for the classification of security incidents (source: EBA Guidelines on major incident reporting under PSD2, page 23) 81
Table 2: Incident Reporting - Criteria for the classification of security incidents (source: EBA Guidelines on major incident reporting under PSD2, page 23) 81
Table 3: Medical Data Exchange - Use cases and assets mapping. Implementation and integration plan 164

List of Acronyms

AIRE	Atos Incident Reporting Engine
AIS	Automatic Identification System
AOS	Advanced Object detection System
API	Application Programming Interface
ATM	Automated Teller Machine
B2C	Business to Citizen
BIT	Business Information and Tracking
CA	Certification Authority
CCN	Common Communication Network
CFO	Chief Financial Officer
CISO	Chief Information Security Officer
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CR	Consent Receipt
CRO	Chief Risk Officer
CyberSec4Europe	CyberSec4Europe
CSR	Consent Status Receipt
CSS	Container Status System
CT	Capacity Token
CVE	Common Vulnerabilities and Exposures
DEMO	Demonstrator
DID	Decentralized Identity
DIF	Decentralized Identity Foundation
DNS	Domain Name System
DP	Dynamic Positioning system
DPO	Data Protection Officer
EBA	European Banking Authority
EBITDA	Earnings Before Interest, Taxes, Depreciation and Amortization
EC3	European Cybercrime Centre
ECB	European Central Bank
ECDIS	Electronic Chart Display and Information System
eIDAS	Electronic IDentification Authentication and trust Services
EMCS	Excise Movement and Control System
EPC	Engineering, Procurement & Construction
FBF	French Banking Federation

FI	Financial Institution
GDPR	General Data Protection Regulation
GOS	Gate Operative System
GUI	Graphical User Interface
HADES	Automatic Analysis of Malware Samples
IBAN	International Bank Account Number
ICLT	Incident CLassification team
ICT	Information and Communication Technologies
IdM	Identity Manager
IDM-UCx	Privacy-Preserving Identity Management Use Case x
IMO	International Maritime Organization
IMT	Incident Management Team
IR-UCx	Incident Reporting Use Case x
IoT	Internet of Things
IRT	Incident Reporting Team
JUDAS	JSON Users and Device Analysis tool
KYC	Know Your Customer
LEA	Law Enforcement Agency
LoLo	Lift-On-Lift-Off vessels
MD-UCx	Medical Data Exchange Use Case x
MT-UCx	Maritime Transport Use Case x
MISP	Malware Information Sharing Platform
NCA	National Competent Authorities
NGSI	Next Generation Service Interface
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NoBo	Notification Body
OBA	Open Banking API Architecture
OBSIDIAN	Open Banking Sensitive Data Sharing Network for Europe
OB-UCx	Open Banking Use Case x
OES	Operator of Essential Service
OF2CEN	On-line Fraud Cyber Centre and Expert Network
OSMP	Observatory for the Security of Means of Payment
PA	Public Administration
PAP	Policy Administration Point
PCS	Port Community System

PDP	Policy Decision Point
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technology
PFSO	Port Facility Security Officer
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PMIS	Port Management Information System
PSD2	Payment Service Directive 2
PSI	Private Set Intersection
PSP	Payment Service Provider
REST	Representational State Transfer
RCS	Radio Communication System
RoRo	Roll-on/Roll-off vessels
RTUs	Remote Terminal Units
SCA	Strong Customer Authentication
SCADA	Supervisory Control and Data Acquisition
SCH-UCx	Supply Chain Security Assurance Use Case x
SDK	Software Development Kit
SDVA	Social Driven Vulnerability Assessment
SIE	Siemens
SIS	Ship Information System
SLR	Service Link Record
SMC	Smart City
SMC-UCx	Smart Cities Use Case x
SME	Small to Medium-sized Enterprise
SMTP	Simple Mail Transfer Protocol
SPARQL	Protocol and RDF Query Language
SSM	Single Supervisory Mechanism
SSO	Single Sign On
SSO (Maritime Transport)	Ship Security Officer
SSR	Service Link Status Record
TOS	Terminal Operating System
TÜV	Technischer Überwachungsverein / Association for Technical Inspection
UAF	Unified Authentication and Authorization Framework
UC	Use Case
UML	Unified Modelling Language

VIS	Visitor Information Service
VTMS	Vessel Traffic Management System
VTS	Vessel Traffic Service
WMS	Warehouse Information Service
WP	Work Package
XACML	eXtensible Access Control Markup Language

1 Introduction

Deliverable D5.1 [1], titled "Requirements Analysis of Demonstration Cases Phase 1", research centres and industry members of Work Package 5 (WP5) worked in concert to identify an initial set of requirements for the seven demonstration cases – also known as "demonstrators". These requirements played a key role in identifying the technological and research roadmaps of the project [2]. For each demonstration case, D5.1 presented its use cases and their functional and non-functional requirements describing the conditions that ensure the system's correct operations.

The demonstration cases are the core of the project, the results of a coordinated effort 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 work WP5 did to produce D5.1. We go deeper in the engineering side of the demonstrators. For each demonstrator, we structure the discussion in two parts:

- *Specification* presents a traditional software engineering analysis of the use cases. After a description of the use case's scenario, it lists its preconditions, workflow, preconditions, and relationship (if any) with other use cases. UML diagrams complement the use case's workflow, providing further clarity to its functionalities.
- *Set-up* discusses the demonstrators as the sum of their use cases. It connects the demonstrator to its use cases, describes its functionalities and workflow. Where possible, we go further and provide an initial description of the demonstrator's user interface. Finally, we emphasize the connection between WP3's assets and WP5's demonstrators by listing which assets the demonstrator plans to use and how it will use them.

D5.2 is a fundamental step in CyberSec4Europe's (and WP5 in particular) roadmap. We acknowledge that, at this stage of the project, the demonstrators are their infancy. The information in this document may change in the project's second cycle, especially the "set-up" part of the discussion. Therefore, where we were not yet ready to provide details, we outlined future plans for the demonstrators.

1.1 Structure of the Document

The document is structured as follows:

- Section 2 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Open Banking* demonstration case.
- Section 3 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Supply Chain Security Assurance* demonstration case.
- Section 4 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Privacy-preserving Identity Management* demonstration case.
- Section 5 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Incident Reporting in the Financial Sector* demonstration case.
- Section 6 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Maritime Transport* demonstration case.
- Section 7 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Medical Data Exchange* demonstration case.

- Section 8 presents the use cases' specification and demonstrator's set-up of CyberSec4Europe's *Smart Cities* demonstration case.

Finally, section 9 concludes the document.

2 Open Banking

This section provides an overview of two demonstration use cases entitled:

(1) *Share Your Fraud* consists of two individual scenarios *Means of Payment Fraud* and *Credit Renegotiation Broker Fraud*. The demonstrators illustrate how the OBSIDIAN network and the KYC sharing technologies can be applied to either prevent fraud or intervene after a set of fraudulent transactions have taken place. The first section gives an overview of the two scenarios, presenting relevant interaction workflows and describing their actors. The rest of the section provides details on the demonstrator setup and the intended target groups.

(2) *Open Banking API Architecture* features six similar but distinct scenarios:

(1) Illegal access to the system

(2) Unauthorised information change

(3) Unauthorised escalation of privilege

(4) Data leak

(5) Massive data leak through HTTP client

(6) Compromised service

This section provides a high-level overview of the demonstration use case and its goals, followed by a description of the actors involved, pre/post conditions and a basic flow diagram.

Finally, we report relevant constraints and assumptions to be considered while implementing this demonstration use case.

For all six scenarios the reference architecture and its components are described in the following figure which represents a general API-based Open Banking platform.

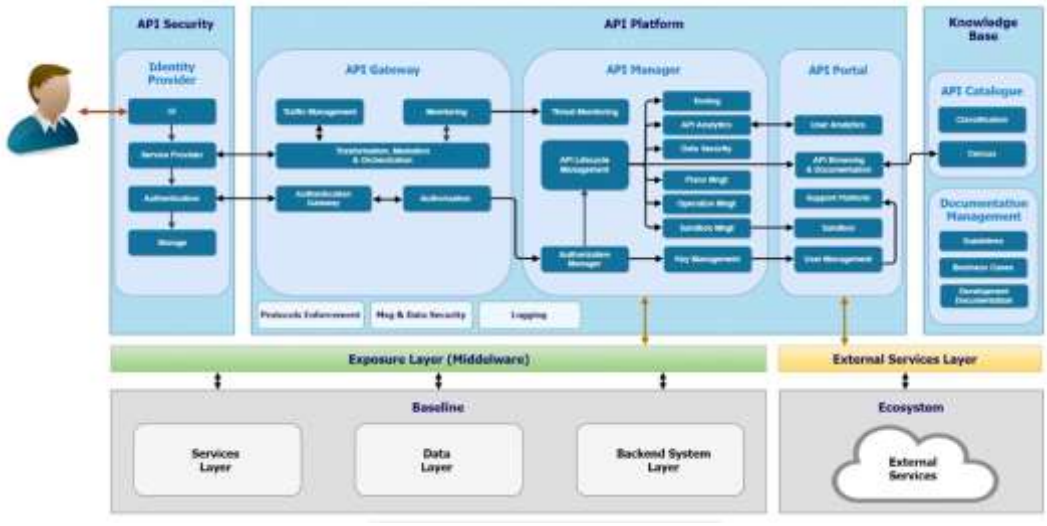

Figure 1: Open Banking - General Open Banking Architecture

2.1 Use Cases Specification

2.1.1 Use Case OB-UC1: Sharing of Identity Verification and Fraudulent Activity

Today financial fraud is global. As bank strategies are focused on digitalising critical processes like opening a bank account or adding a transfer beneficiary to a bank account, it has become very easy for hackers to carry out fraudulent transactions from their living rooms within a short period of time and without their physical identity being fully exposed.

Moreover, they can attack several banks without having to change their mode of operation, given that today banks don't share information on frauds that have been effective and any associated data.

Finally, with new applications of technologies like Instant Payment which provide bank users with real time money transfer services, it will be even more difficult to fight fraud, as banks won't have any time delay in which to carry out recalls in case of fraudulent transactions.

We propose to experiment the implementation of a *trust network* aimed at providing banks with a channel to share and exchange critical information about effective frauds, leveraging the latest online open banking services

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

In France, between 2017 and 2018, the introduction of fraud cheques significantly increased in all bank networks. The fraudster uses a single operational mode which consists of opening an account in a given bank, crediting it with money from some fraudulent cheque provided by another bank, and, before the cheque can be detected as fraudulent, transferring the credited money to another bank account in order to withdraw the money from a cash machine.

Another consequence of the lack of cooperation between banks is the rising leadership in Europe of non-European ICT providers in the field of risk scoring, leveraging globalised fraud information centralisation. Several of these ICT providers[1] offer risk management services aimed at scoring transactions in a bank information system to detect which ones are fraudulent. But:

- Few or none of them offer services featuring all fraud typologies (transfer fraud, cash machine fraud, cheque fraud, payment fraud etc.);
- Their solutions are based on black box architectures to protect their competitive advantage.

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

- To become leaders in the field of centralisation and correlation of fraud information by contracting one-on-one with each bank;
- To increase their market leadership by fuelling their product roadmaps with sharp knowledge of globalised fraud use cases, and then becoming essential actors by creating evidenced-based addictions to their services.

Finally, several organisations aiming at developing cooperation between financial actors already exist[2] but the data they share isn't that of frauds that have been effective: for example, an IBAN signature used to realise a

[1] IBM, ThreatMetrix, Ping Identity and others
[2] https://www.first.org/; https://ec.europa.eu/anti-fraud/

fraudulent transfer. These organisations are more focused on delivering cyber threat intelligence services and less on sharing effective transfer fraud information.

Fraud Trends

The security aspects of PSD2 including the introduction of strong customer authentication (SCA) help the fight against fraud leveraging identity theft techniques. Nonetheless, the majority of financial losses are due to successful modes of fraud operations for which user authentication is inadequate. These include scenarios in a report based on fraud data from a major French bank in which:

- the legitimate user is manipulated through various social engineering techniques (technician or supplier fraud and other scams), which constitute 37% of fraud cases;
- However, the most prevalent instances of fraud occur when the fraudster is a deceitful customer who carries out the transfer of funds from an unsuspecting bank on the basis of creditworthiness derived from bogus documentation, which represents 54% of fraud cases.

Counter Fraud Strategy

In order to demonstrate countermeasures to prevent fraudsters from being validated as a payee in fraudulent transactions and from easily opening any account by using falsified, false or stolen KYC information, the demonstrator has adopted three complementary work streams, based on extending existing methodologies:

(1) **Scoring transactions:** currently banks carry out contextual risk assessment through terminal and connection behavioural analysis (using, for example, scoring endpoint technologies like IBM Trusteer). We extend this analysis to a payee's data by sharing fraudulent IBANs between open banking players, ensuring adequate conformity to the GDPR and the French banking secrecy law[3];

(2) **Profiling frauds:** at present the approach to surveilling a fraudster's modes of operation is through the detection of any falsified, false or stolen documents used to open a bank account. In France, the first ongoing action consists of requesting information about a stolen or falsified identity document to the central database operated by ANTS[4] to detect any fraudulent use during the account onboarding process. The intention of the demonstrator is to use blockchain-based[5] and other KYC-sharing technologies to detect any KYC similarities between an already experienced fraud and an ongoing online account onboarding transaction, by offering a platform to European banking players to share these critical pieces of information, while guaranteeing compliance to the GDPR and any national banking secrecy requirements;

(3) **Digital identity integration:** supporting trustful and deeply verifiable identities is seen to be a powerful strategy to prevent any fraud occuring without requiring the fraudster to reveal his physical identity. That's why we propose to demonstrate verifiable claims based on a FIDO extension[6] to qualify a digital identity through a trustful partner eco-system.

Real World Examples

For the two scenarios being discussed, here are real world accounts of these frauds:

(1) Means of Payment Fraud

A news report in La Voix du Nord, dated 25 September 2019[7], stated:

[3] Due to business secrecy, bank aren't authorised to directly exchange business information

[4] Agence Nationale des Titres Sécurisés, https://ants.gouv.fr/

[5] See, for example, *D5.1 Requirements Analysis of Demonstration Cases Phase1*, Section 3.4.3 et passim

[6] UAF (Unified Authentication and Authorization Framework) - https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.html

[7] https://www.lavoixdunord.fr/642166/article/2019-09-25/plusieurs-banques-de-valenciennes-victimes-d-escrocs-belges?&pooolrelease

Several banks in Valenciennes victims of Belgian crooks

Last week, four Belgian nationals were sentenced to six months suspended sentence. Thanks to false pay slips or invoices, they swindled several banks in Valenciennes. The prosecution assessed the damage at around 30,000 euros.

These four Belgian nationals opened numerous accounts in bank branches using false documents to obtain cards and chequebooks. Then all they had to do was to draw down all they could in cash, often with transactions of several thousand euros. In one week, one of the fraudsters opened five accounts in Valenciennes branches with false pay slips and a false EDF bill; another opened ten accounts in twenty-five days.

*M. Riglaire, who represented one of the banks victims to these scams, denounced a recurring problem in the region. According to him, "*it's a real problem" *which occurs "*two, three times a week in Hauts-de-France".

(2) Credit Renegotiation Broker Fraud

According to the Assurance Banque Epargne Info Service[8]:

Watch out for identity theft.

Financial scams are more and more numerous and more and more sophisticated (fraudulent websites and emails, canvassing by telephone).

These scams concern all banking products, insurance and investments. These are, for example, false accounts, passbooks, investments in Forex, binary options but also diamonds, crypto-assets, forests, wine or even livestock ...

The crooks use identity theft techniques which can take several forms:

- ***usurpation of your identity**: they use your personal data to open an account or take out credits in your name;*
- ***impersonation of a financial institution**;*
- ***the impersonation of a supervisory authority or its staff** to convince you to perform certain operations.*

***So be extremely vigilant!** Get informed and follow our advice to better protect yourself!*

2.1.1.1 Stakeholders

The main stakeholders in this demonstration use case are:

- **European banks and other Open Banking players** (including payment operators) have an economic interest in such a trust network: they would be able to mitigate their fraud losses and improve trust and then the loyalty of their **customers** by better protecting them from attempted fraud. Extended use cases of such a trust network could include sharing not only blacklist but whitelist information too, that could be used to improve user experience with less friction linked to security procedures and fewer false positive security alerts raised.

[8] https://www.abe-infoservice.fr/vos-demarches/se-proteger-contre-les-arnaques/les-alertes-et-mises-en-garde-des-autorites-au-public/attention-aux-usurpations-didentite#2

- Trust between members of this network could be created by leveraging existing **certification authority** eco-systems (CA, banking authorities et al.). These kinds of actors would have a business interest to participate.
- **Legislators** and **privacy professionals** would be involved to create the legal framework. Those in charge of regulation writing and privacy concerns would be involved to create the legal framework, such as the **European Data Protection Board**.
- **Europol,** as well as Interpol and other international LEAs (Law Enforcement Agencies), would also have an important interest in being able to use data related to money laundering, terrorist and criminal financing activities.
- **Cybersecurity providers** would have a business interest in either implementing the network through innovative technologies or leveraging information output by the network to design other use cases focused on other businesses (such as SMEs, and vertical sectors such as transport or insurance).

2.1.1.2 Actors

The actors listed below are all the entities that interact with the open banking ecosystem which can be of two types:

(i) **Primary actors** have goals which this demonstration case needs to fulfil; and

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

For the first release of the demonstrator we are focussing on two scenarios associated with sharing fraud information.

(1) **Means of Payment Fraud** involves:

(i) Primary actors:

- The **customer** who interacts with the bank to establish an account which then provides ready access to cash and credit. Ironically perhaps, the customer is either the individual or representative of a criminal organisation intent on defrauding as many financial institutions as possible in a number of different ways. From the perspective of the bank or the merchant, the bona fide customer, who has opened an account and is carrying out everyday transactions, only gets unmasked as a fraudster after the fraud is detected;
- The **bank is** represented by a fraud expert who carries out due diligence on the account request through KYC procedures and provides the mechanisms for the **customer** to get access to cash and credit facilities. The banks or financial institutions being targeted are the ones to incur financial loss and loss of brand credibility. Typically, if a fraudster is successful with one bank or financial institution, he will move on to attack another.

(ii) Secondary actors:

- The **merchant** receives the ill-gotten monies from the **customer** i.e., the shops, restaurants, retailers and others who the fraudster attempts to falsely transact with. Ideally, the fraudster, , who could be situated in any worldwide jurisdiction, would seek transactions that are single event or anonymous to avoid detection as long as possible.

(2) **Credit Renegotiation Broker Fraud** involves:

(i) Primary actors:

- The **fraudster** is the individual or representative of a criminal organisation (and who, depending on their mode of operation, could also be a bank customer) who interacts with the user in order to get requisite credentials/documents with the intention of defrauding the user;
- The **user** has a pre-existing arrangement with a credit company and is the target of the fraud.

(ii) Secondary actors:

- The **credit company** is a passive recipient of credit facility requests unaware that they are fraudulent (because they don't have the means to be informed);
- The **bank** is also acting as the recipient of ill-gotten monies from the fraudster that the user eventually seeks reimbursement for.

The demonstrator will be extended in the next phase of the project with more scenarios, intervention/detection mechanisms and potentially additional actors.

2.1.1.3 Preconditions

The banks and the credit companies have aligned KYC mechanisms and participate in the OBSIDIAN network to fight fraud between institutions both nationally and cross-border.

The demonstration workflows start at the point when, in the first scenario, the customer approaches the bank and in the second when the fraudster first contacts the user.

2.1.1.4 Basic Flow

Means of Payment Fraud

Step 1: A bank (or a customer) is defrauded or an attempted fraud takes place (see Figure 2). A complaint is filed.

The information required to detect the fraud are the documents provided to the bank and their associated identity-related data, details of the transaction, the payee's IBAN and the context of the enrolment (for example, online vs face-to-face).

Step 2: The victim bank blocks the IBAN and reports it to the fraudulent IBAN sharing tool.

Step 3: The fraudster carries out another transaction (either fraudulent or not) on a customer at another bank, which receives an alert allowing it to monitor the transaction to prevent any fraud taking place.

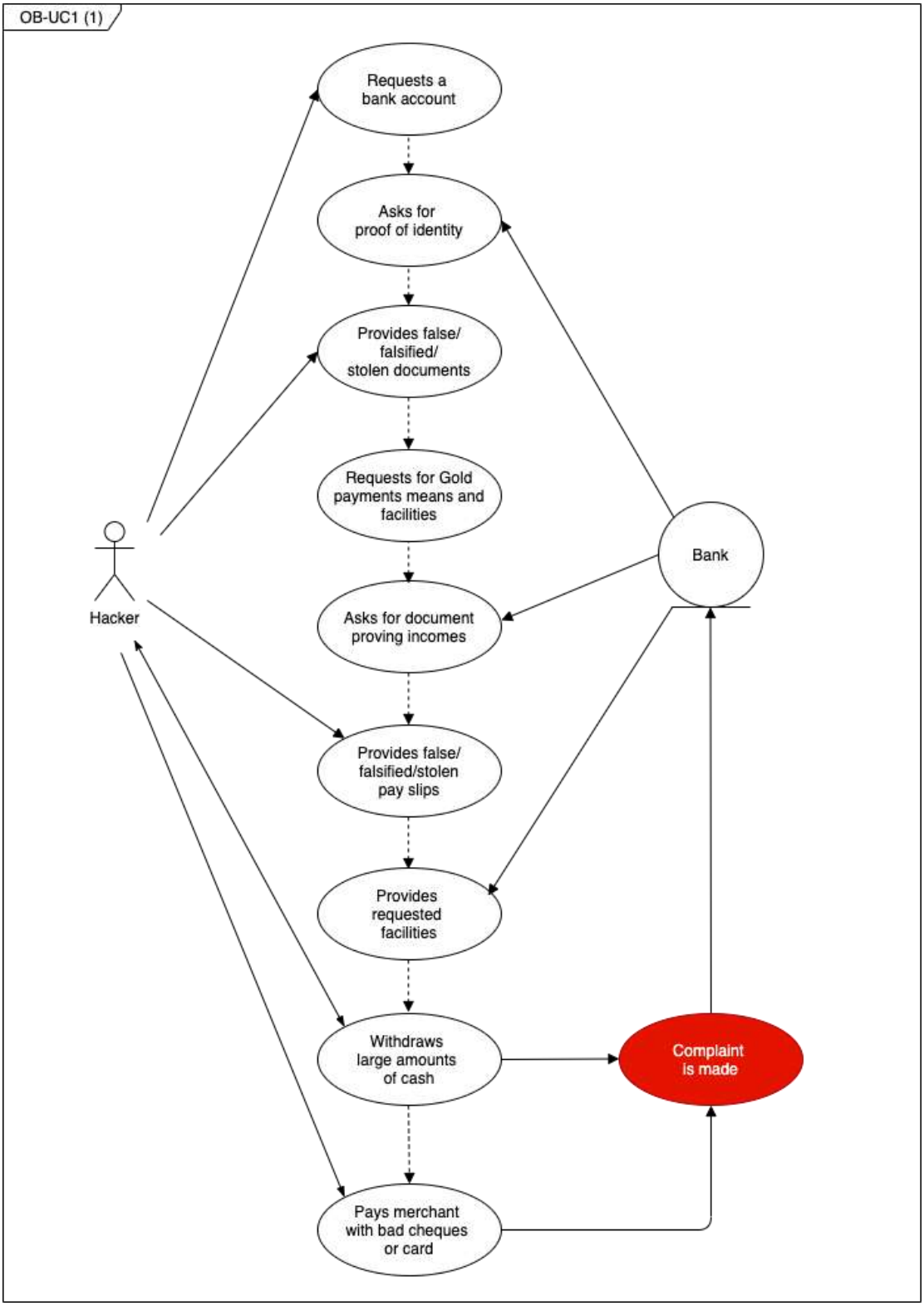

Figure 2: Open Banking - A fraudulent transaction takes place and a complaint is eventually lodged

Next Steps

Step 1: A bank detects a false document or an authentic document used fraudulently following a fraud or during an attempt to enter into a relationship.

The information required to detect the fraud are the documents provided to the bank and the

IBAN used to transfer the monies to.

Step 2: The bank reports the forged document or the fraudulent use of authentic documents in an interbank fraud repository. Additionally, the bank reports the fraudulent use of a stolen or lost document to ANTS[9] or their European equivalents.

Step 3: Other banks can protect themselves against customers attempting to enter into fraudulent relationships and committing fraud by controlling on the fly the input documents and detecting the presence of false documents or authentic documents used fraudulently in their information systems (see Figure 3).

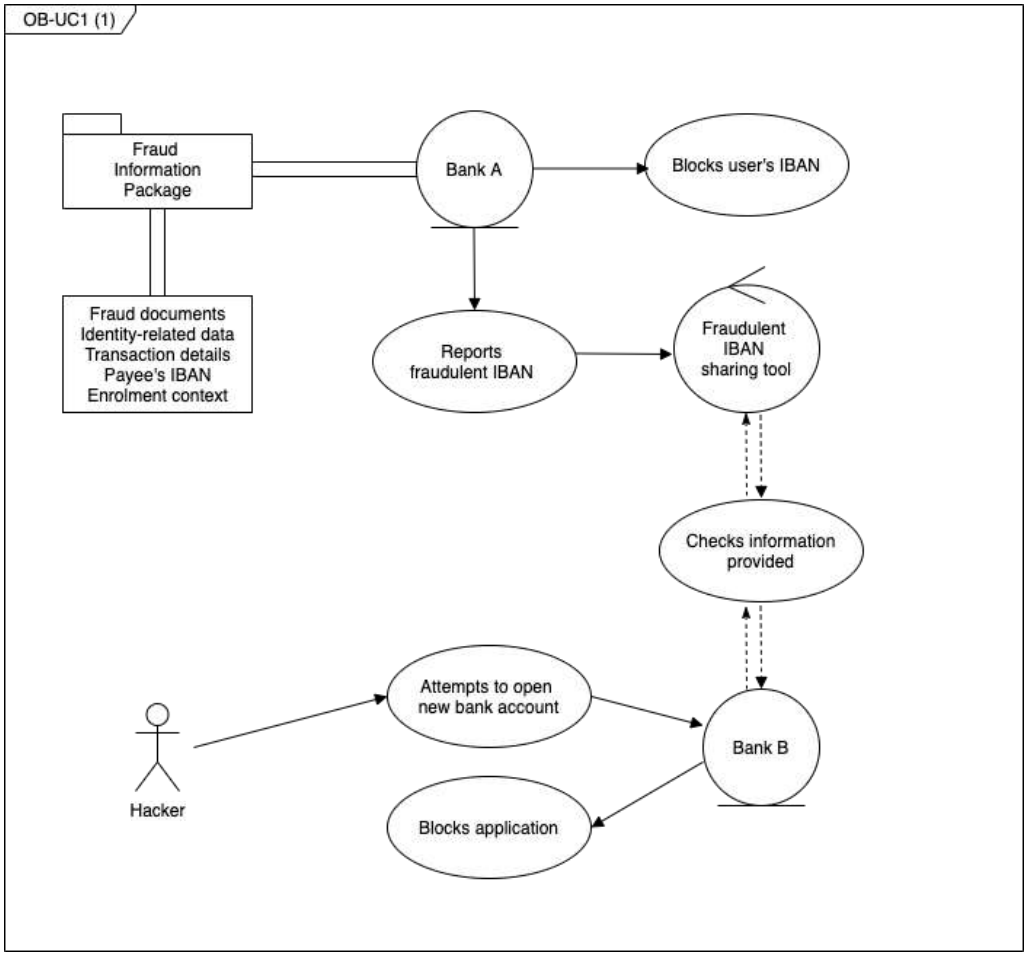

Figure 3: Open Banking - : A reported fraudster is blocked from carrying out further fraudulent transactions

Credit Renegotiation Broker Fraud

Step 1: A fraudster offers to renegotiate a user's existing credit or loan agreement offering a better rate. The user finds this is attractive and provides the fraudster with the verified identity data required to set up a new loan agreement with a second credit company.

Step 2: The fraudster takes out the new loan arrangement with the user's valid identity data. The credit company transfers the loan amount to the user, which the fraudster requests is transferred to him to pay off the old loan.

[9] Agence Nationale des Titres Securises, https://ants.gouv.fr/

Step 3: The user eventually discovers that the fraudster hadn't used the money transferred to him from the new loan to pay off the old loan and now has two loans to pay off (see Figure 4).

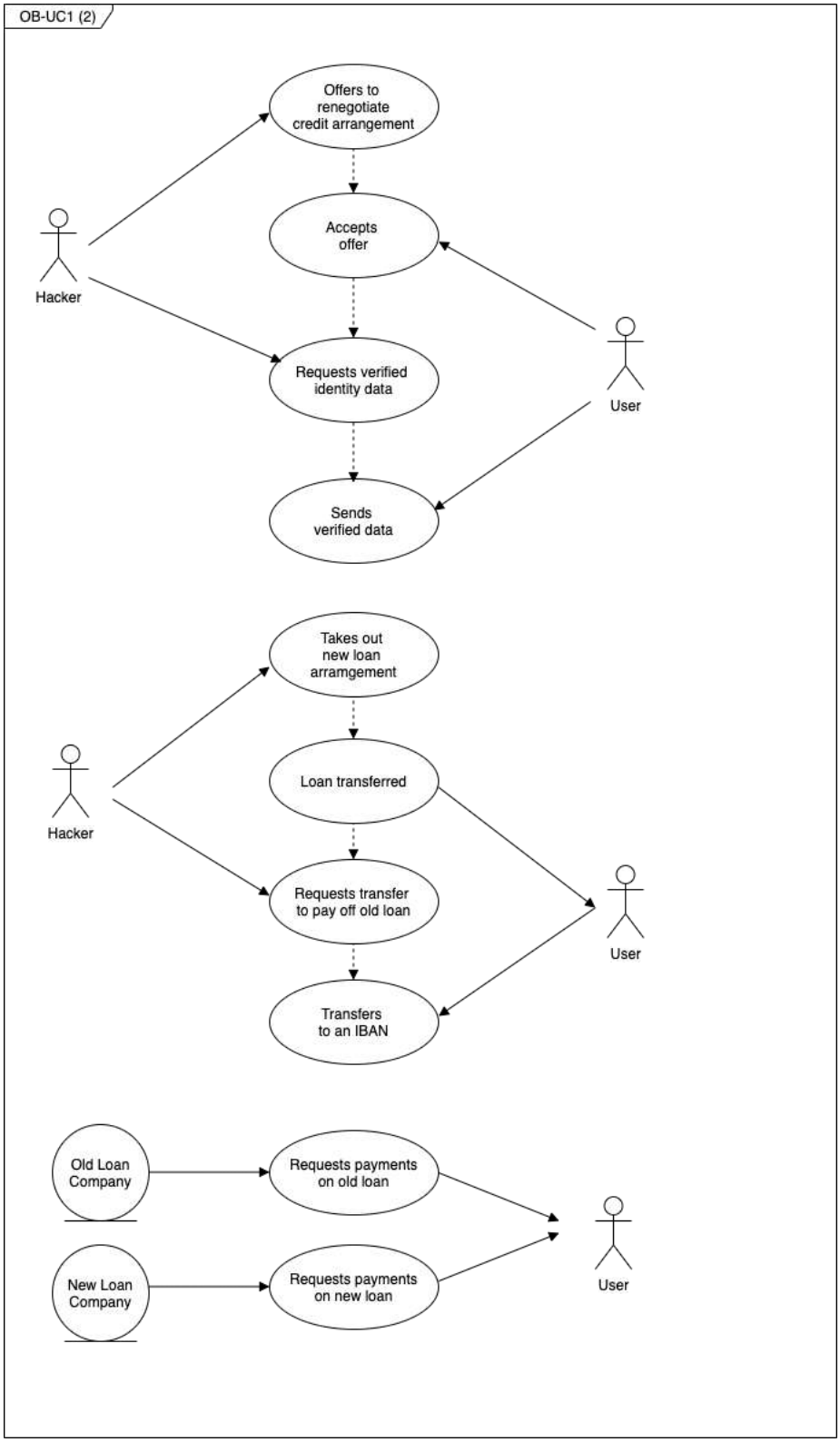

Figure 4: Open Banking - The credit renegotiation scam

2.1.1.5 Postconditions

As a result of intercepting the actual frauds or attempted frauds, fraudsters can be apprehended by the authorities. Acknowledging that if the attempted frauds are undertaken online, it may be difficult to arrest a fraudster. But at the very least, banks can protect themselves against identifiable fraudsters attempting to enter into fraudulent relationships and committing fraud.

2.1.2 Use Case OB-UC4: Open Banking API Architecture

This use case involves six different scenarios involving a hacker or a malicious user who tries:

1. to gain illegal access to the system;
2. to tamper with the data;
3. to gain unauthorized access to information;
4. to access customer data through API vulnerabilities;
5. to access customer data by injecting code into a client-side application;
6. to compromise a service with access to an internal API.

2.1.2.1 Stakeholders

The scenario described is plausible for all European banks and third-party service providers that have an economic interest in the network architecture. In particular, banks are able to easily connect other APIs in the market in order to extend their service offerings by introducing native plug-and-play FinTech solutions. Through embracing the Open Banking API economy, banks are able to further enhance and transform current offerings – increasing their appeal to existing and prospective customers alike.

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

2.1.2.2 Actors

The main actors are hackers or malicious users. Other actors are all the entities that interact with the Open Banking API Architecture ecosystem which can be of two types:

(i) **Primary actors** have goals which this demonstration use case fulfils

- Banks
- Service providers
- Hackers / Malicious attackers

(ii) **Secondary actors** don't have specific goals associated with this demonstration use case, but are involved in its execution

- ICT providers;
- End users (bank customers / Open Banking service users);
- Open Banking pure players (e.g. Fintechs that provide Open Banking platforms).

2.1.2.3 Preconditions

The use case anticipates the deployment of an Open Banking platform as represented in Figure 1. Particular attention must be paid to the minimum security requirements that must be considered when designing an Open Banking platform.

Normally, the most complex attacks involve the exploitation of different vulnerabilities on the same target and those related to the Open Banking architecture.

The application of the examined scenarios highlights the need to apply adequate countermeasures to all existing vulnerabilities, which are identified in the form of requirements applicable to the Open Banking platform.

PSD2 requires each financial institution to make its platform available to third parties. Thus, it is suggested to put in place an assessment to evaluate the effective neutralisation of the listed vulnerabilities which might be implemented through the following steps:

1. Regularly evolve the platform architecture using API technology;
2. Periodically assess and verify potential vulnerabilities;
3. Implement the platform requirements based on evidence from (2).
4. Check whether or not the fraudsters actually have the wherewithal to exploit any of the revealed vulnerabilities.

2.1.2.4 Basic Flow

2.1.2.4.1 Illegal access to the system

A hacker finds a JSON web token vulnerability to access the bank system through the use of spoofing and steals information from a bank customer:

1. Hacker uses the vulnerability to create a new authentication token;
2. Bank system accepts authentication token;
3. Hacker creates a MITM (man-in-the-middle) connection;
4. Hacker extracts information from the bank customer.

Alternate Flow
Malicious user finds a JSON web token vulnerability to access the bank system through the use of spoofing:

1. Hacker uses the vulnerability to create a new authentication token;
2. Bank system accepts authentication token;
3. Hacker changes functionalities of the bank.

This scenario is described in Figure 5, Figure 6, and Figure 7.

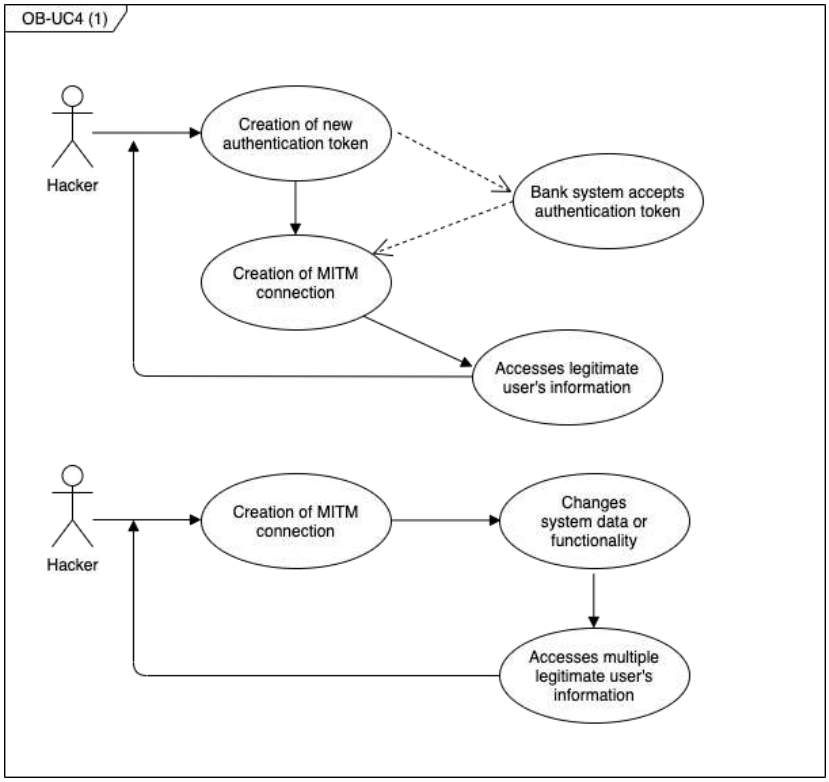

Figure 5: Open Banking - A spoofing attack and the implications for legitimate users

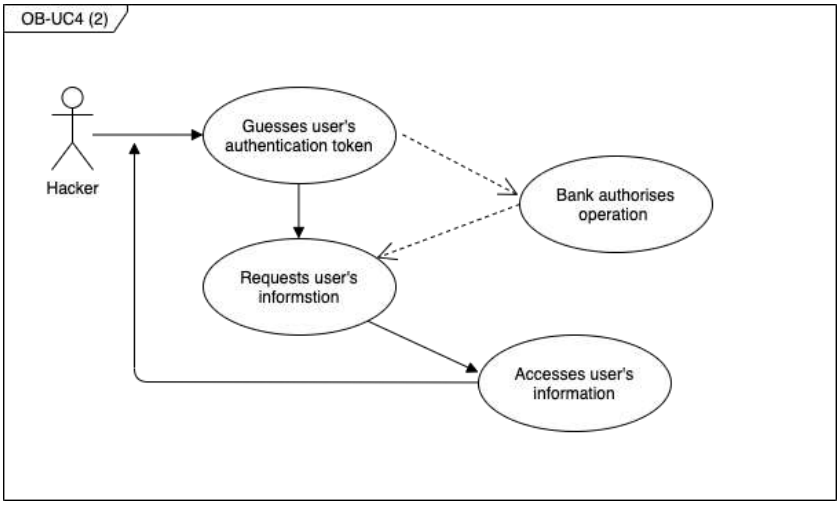

Figure 6: Open Banking - An undetected spoofing attack

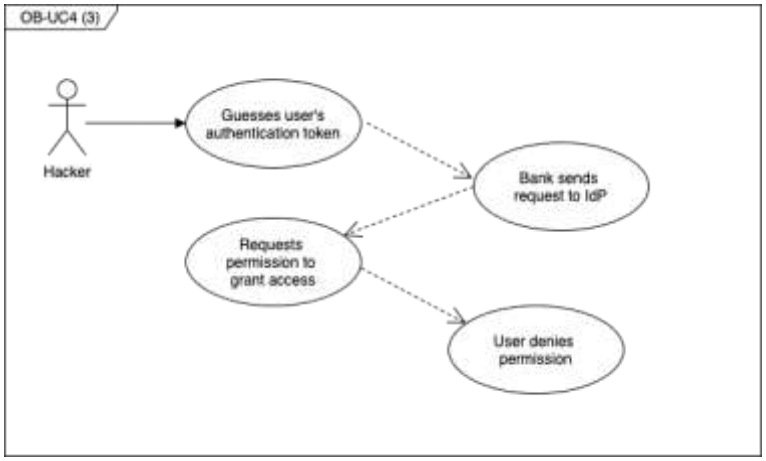

Figure 7: Open Banking - : A prevented spoofing attack

2.1.2.4.2 Unauthorised information change

A hacker finds an XSS[10] vulnerability to tamper with the bank system (see Figure 8 and Figure 9):

1. Hacker uses the vulnerability to access the bank system;
2. Hacker tampers with the bank system;
3. Hacker creates a new API function;
4. Bank customer connects and uses new API function;
5. Hacker changes information in the bank system.

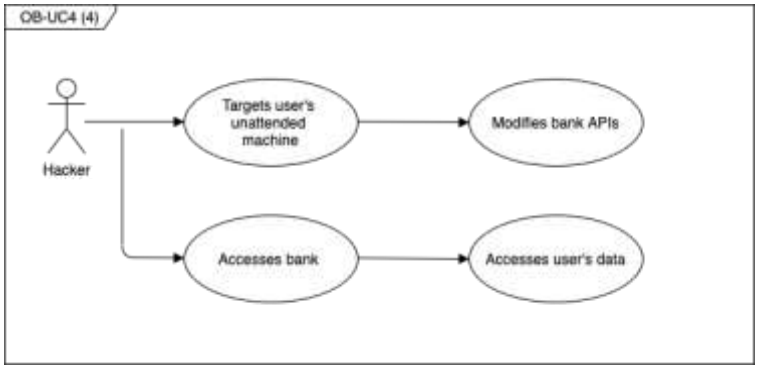

Figure 8: Open Banking - An undetected tampering attack

[10] **Cross-Site Scripting (XSS) attacks** are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. **XSS attacks** occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

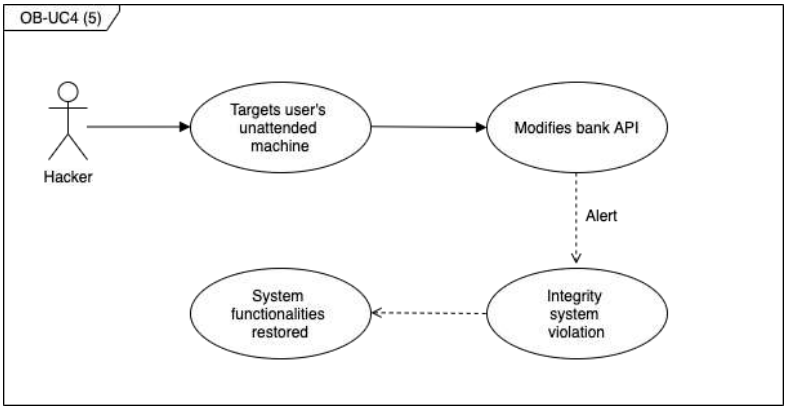

Figure 9: Open Banking - A prevented tampering attack

2.1.2.4.3 Unauthorised escalation of privilege

A hacker finds an OS vulnerability to elevate privileges in the bank system (see Figure 10 and Figure 11):

1. Hacker uses the vulnerability to access the bank system;
2. Hacker tampers with the bank system;
3. Hacker accesses an unauthorised functionality of the bank system;
4. Hacker finds a new vulnerability to accomplish privilege escalation.

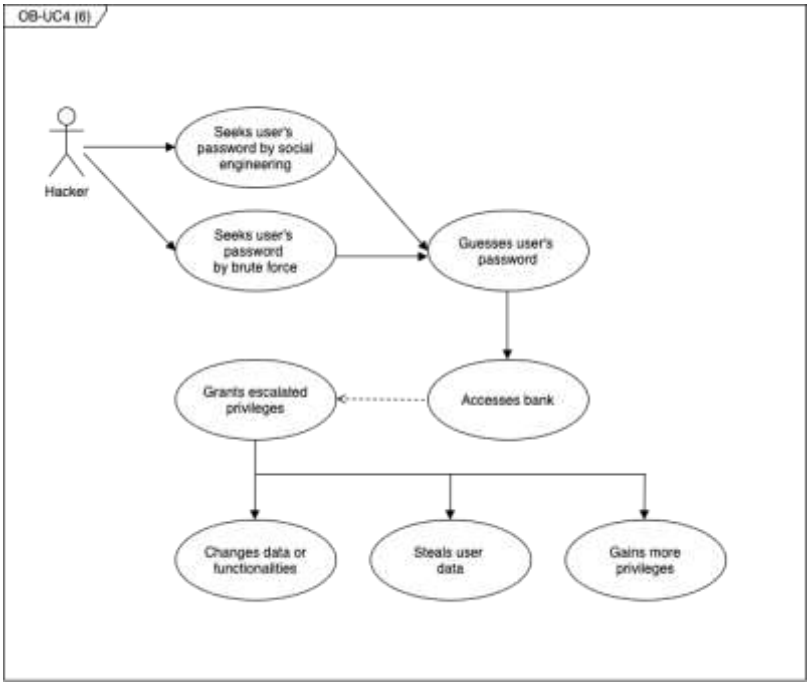

Figure 10: Open Banking - An undetected privilege escalation

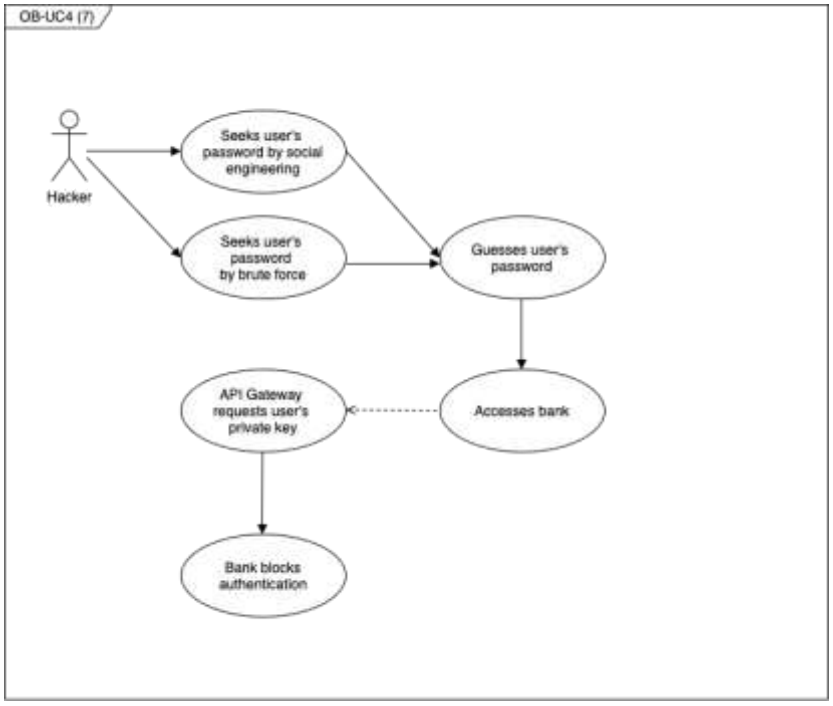

Figure 11: Open Banking - A prevented privilege escalation

2.1.2.4.4 Data leak

An attacker finds a vulnerability in an API method. A very common example[11] is the ability to access the data of others' customers (see Figure 12):

1. Attacker is authenticated with customer account;
2. Attacker searches vulnerabilities in API method;
3. Attacker tests the vulnerability and build an exploit;
4. Attacker exploits the vulnerability from his own device.

[11] API Security Top 10 2019 – TOP 1: Broken Object Level Authorization https://github.com/OWASP/API-Security/raw/master/2019/en/dist/owasp-api-security-top-10.pdf

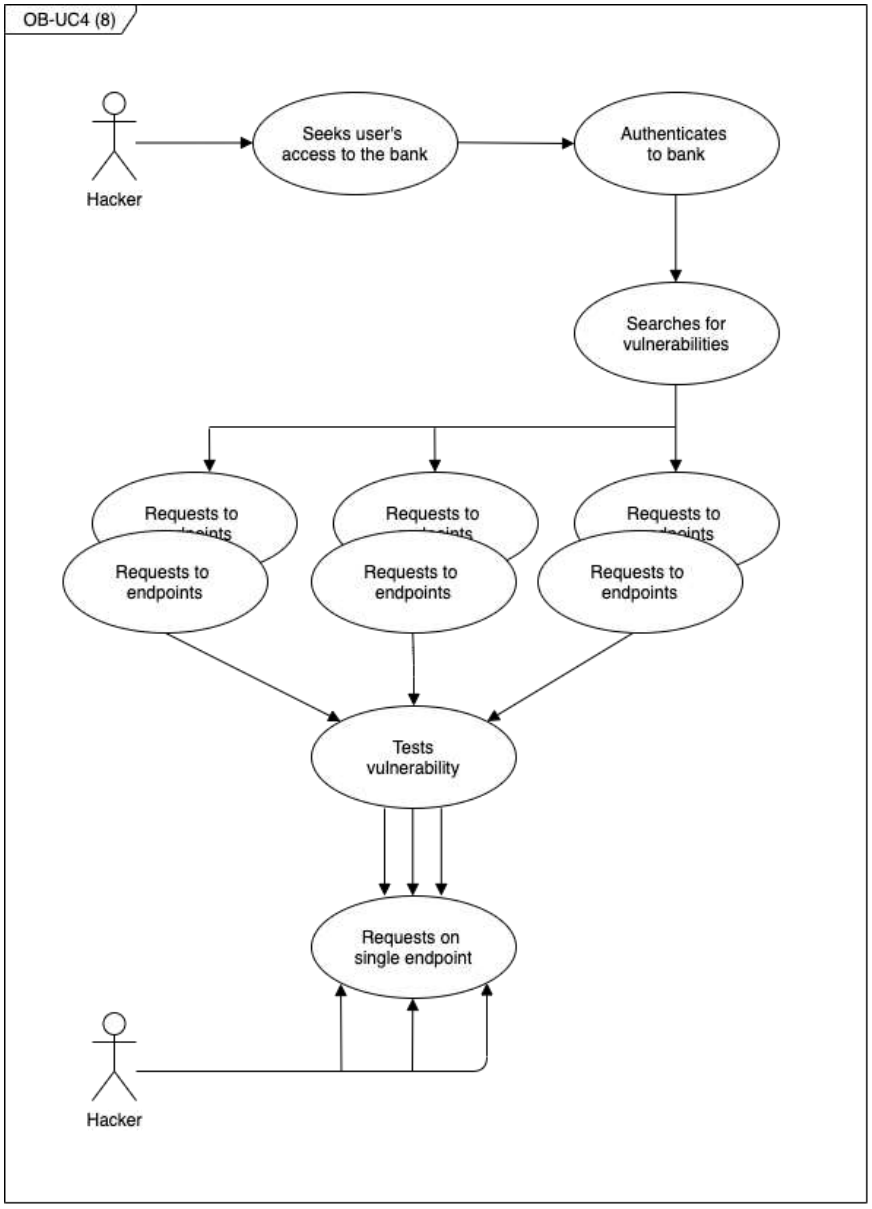

Figure 12: Open Banking - Attacker targets multiple endpoints to develop an exploitation strategy

2.1.2.4.5 Massive data leak through HTTP client

A hacker finds a way to inject code into the client-side app such as a banking web application or PSD2 TPP (third party library[12], XSS[13], etc.) (see Figure 13).

1. User is authenticated;
2. Attacker uses the vulnerability to inject code;
3. Attacker's code gets the personal and banking data;
4. Attacker's code sends the data to hacker's server.

[12] David Gilbertson : I'm harvesting credit card numbers and passwords from your site. Here's how. https://medium.com/hacker-noon/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5

[13] How Hackers Slipped by British Airways' Defenses. https://www.wired.com/story/british-airways-hack-details/

Variant:

1. User is authenticated;
2. Attacker uses the vulnerability to inject code;
3. Attacker's code sends the API access token to attacker's server;
4. Attacker requests the API.

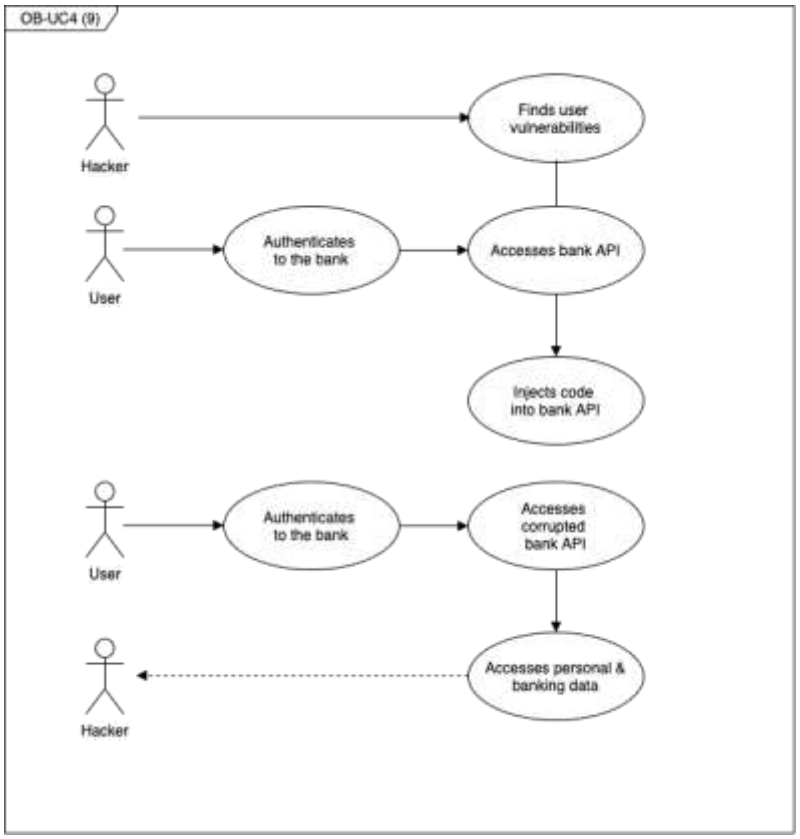

Figure 13: Open Banking - Attacker finds a vulnerability to inject malicious code into API

2.1.2.4.6 Compromised service

A hacker compromises a service which has access to an internal API with a service account (see Figure 14):

1. Attacker compromises an external service: for example, an external API that has access to an internal API;
2. Attacker uses the internal access to the API to access the personal data of all the bank's customers;
3. Attacker extracts the data using the internal API.

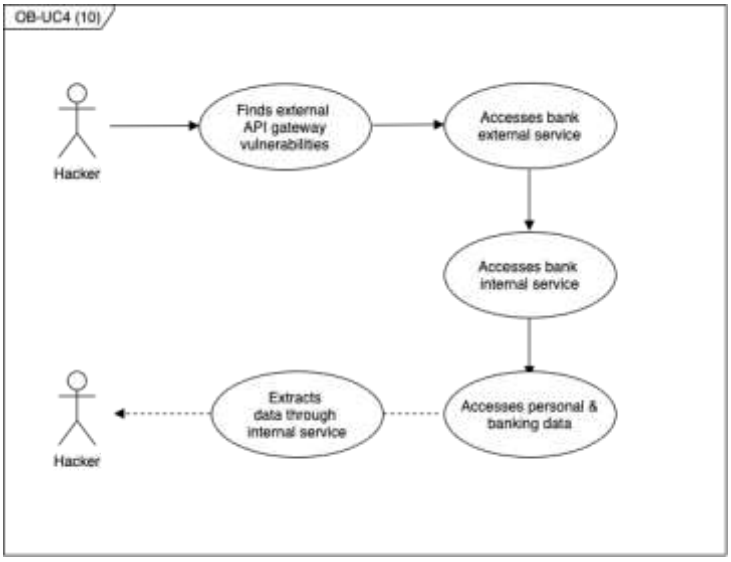

Figure 14: Open Banking - Attacker compromises a service through getting access to an internal API

2.1.2.5 Post Conditions

2.1.2.5.1 Illegal access to the system

Information in the bank system is changed after the execution of this scenario. In particular, the hacker has:

- added new authorised users to the system for creating a new attack pattern;
- injected in the API system new API functions to view and change information of legitimate users;
- changed the user interface of the API system or of the bank itself to create new forms to be used for a future phishing campaign.

2.1.2.5.2 Unauthorised information change

Information in the bank system is changed after the execution of this scenario. In particular, the hacker has:

- changed user information (e.g. name, surname, telephone numbers) for new and existing bank customers;
- changed the API system with new API functions to change information of legitimate users;
- added new API components to redirect function calls.

2.1.2.5.3 Unauthorised escalation of privilege

The hacker has new permissions in the system. With these new privileges the hacker has:

- changed the data or functionalities of bank system;
- stolen legitimate information data;
- gained new privileges to access new system functions (e.g. add / delete / edit bank users).

2.1.2.5.4 Data leak

The attacker has all the data exposed by the vulnerability.

2.1.2.5.5 Massive data leak through HTTP client

The attacker has the data exposed by the APIs for all customers who executed the code in their browser.

2.1.2.5.6 Compromised service

The attacker has the data exposed by the internal API to the external service (API) through which the data was exposed.

2.2 Demonstrator Set-up

2.2.1 Use Case OB-UC1: Sharing of Identity Verification and Fraudulent Activity

For both use case OB-UC1 (Sharing of Identity Verification and Fraudulent Activity) scenarios, we present the demonstrator first from the perspectives of the primary actors and then those of the secondary actors, showing and explaining the respective user interfaces and interaction flows.

2.2.1.1 Relation to Use Cases

While the demonstrator is based on OB-UC1 (Sharing of Identity Verification and Fraudulent Activity)[14], it also leverages OB-UC2 (OBSIDIAN - Open Banking Sensitive Data Sharing Network for Europe)[15] and OB-UC3 (Privacy Preserving Verifiable Credentials)[16].

2.2.1.2 Relation to WP3 Assets

The 'Scalable and Private Permissioned Blockchain' asset[17], the permissioned blockchain platform of choice to implement CyberSec4Europe architecture's blockchain services, is integrated into this demonstrator.

The 'Verifiable credential user-centric identity management (VCUCIM)' asset is integrated into this demonstrator[18].

2.2.1.3 Description and Workflow

Means of Payment Fraud

User View #1 – Successful Fraud

The demonstrator opens with a user (the customer) sitting at a workstation making an application to open a bank account. She is asked for proof of identity and a utility bill or any other proof of address and provides documents that we are informed are not genuine. The bank accepts her credentials and acknowledges her

[14] See *D5.1 Requirements Analysis of Demonstration Cases Phase1*, Section 3.4.3 et passim
[15] See *D5.1 Requirements Analysis of Demonstration Cases Phase1*, Section 3.4.4 et passim
[16] See *D5.1 Requirements Analysis of Demonstration Cases Phase1*, Section 3.4.5 et passim
[17] See *D3.2 Cross Sectoral Cybersecurity Building Blocks*, Section 9.2, pp.38-39
[18] See *D3.1 Common Framework Handbook 1*, Section 5.4, p.33

request and issues her with an IBAN. Once the user receives acceptance of her request, she is asked to deposit a minimum of 10 € into the new account.

She then makes a request for Gold status which provides high overdraft facilities, access to online transfer service and other high value benefits. The bank requests proof of income and she sends a false contract of employment and falsified payslips and/or falsified or stolen bank statements and/or falsified or stolen tax notices. Once satisfied, the bank provides her with the Gold facility.

Externally (by video), the user is seen approaching an ATM and withdrawing cash and then entering several retail sites and making purchases using her Gold credit card and/or bank cheques. Both instances require the use of the newly created IBAN.

Back at her workstation, the user makes several money transfers as possible.

The user is then seen opening in parallel several other accounts with other banks and going through the same procedure as above with either the same or a slightly different set of false or stolen documents.

This scenario is described in Figure 15.

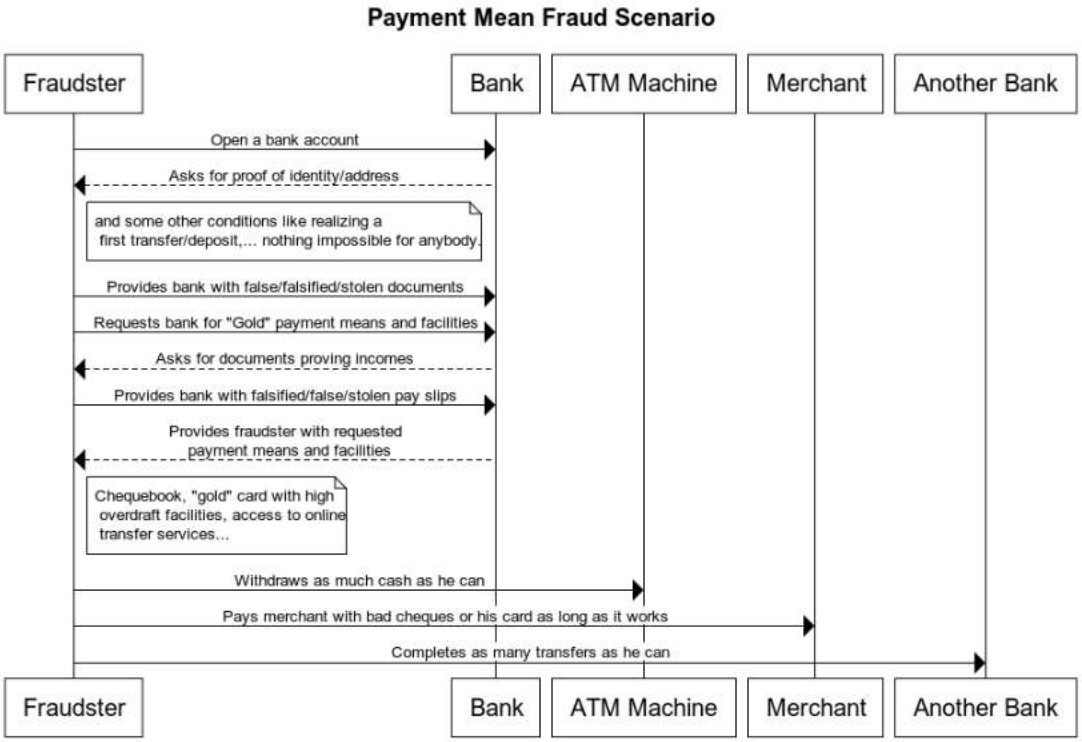

Figure 15: Open Banking - Payment fraud scenario's timeline

Behind the Scenes View #1

- **Monitoring and Logging**

  (1) A fraud expert at Bank J receives a notification that a fraud has taken place involving a new IBAN and/or a set of documents and registers information about the IBAN and/or these documents into its own monitoring database;

(2) Then he publishes this new IBAN information on to the OBSIDIAN network, whatever the architecture is based on whether it's MISP[19] or a blockchain-based technology (see Figure 16);

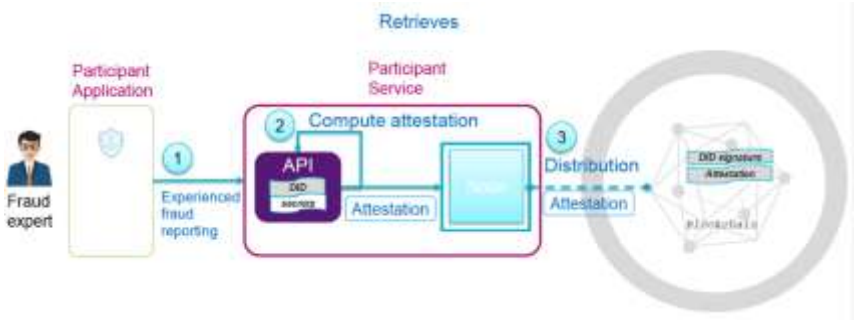

Figure 16: Open Banking - Monitoring and reporting a fraud report

(3) This way, the other participating banks and financial institutions will be notified about this fraudulent IBAN and/or the risk associated with the use of this set of documents, for when they request the OBSIDIAN network to check IBANs or documents implied in the transactions and interactions with their customers (see Figure 17).

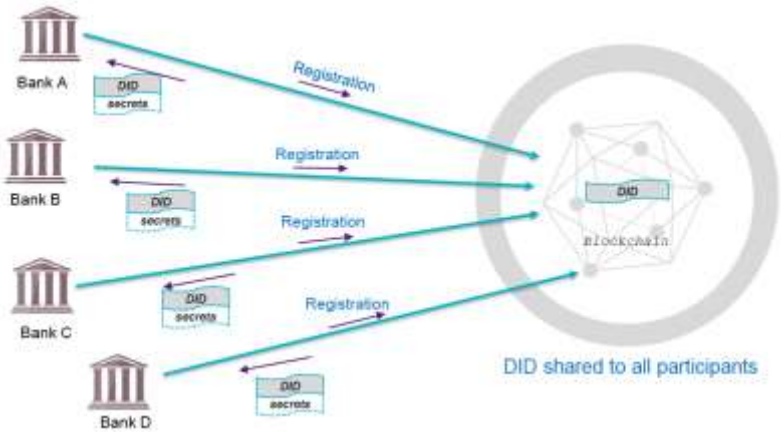

Figure 17: Open Banking - Sharing payment fraud information

- **Fraud Prevention**

(4) A fraud expert sees that a customer at Bank K is trying to add the new IBAN as a beneficiary on his bank account;

(5) Bank K uses the OBSIDIAN API based on the PSI protocol to confirm whether or not this IBAN is fraudulent and to get additional information about the operating mode of the owner of the IBAN;

[19] Malware Information Sharing Platform

(6) Bank K is quickly able to assess that the IBAN is fraudulent and is able to make the good decision that prevents a further fraud (see Figure 18).

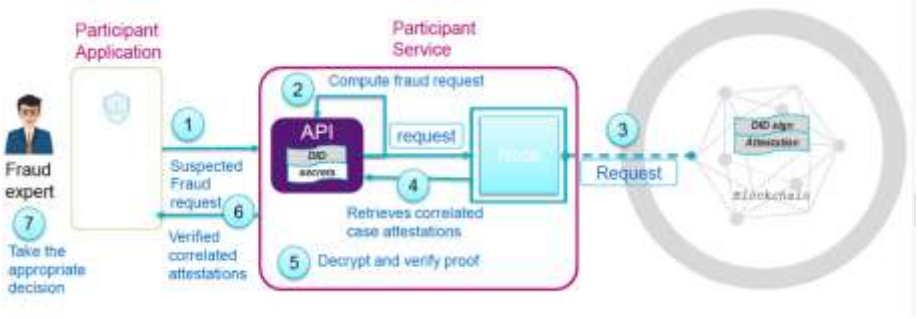

Figure 18: Open Banking – Verifying a suspected fraudulent request

User View #2 – Unsuccessful Fraud

The following two user views demonstrate how the fraud attack described above can be prevented by the use of verifiable credentials and KYC sharing.

- **Onboarding with Verifiable Credentials**

  A. The first user sits at a workstation making an application to open a bank account. She is asked to present her verifiable credentials.

  Verifiable credentials are the electronic equivalent of the physical credentials we have today such as plastic cards, passports, tickets, qualifications etc. Verifiable credentials are cryptographically protected and signed and are stored in end users' devices such as mobile phones, laptops etc allowing users to carry them around with zero portability effort.

  The user submits credentials which can be verified by the bank, and she is invited to open her account.

  B. The second user sits at a workstation making an application to open a bank account. She is asked to present her verifiable credentials.

  The user submits credentials which are fraudulent being either stolen or forged. As they cannot be correctly verified by the bank because the certification authority process fails, the transaction proceeds no further.

- **Onboarding with Shared KYC**

  A. The first user sits at a workstation making an application to open a bank account. She is asked to present her ID.

  The bank accesses the KYC sharing network to match the user's credentials. The KYC sharing network returns a positive corroboration of the user's ID and the bank offers to onboard the user with confidence.

  B. The second user sits at a workstation making an application to open a bank account. She is asked to present her ID.

  The bank accesses the KYC sharing network to match the user's credentials. The KYC sharing network returns some similarities with an experienced fraudster. Consequently, the bank is not prepared to onboard the user without having a face-to-face meeting which the bank suggests to the client.

Credit Renegotiation Broker Fraud

User View #1 – Successful Fraud

The user is contacted by a credit broker (the fraudster) who offers to renegotiate a credit arrangement the user has at a more attractive rate than the user has at present. The user accepts the offer.

The fraudster requests identity data from the user that includes a copy of a passport page or ID card, proof of address and the credit agreement documentation. The user complies and sends the requested documents.

The fraudster then takes out a new loan arrangement with a credit company in the name of the user for an amount equivalent to the amount of the old credit. The credit company transfers the requested amount to the user's bank.

The fraudster asks the user to transfer the credit amount to an IBAN provided by the fraudster in order to repay the old credit. The user transfers the credit amount to the fraudster.

After some time, the user realises that the old credit arrangement is still operative but that there is now in addition a new credit arrangement. In other words, the user owes twice as much as he did before.

The user seeks reimbursement from the bank.

User View #2 – Unsuccessful Fraud

The user is contacted by a credit broker (the fraudster) who offers to renegotiate a credit arrangement the user has at a more attractive rate than the user has at present. The user accepts the offer.

The fraudster requests identity data from the user that includes a copy of a passport page or ID card, proof of address and the credit agreement documentation. The user complies and sends the requested documents.

The fraudster then takes out a new loan arrangement with a credit company in the name of the user for an amount equivalent to the amount of the old credit. The credit company transfers the requested amount to the user's bank.

The fraudster then tries to take out a new loan arrangement with a credit company in the name of the user for an amount equivalent to the amount of the old credit. But the credit company is able to detect the fraudulent use of the set of documents provided by making a request to the OBSIDIAN network and consequently not proceeding any further with the transfer.

2.2.1.4 Target Groups

The following target groups would be interested in use case OB-UC1:

- **Banks** and **other financial institutions** would be the primary beneficiaries of the results of this use case and would be encouraged to participate in future use case activities;
- The **French Banking Federation (FBF)** and the Italian banking network **(On-line Fraud Cyber Centre and Expert Network (OF2CEN))**;
- **European Payments Council (EPC)** has expressed the desire to move from an unstructured method to a structured and automatic one for information exchanged for anti-fraud purposes, including the identity of the defrauder. For this ambitious goal, it has launched an international working group, of which CERTFin is leader[20], which proposes to discuss and define the format, protocol and tools to be used. Among the tools proposed is MISP;

[20] Since 1 January 2017, ABI Lab has managed the operational activities of the Italian Financial CERT (CERTFin), a cooperative public-private initiative governed by the Italian Banking Association (ABI) and Bank of Italy, aimed at increasing the cyber resilience of the Italian financial system through an operational and strategic support for prevention,

- **The Observatory for the Security of Means of Payment[21] (OSMP)**, created in 2016 by the Banque de France, is a body intended to promote the exchange of information and consultation between all the parties concerned (consumers, merchants and businesses, public authorities and administrations, banks and managers of means of payment) by the proper functioning of means of payment and the fight against fraud. As such, the OSMP takes over all the missions previously devolved to the Payment Card Security Observatory created in 2001, which it succeeds, on a scope extended to all cashless means of payment;
- **Certification Bodies** would be interested in how the demonstrator shows how they can easily interact in a distributed workflow example, including the benefits of distributed, cross-organisational collaboration and the possibility to keep the audit trail in a distributed ledger.

2.2.2 Use Case OB-UC4: Open Banking API Architecture

In this demonstrator we show how the OBA platform can overcome the security issues associated with *unauthorized user*, *unauthorized access, unauthorized use*, *man-in-the-middle-attack*, *UI misuse*, *privilege escalation, integrity/confidentiality compromise and API misuse*. We provide six scenarios in which the attacker is first able to get access to a bank's system or exploit some vulnerabilities against an OBA platform uncompliant with security requirements; and then show how the attacker can be blocked by the application of appropriate countermeasures.

2.2.2.1 Relation to Use Cases

The only use case in relation to this use case demonstrator is OB-UC4[22].

2.2.2.2 Relation to WP3 Assets

The demonstrator does not integrate any of the assets from WP3.

2.2.2.3 Description and Workflow

2.2.2.3.1 Illegal access to the system

This describes the possible situation related to an attacker performing a *spoofing attack.* In this type of attack the attacker impersonates another user or device on a network in order to perform malicious activities: for example, to steal data. The primary victims of the attacker in this scenario are banks and users, although technology vendors and service providers are also impacted.

As seen from the perspective of the attacker, the attacker obtains an authentication token to bypass the bank authentication system. When the system allows the attacker access, he performs a *man-in-the-middle attack* (MITM) which results in the theft of the user's data information from the bank.

Looking at a variation of this situation from the perspective of the hacker and the user, the hacker tricks a user into clicking on something different or compiling a form which reveals confidential information.

Finally, the attacker accesses the system directly and changes some of the functionalities of the system.

preparation and response to cyber attacks and security incidents and acting as a national ISAC (information sharing and analysis centre) for the banking sector

[21] Observatoire de la securite des moyens de paiement - https://www.banque-france.fr/stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement

[22] See *D5.1 Requirements Analysis of Demonstration Cases Phase1*, Section 3.4.6 et passim

Open Banking platform* without *OAuth security

Here the actions related to an attacker performing a spoofing attack: the attacker guesses the token used by the bank to authenticate a user.

In this scenario the OBA doesn't satisfy the security requirements. The bank provides a REST API developed for the backend adopting a very poor token-based authentication system which allows third parties to easily bypass such controls and extract data or perform unauthorised operation.

The vulnerability is intrinsic to the generation of the token. The attacker is able to obtain the token by performing simple statistical predictions about possible future values. Together with the lack of an expiring time of the token and the missed permission of the user, the attacker can deceive the bank's authentication system.

At this point the attacker uses the guessed token to the bank which authenticates the malicious user enabling a legitimate session.

The attacker uses the APIs provided to retrieve information about the user or worse still perform unauthorised payments.

The actors actively involved are the attacker and the bank. The victims are the bank itself and the user who is unaware of the data or money theft.

Open Banking platform* with *OAuth security

Here the attacker cannot perform a *spoofing attack* by guessing the token.

The scenario is the same as the previous one, but now the OBA platform satisfies the security requirements. The authentication task is performed by the identity provider component (IdP). The authentication is implemented through OAuth.

In this case the bank exploits the OAuth authentication mechanism which basically requires the user's permission to allow a third party to call the bank's REST APIs. The user denies permission so that the attacker cannot cheat the bank's authentication system.

As before the attacker is able to guess the token generated by the system, exploiting a bad design choice. Then the attacker sends the token to the bank's authentication system. At this point the IdP component must send a request to the real user who the attacker is seeking to impersonate. The real user doesn't give her permission to the bank. The main reason for the denial of the user's permission is that she has not actually requested performing such an operation. So, the bank doesn't permit the attacker to call the APIs.

In conclusion the adoption of safety requirements allows the bank to block the attacker. The new authentication mechanism removes the security issue of the *unauthorised access* by performing a direct request to the real user.

2.2.2.3.2 Unauthorised information change

Figure 19 provides an overview about the possible real cases related to an attacker performing a *tampering attack.* In this type of attack the attacker changes or deletes a resource without authorisation. If the attacker is able to tamper with it, there can be some consequences on the usage of the system itself, such as the attacker being able to add or remove some functional elements. The victims of the attacker in this scenario are the bank, the user and the service providers.

In the scenario the attacker is able to access the bank system and compromise it.

The attacker modifies or creates new API functions that will be used to perform malicious activities.

The attacker's goal is to make the user use the malicious APIs. As a consequence, when the user invokes the

crafted APIs, the system could suffer two types of compromises: *integrity compromise* and *confidentiality compromise.*

Integrity compromise implies that the attacker is able to change functionality data so that the system is transformed to work in a manner differently to the way in which the service was designed. *Confidentiality compromise* implies that the attacker is able to access data that he is not authorised to view.

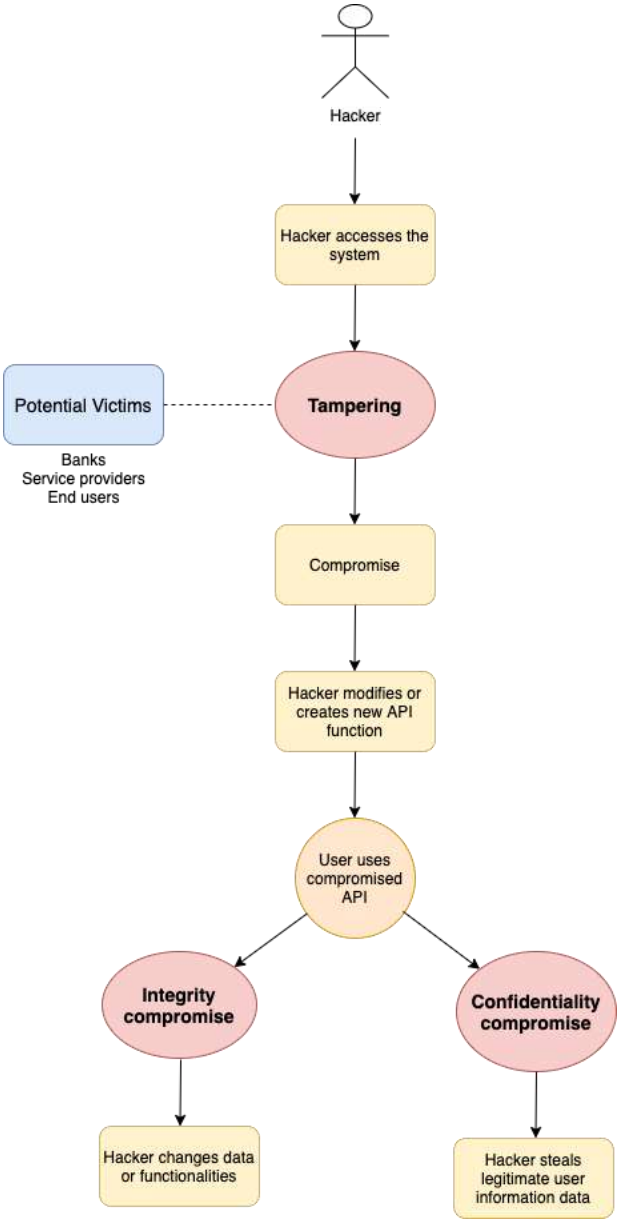

Figure 19: Open Banking - A tampering attack and its consequences for the victims

Open Banking platform* without *API's validation security requirement

This shows the actions related to an attacker performing a *tampering attack*, whereby the attacker is able to get access to an unattended machine.

The OBA in this scenario doesn't satisfy the security requirements. The bank provides a REST API developed for the backend without an integrity checker to monitor unauthorised API changes. It would allow an attacker to modify the API in order to steal legitimate user data or change the normal system functionalities.

The attacker could exploit a victim that leaves her machine unattended and then proceed to tamper with the system. Therefore, the hacker modifies the bank APIs in order to be able to access the user's data.

At this point the user invokes the malicious APIs to perform her operations. The unsuspecting user doesn't know that the attacker can now view her data in an unauthorised manner.

The actors actively involved are the attacker, the bank and the user. The victim is the user who is unaware that she has had her data stolen. The bank too is a victim of such an attack**.** The bank system is compromised and is causing harm to other users.

Open Banking platform* with *API's validation security requirement

This shows how the attacker cannot compromise the system without being detected by the system.

The scenario is the same as the previous one, but now the OBA platform satisfies the security requirements. An integrity check is performed by the *API Manager* which provides controls to prevent integrity compromises. The check is performed through hashing techniques.

Let's see in detail as the attacker is blocked. As before the attacker is able to make changes to the bank APIs, exploiting bad practice. Then the attacker replaces the legitimate API with a malicious one. The *API Manager* raises an alert because it detects an unauthorised change in the system, at which point the system administrators can restore the proper system functionalities.

In conclusion, the adoption of safety requirements allows the bank to block the attacker. The integrity check mechanism raises alerts whenever the system is compromised.

2.2.2.3.3 Unauthorised escalation of privilege

Figure 20 provides an overview of the possible real cases related to an attacker exploiting a vulnerability to perform a privilege escalation. Privilege escalation is frequently used in preparation for a more specific attack, allowing intruders to deploy a malicious payload or execute malicious code in the targeted system. However, the attacker could simply extract data or change the functionalities of the system. Potential victims of the attackers in this scenario are banks, service providers and Fintechs.

The attacker accesses the bank system and is able to make changes to data or system functionality through an unauthorised use of privileges.

The attacker is then in a position to steal legitimate user data. And in addition, the attacker is able to grant himself more privileges to do even more damage.

The actors actively involved are the attacker and the bank.

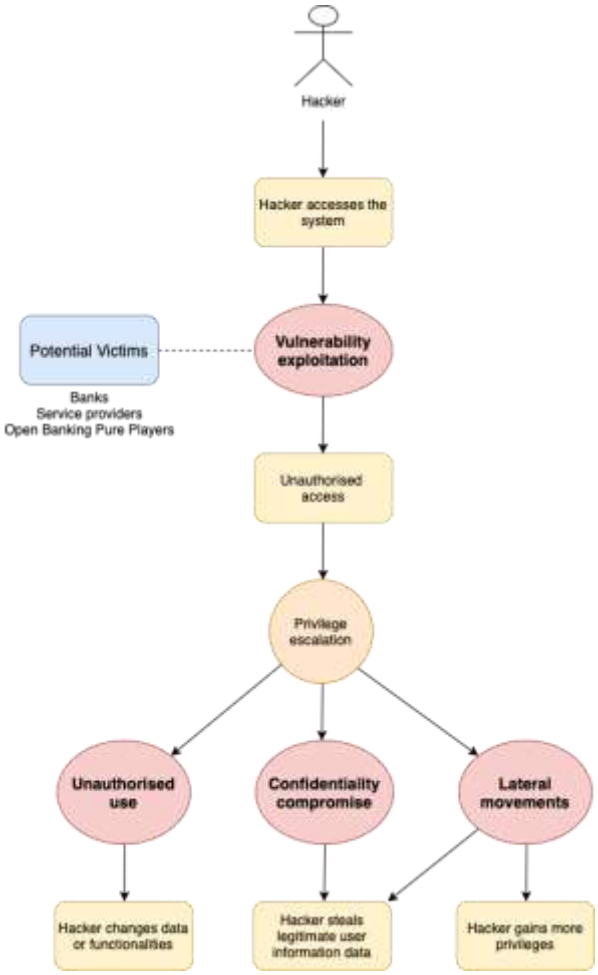

Figure 20: Open Banking - Schema representing an attacker exploiting a vulnerability to realize a privilege escalation with the relative consequences for the victims

Open Banking platform* without *key based authorisation security

This shows the actions related to an attacker exploiting a vulnerability of a bank system to perform a *privilege escalation*.

The OBA doesn't satisfy the security requirements by having banks allow its customers perform operations after authenticating with username and password, thus letting attackers easily guess the customer passwords in different ways.

The vulnerability lies in the password chosen by the user. The attacker is able to obtain it through social engineering techniques or brute force attacks.

Once the attacker has guessed the user's password, it is easy for him to perform malicious activities.

The actors actively involved are the attacker and the bank. The victims are the banks and the service providers.

Open Banking platform* with *key-based authorisation security

This shows the attacker cannot perform *privilege escalation* by guessing the user password.

The scenario is the same as the previous one, but now the OBA platform satisfies the security requirements. The *API Gateway* component provides controls to ensure that unauthorised flows cannot occur, realised

through *key-based authorisation*.

As before the attacker is able to exploit a system vulnerability to access the system.

The attacker finds out the user credentials but, when attempting to access the system, is blocked when the *API Gateway* requests the user's private key to authenticate.

The adoption of the appropriate security requirements allows the bank to block the attacker. *Key-based authorisation* overcomes the *unauthorised access* security issue.

2.2.2.3.4 Data leak

An attacker finds a vulnerability in an API method. A very common example is the ability to access the data of other customers. This scenario is taken from the perspective of the attacker.

We see the attacker authenticating with a user's account credentials, which allows him to search vulnerabilities in the API system.

Having found a suitable vulnerability, the attacker is seen to test it and develop an exploitation approach. Once confident of success, the attacker then uses the vulnerability from his own device to bombard the bank's system with data (and other) requests.

2.2.2.3.5 Massive data leak through HTTP client

A hacker finds a way to inject code into the client-side app such as a banking web application or PSD2 TPP (third party library, XSS, etc.). Again, the scenario is taken from the viewpoint of the hacker.

The attacker sees that the user has successfully authenticated to the bank and uses a vulnerability he has previously discovered to inject code into the user's application. Unbeknownst to the user, the next time the user authenticates to the bank it contains the attacker's inserted code which makes a call to the bank's API to send data. The API response is to send the requested personal and banking data to the attacker's server. The user has unwittingly assisted the attacker in deceiving the bank and stealing the user's data.

A variation on this scenario has the attacker inject code into the user's application and requests the API to send an access token to the attacker's server, so that the attacker is now in a position to directly interrogate the API.

2.2.2.3.6 Compromised service

In this scenario, a hacker compromises a service which has access to an internal API with a service account. We again watch from the attacker's viewpoint.

The hacker is able to compromise an external service, such as an external API gateway that provides him with access to one of the bank's internal API. With this access, we then see the hacker make requests to the internal API to provide access to the personal data of all of the bank's customer data. Once the data is accessed, the attacker is able to download it to his own server.

2.2.2.4 Target Group

For the described demonstrators it is important to involve the following actors:

- **Banks** and **other financial institutions,** including **Fintechs,** would be the primary beneficiaries of the results of this use case and would be encouraged to participate in future use case activities;
- **Service providers** and **technology vendors**.

3 Supply Chain Security Assurance

This section provides an overview over the demonstration use cases for CyberSec4Europe titled *Supply Chain Security Assurance*. We introduce two individual use cases named *SHC-UC1 Supply Chain for Retail* and *SHC-UC2 Compliance and Accountability in Distributed Manufacturing*. The demonstrators will illustrate how the distributed ledger[23] technologies can be applied to enhance security and compliance of distributed workflows in supply chain and manufacturing processes.
This chapter is organised as follows: we will first give an overview over the two distinct use cases, presenting relevant interaction scenarios (flows) and describing their actors. The subsequent section will provide details on the demonstrator setup and the intended target groups.

3.1 Use Cases Specification

3.1.1 Use Case SCH-UC1: Supply Chain for Retail

This use case models the supply chain for the retail business. We especially focus on dispute resolution: two parties initiate a dispute whenever there is an inconsistency between an order of goods and the received shipment. Disputes management costs a considerable amount of time and money to a company. We argue that leveraging the blockchain to manage the supply chain's processes can bring considerable advantages to disputes management [1]. In what follows, we describe three examples which may cause a dispute.

Example 1. The simplest case we can think of when we think about disputes, is finding an error in the shipment or a delay in its delivery. In the former, the shipment might have an incorrect amount of goods, or damaged goods, or even the wrong type of goods. The recipient will raise a dispute to force the shipper to send another shipment that amends the mistake of the previous one. A delivery's delay may or may not be critical to the recipient's operation, though it causes great inconvenience. If the recipient is a healthcare facility, a delay might have serious consequences and might cost lives. The recipient may ask for a refund, depending on how much the delay affected its operations. In both cases, shipper and recipient lose time and money to straighten out the situation.

Example 2. Supply chains use trucks to deliver some of their shipments along the chain. Raising the truck drivers' wages can cause inconsistencies that lead to disputes. The problem is that companies will adjust (i.e., raise) the shipments' costs to reflect the change in the wages *without* notifying the shipments' recipients. The costs increase affects not only all future orders of goods, but those *already confirmed* as well; at shipment delivery, the recipient will be confronted with a higher due payment amount to the shipper. In such cases, the receiver will most likely initiate a dispute because of the discrepancy in due payment amounts (the one negotiated at order creation, and the one presented at shipment delivery). This happens because in current supply chain management systems there is poor data synchronization, therefore only the goods' shipper is aware of the price change.

Example 3. Suppose that a shipment, *Shipment A*, has to deliver a certain quantity of *Product A*, to a recipient, *Recipient A*. Now support that, while *Shipment A* is still in transit, possibly waiting for dispatch at one of the shipper's warehouses, the shipper accepts another order of *Product A* from another client, which we call *Recipient B*. This new order requests a smaller quantity of *Product A*, but is classified as "high priority" (e.g., *Recipient B* is a VIP customer). To satisfy its VIP customer, the shipper splits the ongoing *Shipment A* in two smaller shipments:

- *High priority shipment*: a delivery sent to *Recipient B*, containing the amount of *Product A* requested by her. We call this *Shipment B*.

[23] "A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. " [19]

- *Regular shipment*: A delivery sent to *Recipient A*, containing the amount of *Product A* left after subtracting from *Shipment A* the amount requested by *Recipient B*. We call this *Shipment C.*

Shipment B satisfies *Recipient B*'s needs. However, *Recipient A* will receive *Shipment C*, that is, a shipment with fewer items than those she paid for. The problem cannot be solved by the shipment's truck driver; it needs the involvement of the shipper. Therefore, *Recipient A* will initiate a dispute because of the sudden discrepancy in the number of items received.

These are only three examples of disputes in a supply chain. This use case presents a blockchain-based solution to solve disputes of any kind. In particular, this blockchain deploys a smart contract designed to streamline the dispute process. We call this smart contract "Dispute Smart Contract" (DSC).

3.1.1.1 Stakeholders

The following is a list of stakeholders potentially interested in the efficient resolution of disputes in the supply chain:

- Logistics services provider: companies (e.g., UPS, DHL, etc.) that move goods along the supply chain;
- Financial institution: processes payment transactions in the supply chain;
- Government agency: governmental entity that interacts with the flow of goods entering/leaving the country (e.g., customs office, food safety agencies, drug agencies, etc.). Disputes may cause new shipments and deliveries across a country's borders.

3.1.1.2 Actors

In what follows, we list the actors involved in the handling and resolution of a dispute involving a shipment between a warehouse and a store:

- Retailer: buy goods from warehouses.
- Warehouse: sell goods in bulks to retailers.

3.1.1.3 Preconditions

The use case assumes that there is an established supply chain that handles goods, from their creation from raw materials to their delivery to customers. The use case's actors have all an active role in the supply chain. Naturally, they might partake in multiple, independent supply chains, but this is not relevant for the use case.

In this use case, we consider a delivery of goods between a warehouse (sender) and a retailer (receiver), but the scenario we describe here may happen between any two parties along the supply chain (e.g., two warehouses, a manufacturer and a warehouse, etc.). The use case workflow starts after the detection of an anomaly in a delivery of goods, which triggers the dispute. Therefore, a retailer must have made an order of goods from a warehouse, and the goods have been delivered.

Finally, because this demonstrator wants to leverage the blockchain to manage the supply chain, a further precondition is that such a blockchain is in place.

3.1.1.4 Basic Flow

The use case's basic flow is as follows:

5. Use case begins;

6. Retailer starts a dispute procedure by sending a signed blockchain transaction (tx_D) to the DSC. The transaction includes a reference to the original order transaction stored in the blockchain's ledger and evidence of the anomaly;
7. The DSC notifies the Warehouse by providing tx_D as proof that a dispute started;
8. The DSC stores a transaction (tx_S) in the blockchain's ledger with the new dispute's identifier, the date it was initiated, and a reference to tx_D;
9. The two parties negotiate a new off-chain payment agreement;
10. If required after the renegotiation, the Warehouse sends a new shipment to the Retailer;
11. The Retailer pays the Warehouse;
12. The Retailer signs a blockchain transaction (tx_P) that will store metadata of the payment to the Warehouse into the blockchain's ledger;
13. The Warehouse signs a blockchain transaction (tx_R) that will store the metadata of the receipt of the payment received from the Retailer into the blockchain's ledger;
14. The Retailer sends a signed transaction to the DSC to signal that end of the dispute. This transaction includes a reference to tx_P and the current date;
15. The Warehouse sends a signed transaction to the DSC to signal that end of the dispute. This transaction includes a reference to tx_R and the current date;
16. The DSC sets the dispute to "settled" by storing in the ledger a transaction (tx_E) that includes the dispute's id, the date of settlement, a reference to tx_P, and a reference to tx_R;
17. Use case ends.

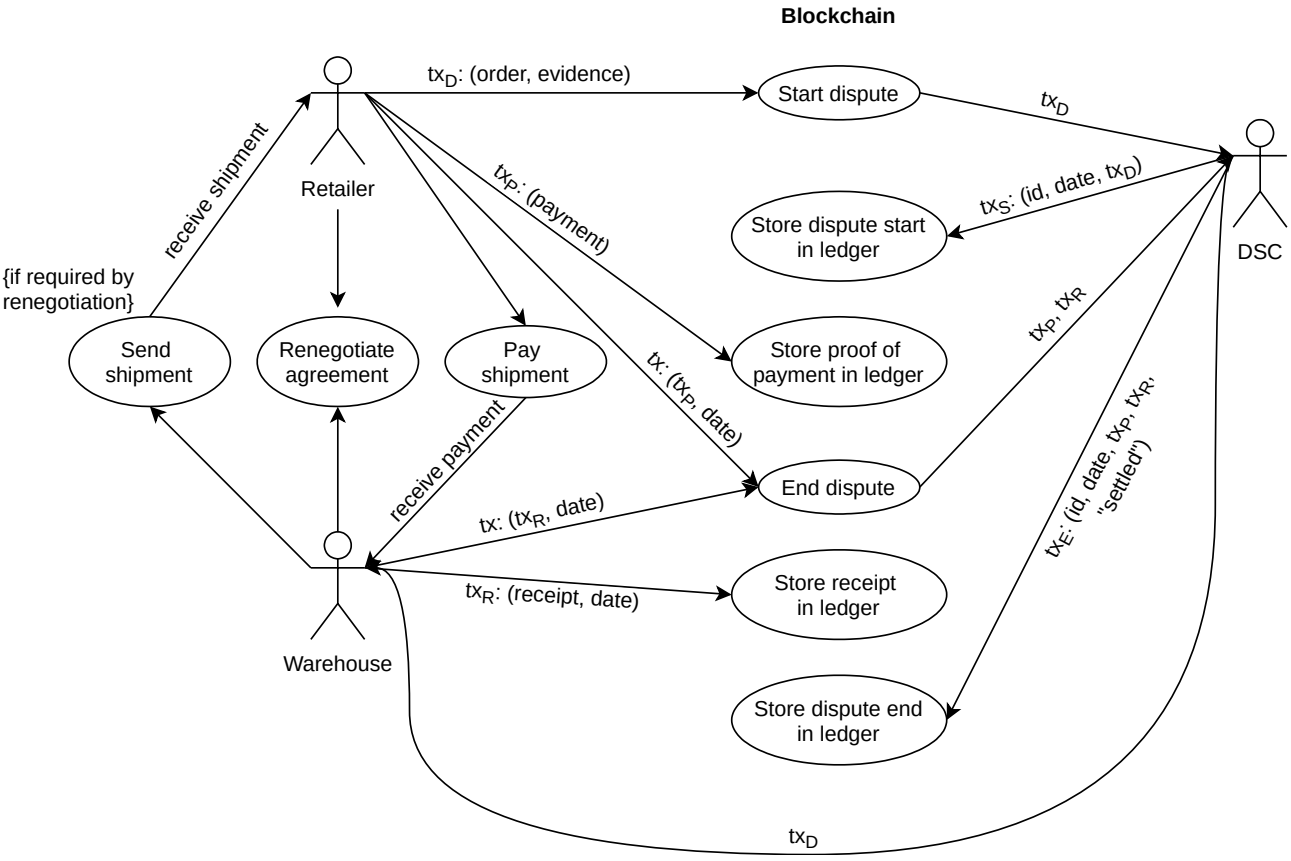

Figure 21: Supply Chain Security Assurance - SCH-UC1 Use case diagram showing the steps involved in a dispute resolution between a warehouse and a retailer store.

3.1.1.5 Postconditions

The dispute is settled.

3.1.2 Use Case SCH-UC2: Compliance and Accountability in Distributed Manufacturing

This use case describes a supply chain system for industrial products and, in particular, focuses on compliance assurance and accountability in distributed manufacturing. This scenario addresses the need for large manufacturers that produce goods via “rather complex” and “distributed processes” to track and monitor not only the location, movements, and availability of parts but also their quality and compliance. In general, compliance in manufacturing refers to technical, legal and corporate requirements, manufacturers have to fulfil in order to create and distribute goods in accordance with regulations and industry standards. This duty of manufacturers (and also of sub-contractors and suppliers) increases with the establishment of regulatory rules, directives, and supervisory bodies in different industry sectors.

The risk of non-compliance has become a pressing concern in recent years, particularly for manufacturers with operations in multiple countries and jurisdictions. Compliance mechanisms and controls include audits, system validations, audit trails, electronic signatures, and documentation of development, manufacturing, and testing. Such procedures must result in verifiable certifications which can be used to demonstrate compliance to regulation such as, for example, the Machinery Directive 2006/42/EC [9]. Companies should increase controls over suppliers and be able to track risks and incidents down to their originating points. For this reason, suppliers are required to (1) collect design, manufacturing, and test data, (2) share them to authorities and to their customers to prove compliance.

Many of these controls and modes to verify the compliance of the regulatory frameworks are also contemplated by guidelines, recommendations and standards such as NIST's *"Cybersecurity Framework"* [10], *"Best Practices in Cyber Supply Chain Risk Management"* [11] and *"Cybersecurity Framework Manufacturing Profile"* [12]. The latter one clearly establishes the need to: *"define, implement, and enforce policy and regulations"* (PR.IP-5) and *"conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements"* (DE.DP-2).

For the demonstrator, we will make use of a manufacturing scenario of construction of electrical stations or substations, in particular, with a special focus on the supply chain. In the given use case, compliance denotes, for instance, the adherence to process steps and part specifications, thus, determining the overall quality of the produced goods. In the centre of our considerations, we have a large industrial manufacturing enterprise called "Engineering, Procurement & Construction" (EPC). The EPC, designs, installs, and delivers custom-built complete electrical stations or substations, for instance with the purpose of enabling a high-voltage electrical current transmission with minimum losses. One of the main components in those stations are power transformers which might take up to one or two years to design and build them. Any malfunctioning of such components, which could require their replacement, may imply the unavailability of the electric grid in the affected region for months or even years. The equipment must be resilient to geomagnetic disturbances, electromagnetic pulses, severe weather, floods, etc. Concerning cybersecurity, they must be built applying secure development processes, making sure that state-of-the-art security mechanisms (e.g., concerning authentication, authorization) are implemented and that they do not contain any malware or logic bombs (which could be implanted as part of complex cyber-attacks).

Manufacturer EPC has, on the one hand, several different customers ("C", "C1", "C2", etc), and, on the other hand, many different suppliers ("S", "S1", "S2", etc), interconnected in a possibly long and complex international production and supply chain. In the end, EPC is responsible for delivering high-quality solutions and will be held liable in the first instance by the customer and by local authorities in case of any problem that can be traced back to the poor quality of the installed equipment, its materials, parts or components. In order to prevent or minimize disruptions, and, in the first place, to avoid the inclusion of low-quality components or counterfeits in the end system, EPC monitors not only the location, movements, and availability of parts, components, and products but also the quality and compliance of the goods with a specified manufacturing and quality assurance process. EPC enforces compliance with those standards and is able to detect the root cause of problems if they arise with the help of a trusted authority. This procedure is non-trivial: Due to the sensitivity of the market relationships, the information expressing which transformer contains which parts built by whom, and the details about the manufacturing compliance of those parts is neither expressed in cleartext in the underlying system, which, we assume, tracks the goods of the supply chain. Nor is that information kept centralized at a particular location and should only be made available when really needed to find the root cause of problems. In other words, the assurance problem, the determination of the exact fault in the production and the supplier responsible for this step requires a particular procedure.

To specify, model, and enforce the use case workflow, we use Petri Nets-based workflow specification and enforcement approach combined with the blockchain (see [13]). Petri Nets are labelled transition systems with which one can model concurrent, cross-organizational processes/workflows, and can simulate and validate the workflows for specific properties such as deadlock-freeness and soundness. Therefore, Petri Nets-based approach is amicable to formal verification, which is an advantage because one can validate workflows and rectify any errors before it can be deployed as smart contracts. In addition, for enforcing the use case workflow and guaranteeing workflow integrity, we use the Petri Nets abstraction layer in our demonstrator, which is shown in Figure 33. As part of the future work within CyberSec4Europe, i.e., in phase 2, we plan to extend our research and the demonstrator by adding protection of confidentiality of private data and accountability aspects via a judging protocol to handle dispute resolution and root-cause analysis

In our use case, another two entities will play important roles: the notification body (NoBo) and the judge. Both represent well trusted third parties inside the ecosystem. The NoBo is an authority that supervises the execution of a workflow for the construction of a plant or electrical station, respectively substation. It is informed about the progress of the construction activities and proposals and interacts by means of either accepting or rejecting certain process steps. In Germany, for the construction of plants, this role can be assumed for instance by the TÜV (*Technischer Überwachungsverein / Association for Technical Inspection*). The judge is an entity needed to resolve conflicts where it is apparent that an entity has not behaved according to the established rules (workflows and policies), but it is first unclear who this party is. There is an accountability procedure in place to determine the root cause of a detected problem and entity responsible for the error. The judge is able to revise a log and ask questions to the suspects. The protocol terminates in the normal case by identifying the root cause and one of the participants, who has misbehaved. The judge is also responsible for determining appropriate compensating measures.

3.1.2.1 Stakeholders

The main stakeholders of this demonstration use case are:

- The manufacturer of a good, which wants to optimize his processes, reduce costs, have a better overview of the exact state of the supply chain in order to act on time to any problem that could appear. In our demonstration use case, the manufacturer acts as Engineering, Procurement, and Construction contractor (EPC), which coordinates the construction of a system. In the subsequent flows, we will abbreviate the manufacturer by **EPC**.
- The end **customers** of the produced goods, for instance the operator of and energy distribution infrastructure and/or power plant. Since they are interested in the overall functioning of their infrastructure or system, they will be responsible for the quality of the integrated products. In case of any problem due to the poor product quality or late delivery of the ordered goods, production and quality will be affected on their side, typically leading to financial losses.
- The **suppliers**, which deliver parts, components, or raw materials for the production. They are interested in their parts being available on time for production and that the main manufacturer or the end customer accepts them as a reliable and trusted partner.
- The **notification body (NoBo)** is a public entity that monitors the construction of the product and is notified about the single compliance-relevant steps during the process.
- The **judge** is responsible for identifying and judging the root cause of incidents (e.g., accident in a power plant) or complaints about poor quality of a product and or compliance issues. This agency has the authority to judge on accountability and liability issues, including the compliance of production with required standards and to trigger compensating actions against non-compliant entities.

3.1.2.2 Actors

In this section we provide a list of actors with brief descriptions. Actors are all the entities that interact in the context of the distributed manufacturing ecosystem. For a first release of the demonstrator we focus on the two steps of publishing and accepting a design - e.g., the design for an electrical station or substation. Those two steps will be executed by EPC and NoBo:

- The manufacturer, i.e., **EPC** publishing a design for an electrical station or substation. Also, EPC will also conduct a feasibility study.
- The **notification body (NoBo)**, checking the design and providing an associated feasibility study. When checking the compliance of the provided assets with the product requirements and specification

and ensuring that the provisioning has been provided in compliance with the overall workflow, NoBo will accept the design.

The demonstrator will be extended in the subsequent phases of the CyberSec4Europe project i.e., in Phase 2 and its related deliverables (D5.4, D5.5, and D5.6), further involved actors (e.g., suppliers and judge) and the next steps such as accountability aspects will be added to the demonstrated use case.

3.1.2.3 Preconditions

EPC and customer have aligned on the functional and non-functional requirements of the electrical station or substation. The EPC will use this information for creating a design of the electrical station or substation. That is, as preconditions we assume that a design and a feasibility study (for the design) are provided. The demonstration workflow starts at the point in time where the EPC publishes the design and starts creating an associated feasibility study.

3.1.2.4 Basic Flow

The workflow is run in a collaborative and distributed way by all the different actors of the ecosystem. The underlying technical system and infrastructure consist of servers, smart parts and processing units in production, testing, storage, and transport. There is no global workflow management: each of these entities is processing the information it has in hand and uses its local policies. The relevant information about the workflow is provided by means of **tokens**, which can be stored locally by the entities or a distributed ledger, i.e., blockchain. When a part (or another entity) completes a step of the workflow, successfully, and it has to provide proof about its activities. Technically, this is achieved by obtaining or creating a signed token that certifies the event. This token can be consumed - i.e., evaluated and processed - in subsequent steps of the workflow for ascertaining the preconditions for those next steps. Tokens do not only keep history about the execution of the workflow: as in more conventional systems like OAuth they may also provide evidence about attributes of parts or machines or trust assertions, etc.

The normal flow of the demonstration use case looks as follows:

- Use case begins.
- **EPC** publishes the design for an electrical station or substation. As input of that step, EPC consumes two tokens.
    - T_Design: that input token specifies that a design for the electrical station or substation is available. The token identifies the respective design (e.g., a specific design document) and certifies its origin (e.g., denoting that it has been created by a certain employee of EPC, e.g., in the role of “Designer”).
    - T_FeasibilityStudy: that input token declares that a feasibility study for the given design has been created, verifying the design’s compliance with the functional and non-functional requirements of the product. That input token, for instance, can be provided by another employee of EPC, e.g., in the role of “Tester”.

  If both tokens, i.e., T_Design and T_FeasibilityStudy, exist and can be verified, they will be consumed in the step “Publish Design”. In concrete, another employee of EPC - in the role “Project Manager” - consumes both tokens T_Design and T_FeasibilityStudy and publishes the design.

  The activity of the step is the publishing of the design, which is technically represented by the output token T_DesignPublished.

- **NoBo** accepts the design for the electrical station or substation. Thereby, NoBo has to provide an (input) token T_NoBoAcceptance specifying that it is a notification body for electrical components that accepts the design. This input token is consumed together with the token T_DesignPublished.

  The activity of this step is "AcceptDesign", i.e., the design acceptance, which is technically represented by the output token T_DesignAccepted.

- Use case ends.

The following diagrams illustrate both steps. For the modelling and representation of the workflow, we use Petri Nets. Figure 22 illustrates step (1), i.e., the initial phase where T_Design and T_FeasibilityStudy as input tokens exist. The transition PublishDesign represents step (2) of the basic flow. The Petri Nets transition, as described above, consumes both tokens and creates a new token T_DesignPublished. That situation is illustrated in Figure 23. The token T_NoBoAcceptance is provided as input token (e.g., via an external service, e.g., NoBo logging on to the overall workflow system and providing its authentication token). When both tokens T_DesignPublished and T_NoBoAcceptance are available as illustrated in Figure 24, the transition AcceptDesign can be fired. This represents step (3) of the workflow. The final state of the basic flow is illustrated in Figure 25, where T_DesignAccepted is available as resulting token, representing the final state.

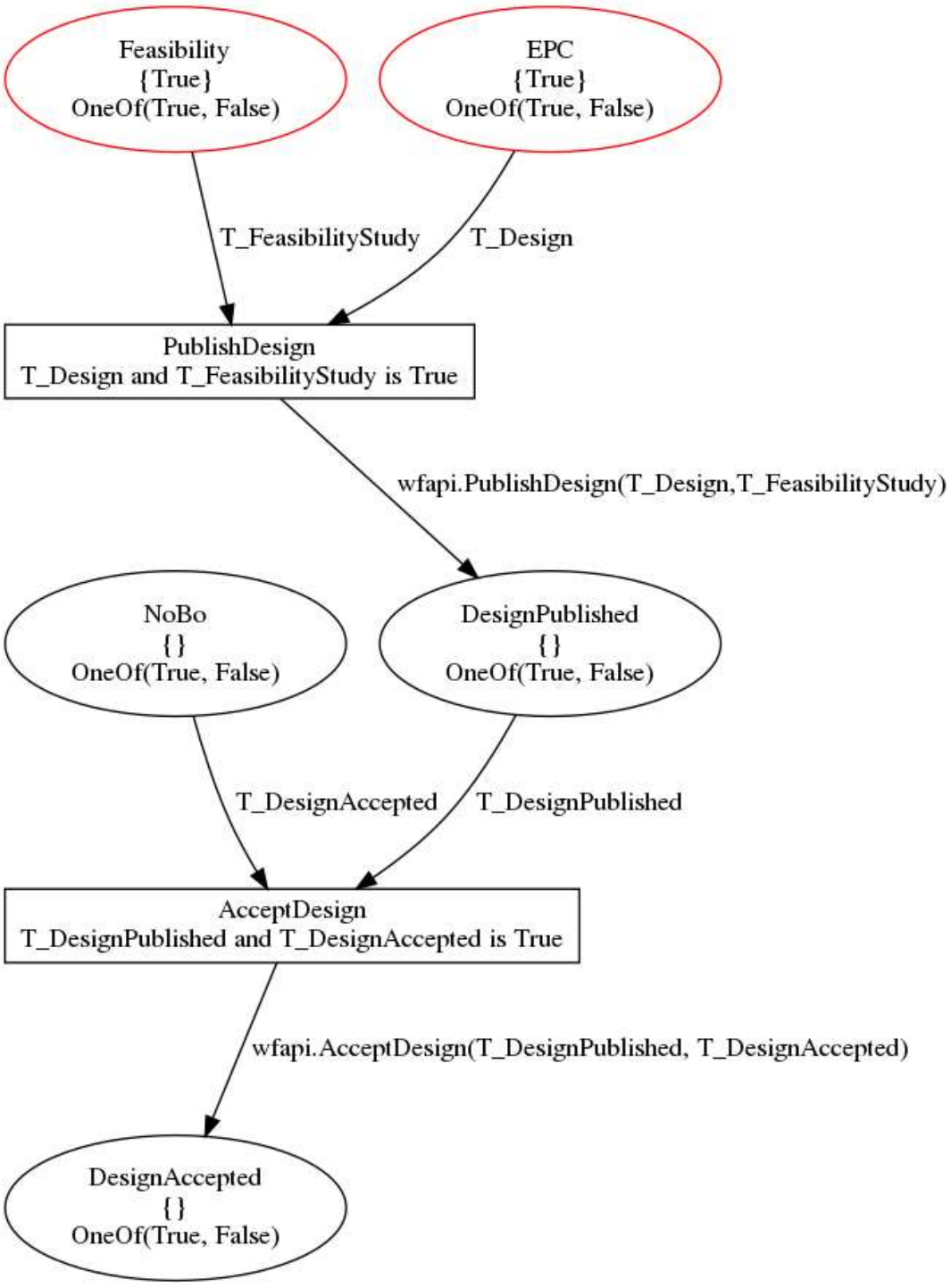

Figure 22: Supply Chain Security Assurance - Initial phase where T_Design and T_FeasibilityStudy as input tokens exist.

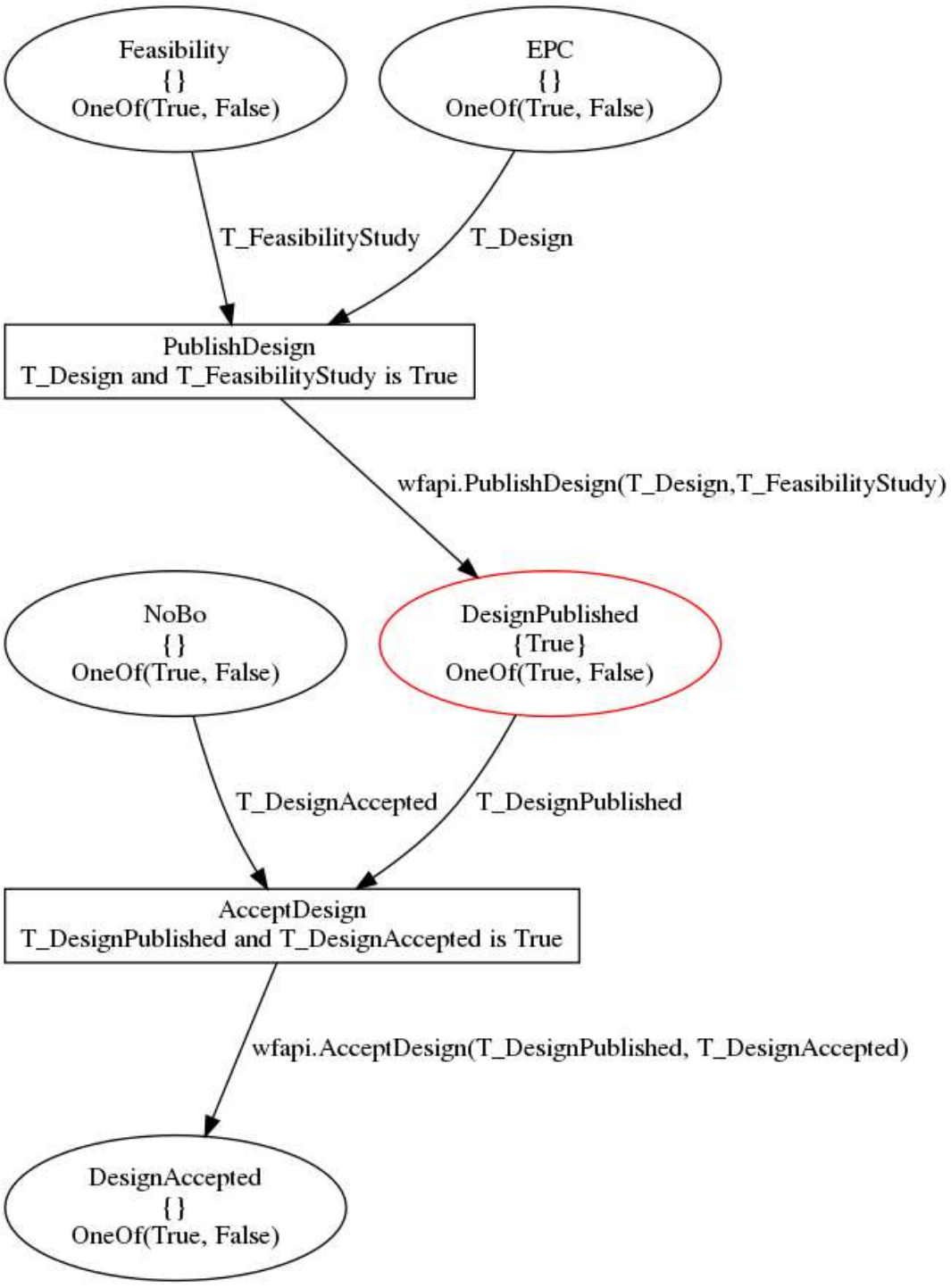

Figure 23: Supply Chain Security Assurance - Transition PublishDesign consumes both tokens and creates a new token T_DesignPublished.

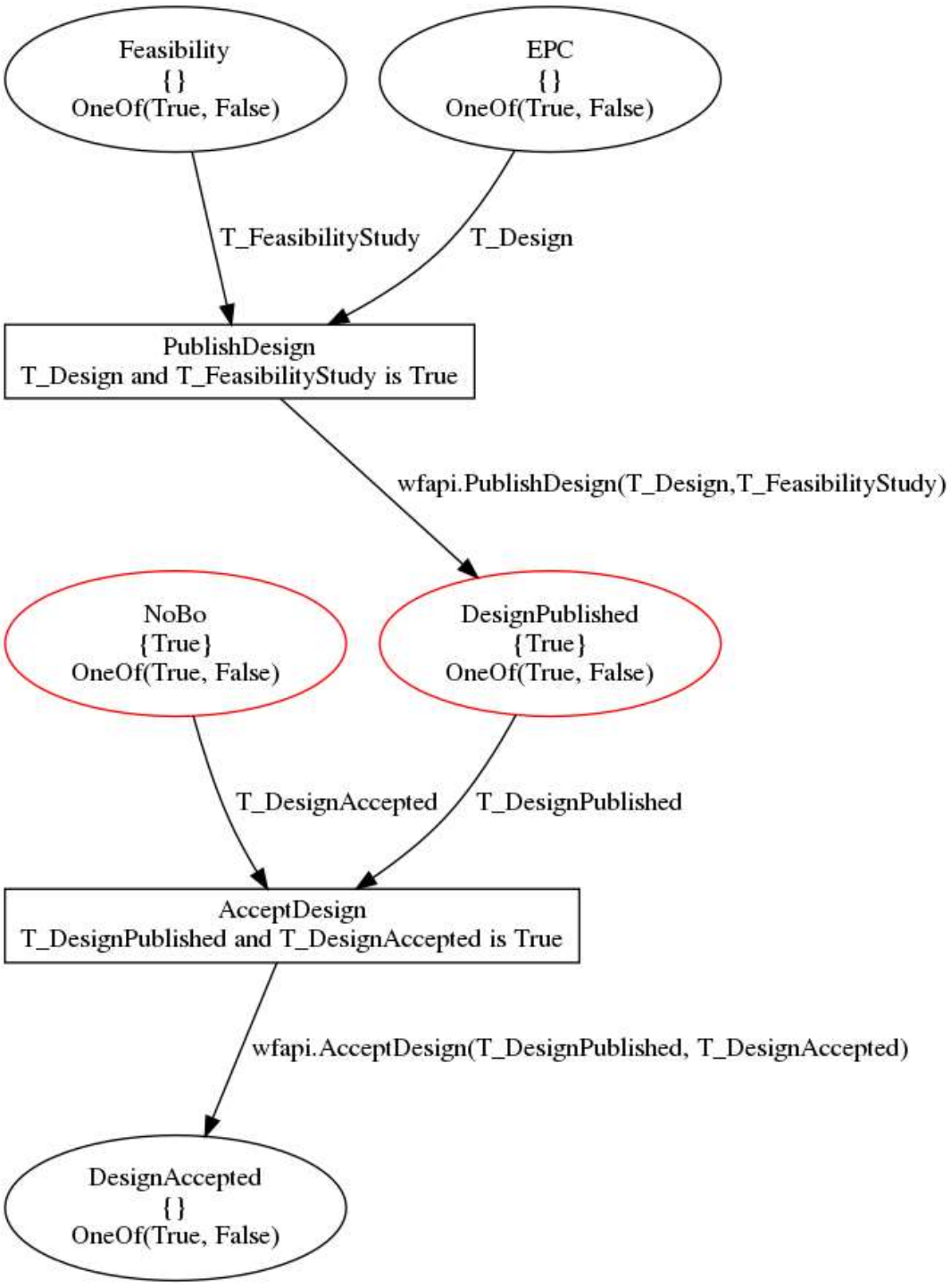

Figure 24: Supply Chain Security Assurance - Tokens T_DesignPublished and T_NoBoAcceptance are available.

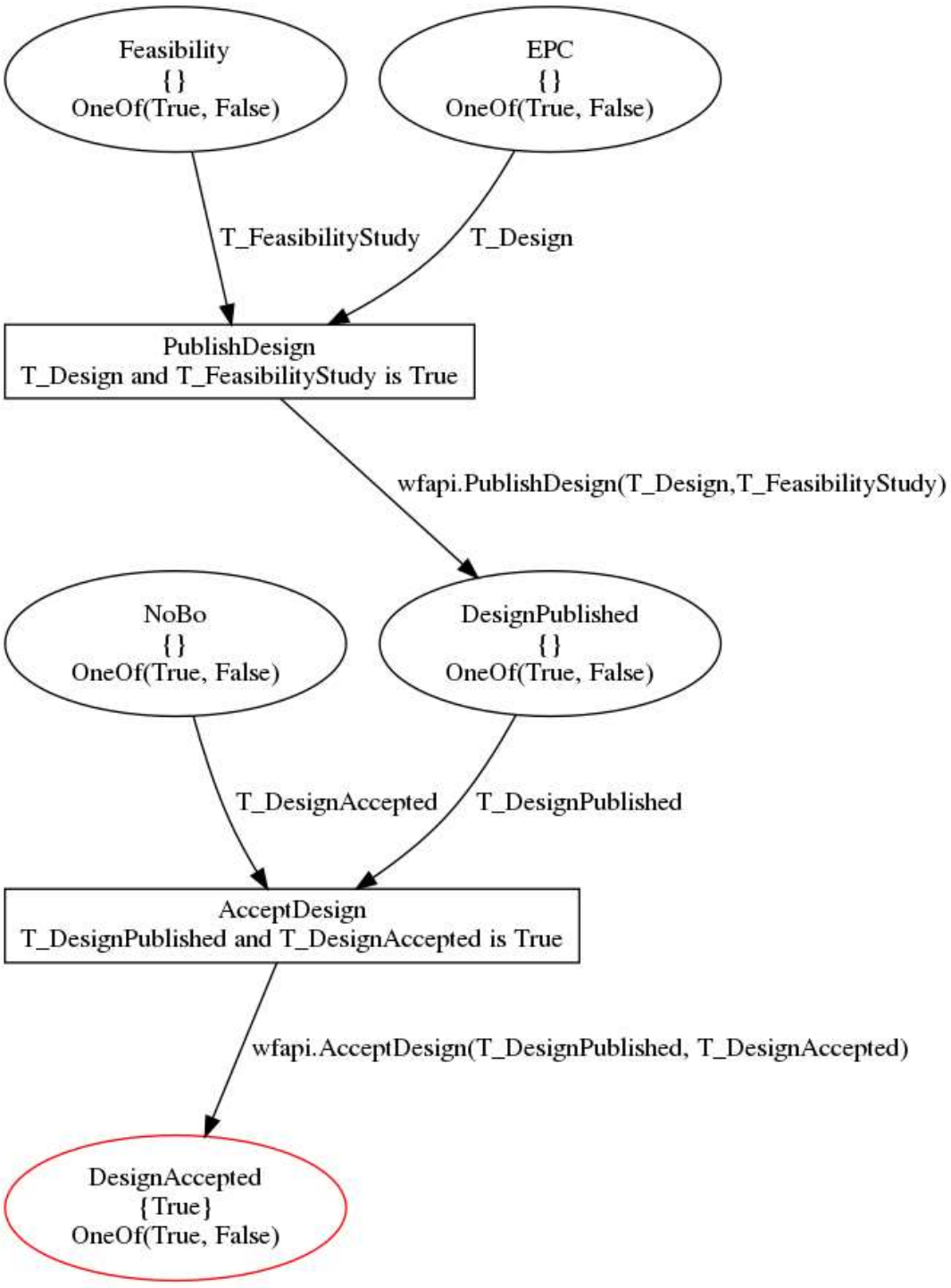

Figure 25: Supply Chain Security Assurance - End of the basic demonstration flow where the Design has been accepted via T_DesignAccepted.

3.1.2.5 Postconditions

- All intermediary tokens (T_Design, T_FeasibilityStudy, T_DesignPublished, T_NoBoAcceptance) have been consumed.

- At the end of the workflow, the token T_DesignAccepted represents the state of NoBo having accepted the design that was published by EPC.
- All steps executed by the workflow are reproducible, i.e., verifiable, as the tokens (created ones and consumed ones) are still available and stored reliably by the distributed ledger (which is implemented by the underlying blockchain architecture). The distributed ledger represents the workflow's audit trail.

3.2 Demonstrators Set-up

3.2.1 Use Case SCH-UC1: Supply Chain for Retail

3.2.1.1 Relation to Use Case

This demonstrator implements use case *SCH-UC1 – Supply Chain for Retail*. It shows, with a simple interface, how a blockchain can help, and automate, the management of supply chain processes. The dispute use case we present in this document is a core part of the demonstrator, showing the disputes under way and leveraging smart contracts to solve them. We chose to focus on this aspect of supply chain management in this first version of the demonstrator, because we argue that it is a key issue that is often badly handled by supply chains today.

3.2.1.2 Relation to WP3 Assets

The demonstrator will integrate two assets from WP3:

- Blockchain Platform (NEC): the demonstrator leverages this asset as its blockchain platform. This blockchain architecture allows private transaction exchanges by ensuring that only the relevant stakeholders receive the information. Additionally, the technology scales by allowing parallel consensus in the network via satellite chains. We can think about a satellite chain as a small, independent blockchain with its own ledger, smart contracts, consensus algorithm, and participants. However, satellite chains can communicate and exchange transactions. In this demonstrator, each satellite chain represents a flow of goods and all the entities involved in their processing (e.g., manufacturers, suppliers, warehouses, retailers). For example, a warehouse could form a satellite chain with all the retail stores that it provides with goods. The chain would record all the interactions (orders, payments, deliveries) between the warehouse and the stores.
- Consensus Research (NEC): this asset will work in concert with the "Blockchain Platform" one. Namely, we will integrate the research results as the consensus algorithm of the blockchain platform. The consensus algorithm is the core of any blockchain platform; the nodes of a blockchain use this algorithm to reach *consensus* over what is right and what is wrong in the ledger. A node can add new information to the blockchain's ledger only if it is approved by the majority of the other nodes. In the context of this use case, this would mean, for example, storing information about a dispute in the ledger. Given the size of today's blockchain platform, it is therefore important for a consensus algorithm to be fast and scalable. This asset's goal is to produce an efficient consensus algorithm of use to this demonstrator.

CyberSec4Europe's deliverable D3.2 [4] provides further details about the aforementioned assets.

3.2.1.3 Description and Workflow

The demonstrator's purpose is to show how a blockchain can track a supply chain's activities. In this first version of the demonstrator, we focus on showing its functionalities in a simple interface. Note that most

components are in their infancy and are meant to give a glimpse of what the final demonstrator will look like. Figure 26 shows the demonstrator in action. We marked the demonstrator's main components, namely:

① Main window: the main window shows the status of the supply chain's processes. This example keeps track of material shipments, production of goods, and distributors (e.g., warehouses). for the sake of simplicity, we name them "raw material xx", etc.

② Process status: For each process, we show its status along the supply chain: for materials, we show it as *ordered* (someone put it in an order for a certain amount of this particular good, and the supplier received the order), *shipped* (supplier sent out the goods and they are now in transit), or *received* (the goods were delivered). For the production of new goods, we additionally track when the production started and when it completed (*started* and *completed* respectively in Figure 26). Each of these statuses is backed by a blockchain transaction securely storing it in the blockchain's ledger

③ Additional information pop-up: users can click on each material's status in the main tab to have more information. For example, in Figure 26 we expanded a status *shipped*. The pop-up dialog gives the transaction's unique id in the blockchain's ledger, the order id, the quantity of that particular material in the shipment, and its price.

④ Dispute warning: signals a problem with the shipment which caused a dispute. This is how the demonstrator shows, at a glance, the presence of a dispute.

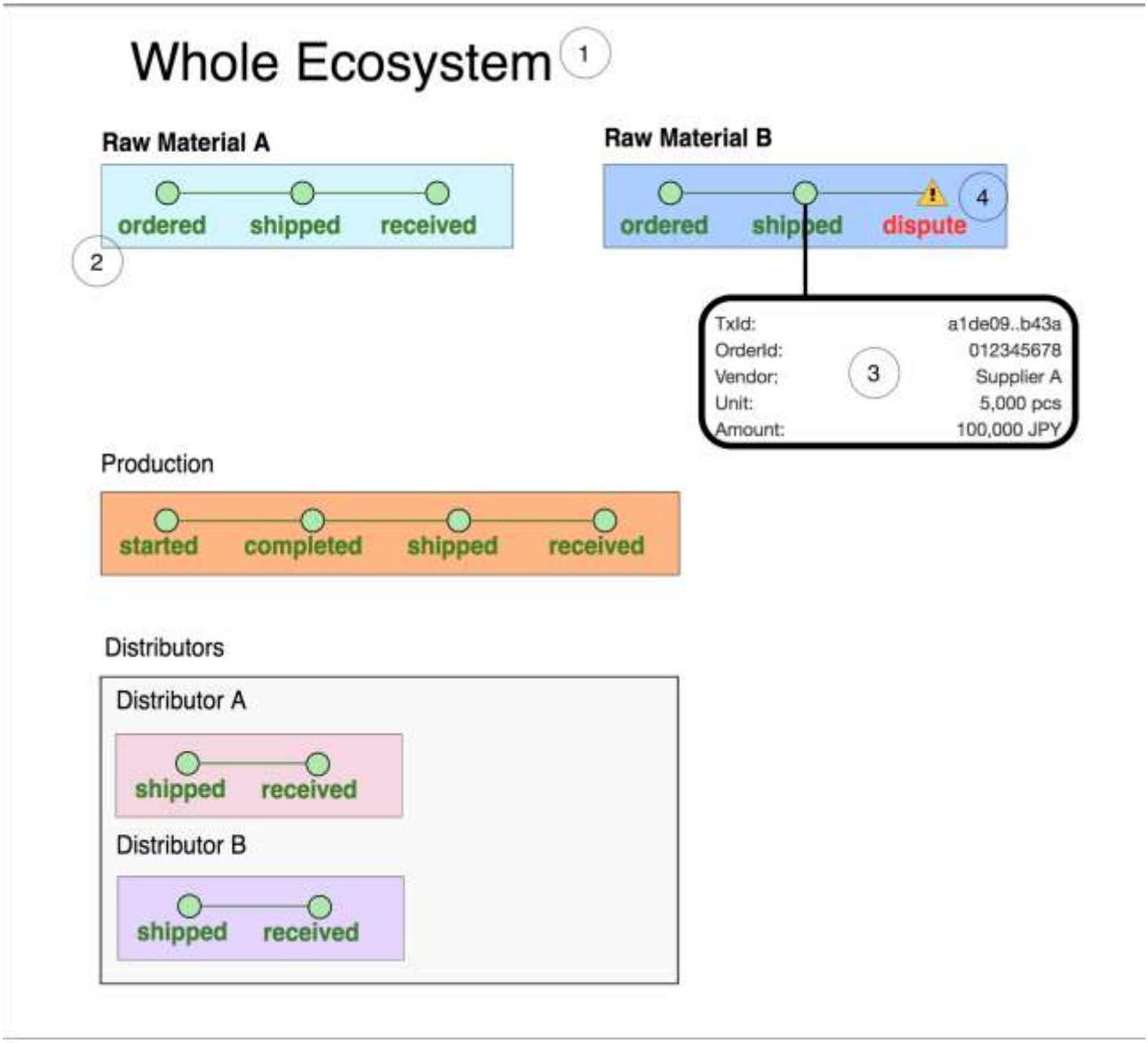

Figure 26: Supply Chain Security Assurance – SCH-UC1 Demonstrator's main view.

3.2.1.4 Target Group

The target group consists of organizations that are part of the supply chain. In the example of a retail supply chain, this includes the retailer who purchases the goods, the distributor, the supplier and the original manufacturer. Figure 27 illustrates a typical supply chain and the transaction lifecycle:

In existing supply chains, the retailer has limited visibility into the supply chain because i) the Enterprise Resource Planning (ERP) systems of the different stakeholders are siloed and incompatible with each other; and ii) stakeholders are concerned about confidentiality, thus sharing little information. If there is a delay or error in the shipment, the retailer raises a dispute and a significant amount of time is spent on review, evidence gathering, negotiation, and settlement. Using a trust-minimized blockchain infrastructure, the nodes of the various participants are synchronized in real-time and there is consensus on the state of the supply chain transaction. The asset "Blockchain Platform" and, as a consequence, this demonstrator, uses a unique satellite chain architecture, where the business data is only visible to participants within each satellite chain. This ensures transaction confidentiality.

As all participants have the same view of the status of deliveries and transactions, participants can i) recognize delays faster and take remedial action without raising a dispute; and ii) if there is a dispute, then the process of review, evidence gathering, negotiation, and settlement is significantly quickened. Disputes are resolved faster and capital that was previously locked up in lengthy disputes is now put to use more efficiently.

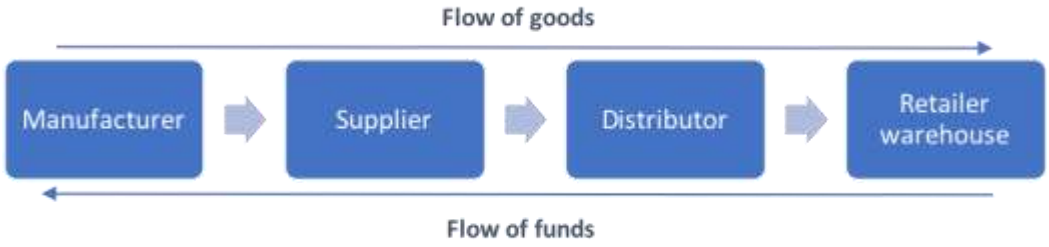

Figure 27: Supply Chain Security Assurance - Illustration of a typical retail supply chain.

3.2.2 Use Case SCH-UC2: Compliance and Accountability in Distributed Manufacturing

For the demonstration of the use case SCH-UC2 a cloud-hosted application is used. We first present the demonstrator from a user perspective, showing and explaining the respective user interface and interaction flows. The software architecture of the use case implementation is described in further detail in the following subsections.

3.2.2.1 Relation to Use Cases

Users can try out the demonstrator using a browser-based web application. By opening the front page of the demonstrator application, the user will be presented with a login page as shown in Figure 28.

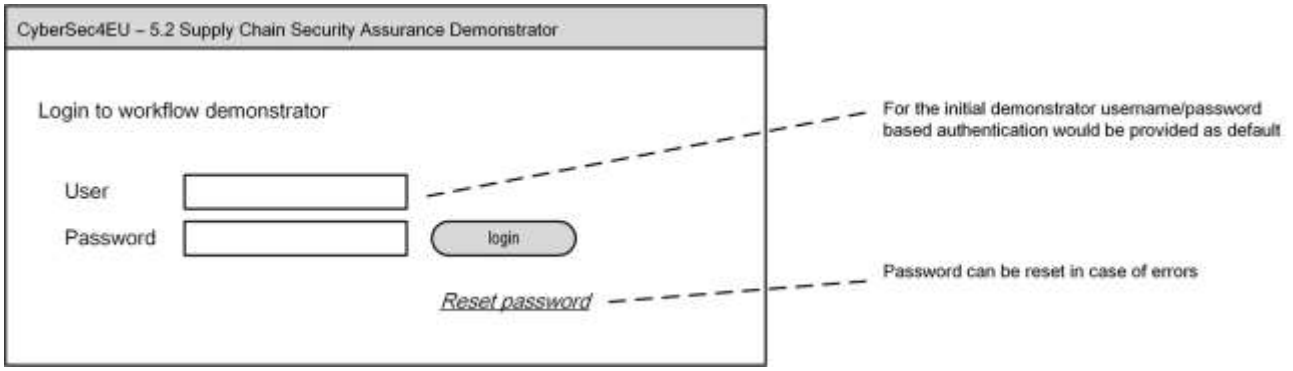

Figure 28: Supply Chain Security Assurance - Workflow GUI: Step 1 (login)

- For the first version of the demonstrator, username / password-based authentication is used. After successful login, the user is presented with a workflow selection page. Productive implementations of the use case will abstract from the workflow-layer and present role-specific input masks for users. The focus of the demonstrator, however, is on the illustration of the workflow enforcement. That's why in particular that architectural layer is presented and highlighted in the demonstrator's user interface. In the given example, the user can select a given workflow instance like **SCH-UC2 Compliance and Accountability in Distributed Manufacturing** (see Figure 29) which represents a workflow for the design and construction of an electrical substation.

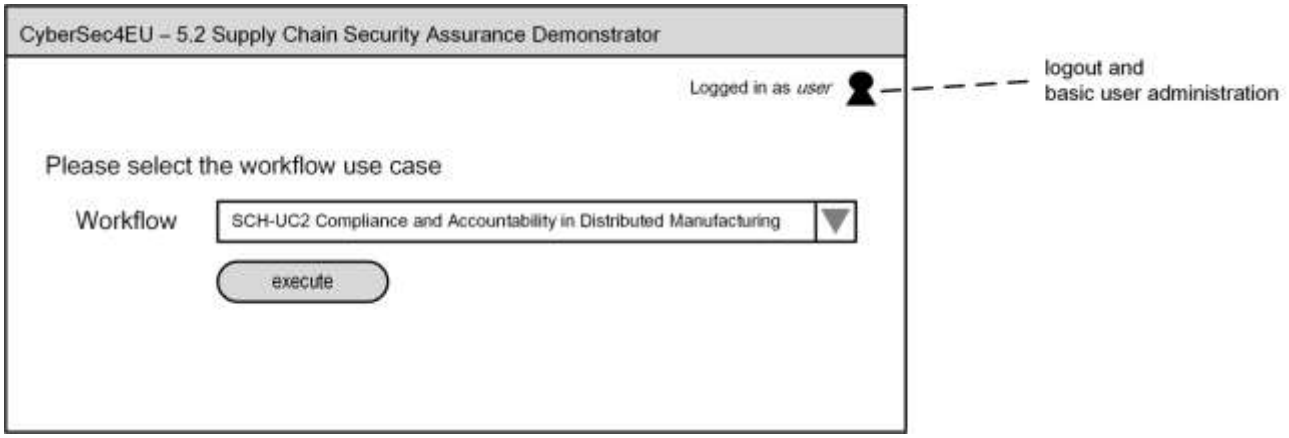

Figure 29: Supply Chain Security Assurance - Workflow GUI: Step 2 (workflow selection)

- Subsequently, users are offered different views on the workflow, respectively the underlying Petri Net model. As shown in Figure 30 they are offered a graphical representation of the Petri Net that provides a user-friendly overview of places and transitions. The current status of the execution can be inferred by colored states. In particular, places with given tokens are highlighted. The same applies to transitions whose preconditions are fulfilled and can be fired. In the given example, the tokens T_DesignPublished and T_NoBoAcceptance exist so that the places NoBo and DesignPublished are highlighted. As the preconditions of AcceptDesign are fulfilled the transition is highlighted as well. Firing a transition or setting tokens is not possible in this view but in the views Places and Transitions, as shown below.

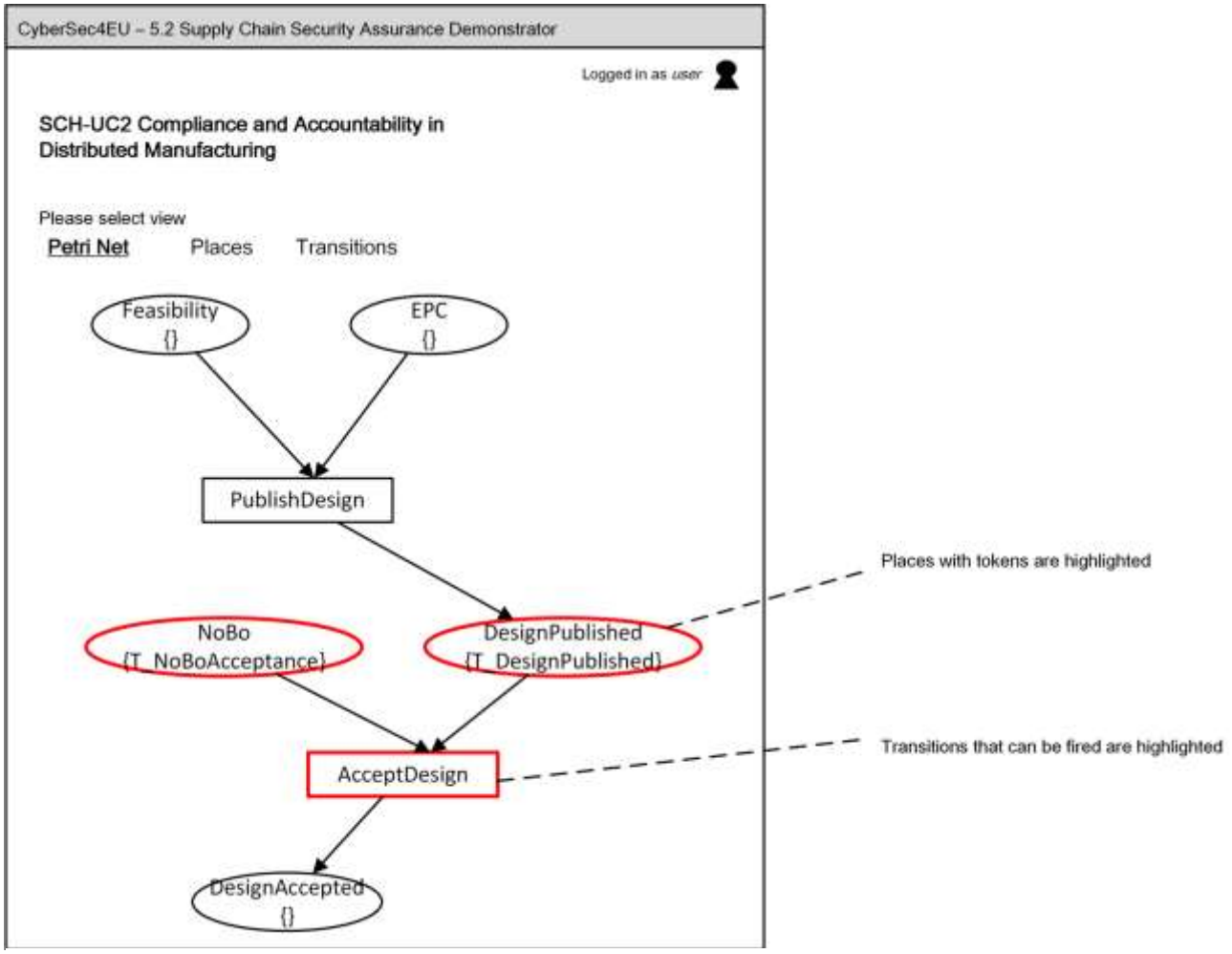

Figure 30: Supply Chain Security Assurance - Workflow GUI: Step 3 (Petri Net view)

- In the given example, all tokens needed to fire the transition AcceptDesign are already given. In general, tokens that are missing to execute a step of the workflow - which technically denotes firing a transition - can be set in the Places view. For demonstration purposes, the user can easily set tokens via the button **add** (see Figure 31). In a productive use case, the user would have to upload specific documents like a test/verification document that is signed by an authorized test engineer. That upload and verification process would then generate respective tokens.

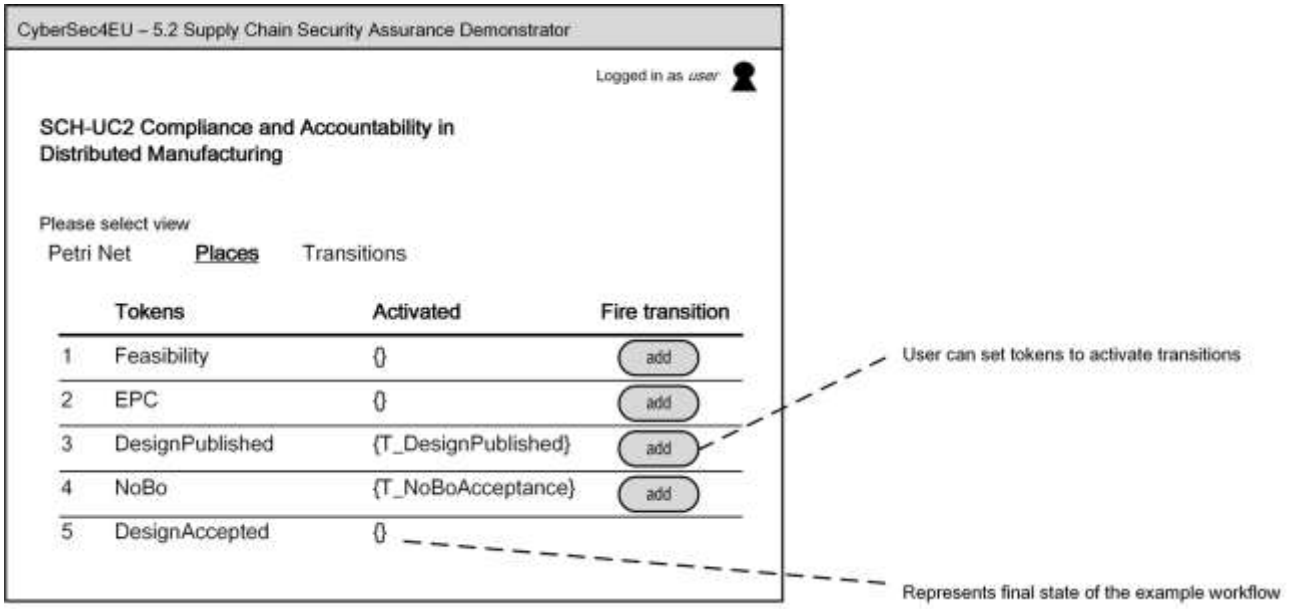

Figure 31: Supply Chain Security Assurance - Workflow GUI: Step 4 (Places view)

- Changing to the Transition view, the user can actually fire enabled transitions. In the given example the transition AcceptDesign can be fired, as the preconditions (in form of tokens T_NoBoAcceptance and T_DesignPublished) are fulfilled. That means, that step 3 of the workflow can be performed, which is about the acceptance of the published design by a trusted third party, i.e., the notification body. T_NoBoAcceptance represents the phase of NoBo attesting that it accepts the published design. In a productive system, the existence of both tokens would automatically trigger the execution of that transition. For demonstration purposes, the execution is made available for users. That is, they are able to perform step (3) of the workflow by clicking on the enabled **fire** button as shown in Figure 32.

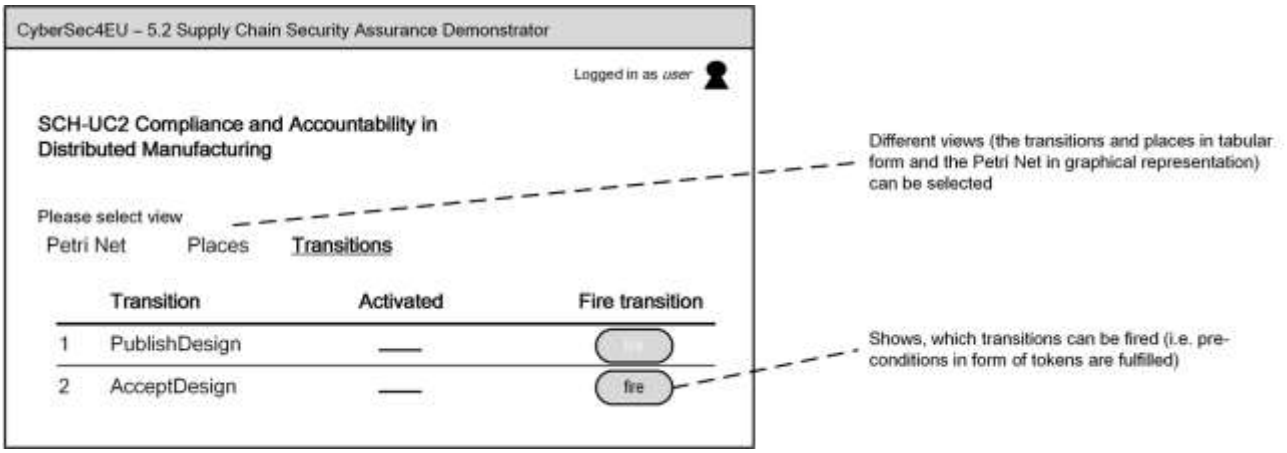

Figure 32: Workflow GUI: Step 5 (Transition view)

- After having executed the transition AcceptDesign, the tokens T_DesignPublished and T_NoBoAcceptance are consumed and a new token T_DesignAccepted is issued. This represents the final stage of the workflow. As multiple executions of the workflow are possible, multiple T_DesignAccepted token instances can exist in the end. Each of them representing a distinct execution case. That also illustrates the fact that intermediary results and end states (both represented via tokens) are reliably stored in the blockchain infrastructure which is an integral part of the system architecture.

3.2.2.2 Relation to WP3 Assets

Blockchain Platform (NEC): the demonstrator relies on a blockchain as the underlying ledger infrastructure. The initial demonstrator is built upon Hyperledger Fabric[24] but will be moved to WP3's Blockchain Platform asset. This blockchain architecture allows private transactions to be run in satellite chains. That concept supports confidentiality protection as actors do not need to share all details of transactions (e.g., internal approval processes on the side of the EPC) to other actors which represents a key requirement for distributed supply chain use cases.

3.2.2.3 Description and Workflow

This section presents the architecture of the demonstrator to showcase distributed manufacturing use case (SCH-UC2). The demonstrator relies on a three-tier architecture as illustrated in the Figure 33.

The layers of the architecture are given by:

- the *presentation layer* which is a web-based user interface;
- the *business-logic layer* that is divided into two application layers:
    - the business-logic is modelled, validated, and specified as Petri Nets workflows. The Petri Nets workflow is then implemented by means of a Petri Net abstraction layer; and
    - the Petri Nets workflows are then translated into Smart Contracts which can then be deployed on a blockchain platform;
- finally, immutability and accountability are achieved by storing the business transactions on a *distributed ledger layer*, i.e., via a blockchain infrastructure.

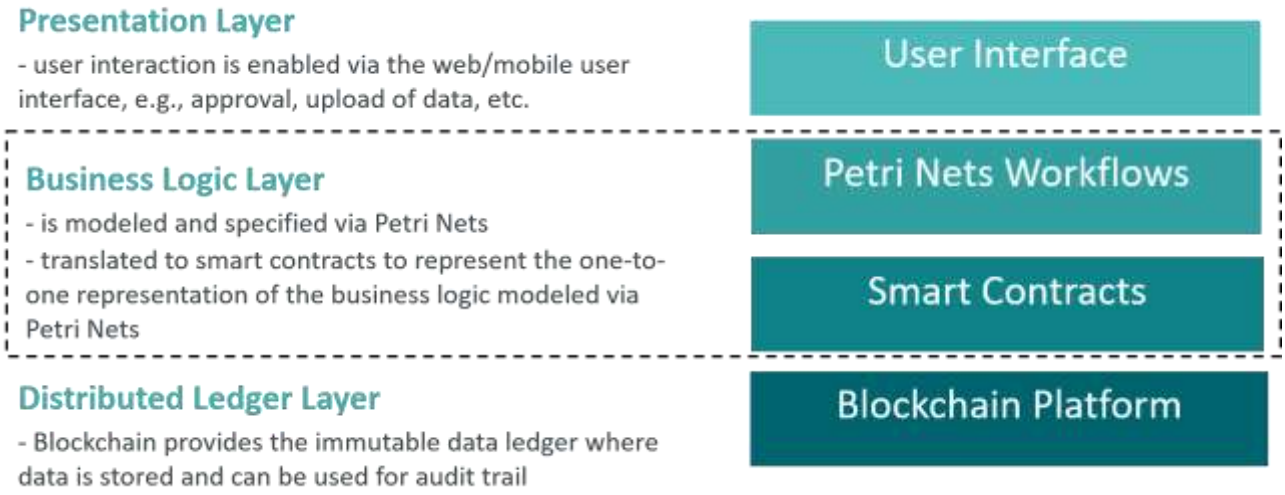

Figure 33: Supply Chain Security Assurance - Different layers of the proposed DEMO architecture.

Presentation Layer

The user interface is designed to be modular, therefore, uses a web application framework with REST API interfaces. For demonstration purposes, we plan to use the Python based web application framework "Flask"[25]. This web application can be extended in the future as per the use case requirements.

[24] https://www.hyperledger.org/projects/fabric
[25] https://palletsprojects.com/p/flask/

Business Logic Layer

The business logic or workflow execution features are exposed as REST API interfaces to enable interoperability and seamless integration with other services. The business logic layer is represented by two different components: Petri Nets workflow abstraction layer and the Smart Contracts.

Petri Net Abstraction Layer

The authors of [14] use Petri Nets for their ability to model a business logic into one or more workflows and verify them for properties such as deadlock-freeness and soundness properties. In addition, Petri Nets are easier to understand and can be used to trace the steps that have been completed and the required next steps in a workflow compared to doing this evaluation based on smart contracts that represent the implementation of the business logic. Furthermore, there is also the possibility to automate the generation of the business logic layer by translating Petri Nets into smart contract blueprints. For example, the authors of [15] presented a Petri Nets based smart contract generation framework.

Smart Contracts

The smart contracts are developed to represent a one-to-one mapping for Petri Net-based workflow specifications, such that they act as the code that interacts with the underlying blockchain platform without changing the business logic. In the proposed demonstrator, we plan to use *chaincode* written in JavaScript to represent the smart contracts. A middleware is introduced to connect the Petri Nets abstractions layer and the chaincode smart contract.

Distributed ledger

The distributed manufacturing use case requires to trace different entities and to hold them accountable for actions committed within the workflow. Also, the entities involved may not want to share their business logic with other competing entities. Therefore, we plan to use a permissioned distributed ledger to restrict access to the business logic and its related transactions. The blockchain platform Hyperledger Fabric[26] is a perfect fit for our use case because of the above-mentioned reasons. Therefore, we plan to use Hyperledger Fabric's channels concept to restrict the information shared between entities and chaincode written in JavaScript to deploy smart contracts.

3.2.2.4 Target Group

The following target groups would be interested in use case SCH-UC2:

- Businesses:
    - The use case is relevant for corporates of the manufacturing sector having complex manufacturing processes and that want to implement distributed supply chain workflows. The example given is the one of the productions of electrical stations or substations, in that sense cost-intensive tailormade goods that are produced in small quantities for which compliance and accountability are key aspects in order to tackle regulatory requirements and handle liability.
    - In addition, certification bodies (TüV) would be interested in the demonstrator that shows how they can easily interact in a distributed workflow example. They will be presented with the benefits of distributed, cross-organizational collaboration and the possibility to keep the audit trail in a distributed ledger.
- Organizations:

[26] https://www.hyperledger.org/projects/fabric

- Public organizations like notification bodies and courts. For them access to audit trail information which is stored in a distributed ledger is demonstrated. That gives them easier access to certified information (e.g., in particular in situations when some entities act less cooperative and are unwilling to disclose information, while others can and are interested in solving conflicts).

4 Privacy-Preserving Identity Management

As indicated earlier, and also in the main goals stated in the previous requirements document D5.1 [1], the privacy-preserving identity management demonstrator is intended to increase the trustworthiness as well as privacy of online identity management systems. A special focus is put on the integrity and privacy-protection of university degree certification systems, and also the demonstration will be performed in this context. The demonstrator will be executed and verified at CTI in Greece.

Before specifying the different use cases in detail, the following figure gives a high-level overview about of relations. We note that while all planned use cases are presented here and in the following, some of them are intended to only be included in the second phase of the demonstrator:

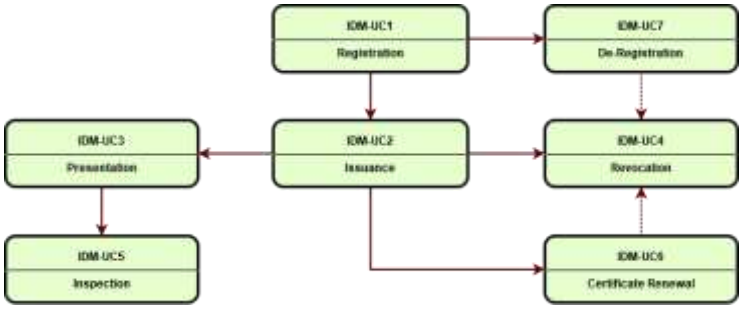

Figure 34: Privacy-Preserving Identity Management - Relations among use cases of the identity management demonstrator

4.1 Use Cases Specification

4.1.1 Use case IDM-UC1: Registration

This use case describes all steps and interactions needed for a user to join a privacy-preserving identity management system. For reasons of identity assurance, and depending on the concrete instantiation and use case, this use case may involve offline (physical) processes like visiting an authority's office, or online steps leveraging existing systems like governmentally-issued eIDs. In the course of the registration, the necessary (master) key material for a user is generated and made accessible to the user, e.g., in software, bound to a hardware token such as a smart card, or through an authority-hosted hardware security module (HSM).

Specifically, for our demonstrator case, this use case contains all steps needed for a graduate to register to our demonstrator and to Degree Certification System. The Degree Certification system has stored the uploaded degrees and professional certifications. The graduate is following the instructions of the CTI's Application Portal in order to be considered as a registered user.

Figure 35 shows the UML use case diagram for the IDM-UC1.

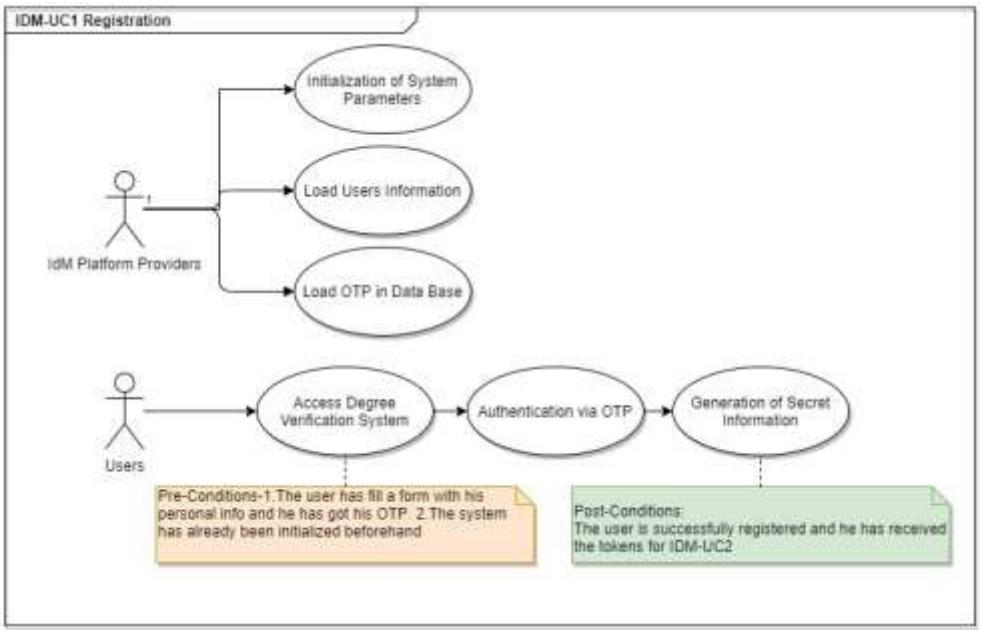

Figure 35: Privacy-Preserving Identity Management - IDM-UC1 Diagram

4.1.1.1 Stakeholders

In the following we briefly recap the main stakeholders interested in the intended demonstrator on privacy-preserving identity management, as already introduced in D5.1 [1]. We will specify all of them under this use case, as all use cases of this demonstrator are highly entangled and cannot be considered standalone. Thus, even if a stakeholder might not be actively interested, e.g., in the "Registration" phase, it will list it in the following because this phase is inherently required for all following steps:

- **Educational institutions such as universities**. In Greece there was an incidence of corruption where people could buy phony university degrees from companies selling "diploma" over the Internet requiring nothing more than a fee. Educational institutions would suffer from a severe credibility loss if fake diploma of their institution emerged. As a result, cryptographically and provably secured means for certificates can be used as a countermeasure, while at the same time potentially leading to easier processes due to paper-less processes;
- **University students**. Students will receive digital certificates for their degrees, passed courses, etc, thereby making their certificates accessible anywhere and anytime. Furthermore, they will be able to selectively share parts of the information in a user-centric way;
- **Employers**. Employers adopting our system will have a way to easily and with very high authenticity guarantees verify whether applicants hold certain academic degrees, thereby minimizing their risk for fraud, following the "digital is original" paradigm. Furthermore, by being able to automatically verify certain predicates of applicants, parts of the application process might be automatized.

The applicability and usefulness of our demonstrator can easily be extended beyond the considered scenarios, leading to additional other stakeholders:

- **National authorities**. Following the "digital is original" paradigm, certain processes might be automatized and simplified for national authorities, e.g., if students – as in the case in certain countries, e.g., Austria – need to prove that they passed at least a minimum number of ECTS points in order to receive family allowance. Also, the risk of fraudulent or faked university degrees is of direct interest to national authorities.

4.1.1.2 Actors

The following actors are actively involved in this use case. Now and in the following, we briefly recap the role and interests of each actor upon their first occurrence. For further details we also refer to the relevant parts of D5.1 [1].

Primary:

- Users. Users wishing to obtain credentials on their attributes from issuers, and later present (parts of) these attributes to service providers in a privacy-preserving manner. Specifically, in our demonstrator domain, graduates receive certificates on degrees or passed courses, and can later selectively reveal this information, e.g., when applying for a job position, to local authorities, etc.;
- IdM platform providers. These providers are hosting and maintaining the central infrastructure needed for an identity management system. Depending on the concrete instantiation of the system, their sole responsibility may be to provide certain system parameters, but they may also act as a relay/proxy for messages being exchanged between the different actors, or even take over substantial parts of the computation to achieve a light-weight solution on the user's side. While for the first round of our demonstrator no the IdM platform providers do not have an active role (except for setting up parameters), this might change in further iterations of the pilot; we thus keep them as an actor for modularity of our design.

Secondary:

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

4.1.1.3 Preconditions

- A registered student wishes to join the system. The user's identity has already been verified by the university, and this information has been made accessible to the Degree Verification System;
- The system has already been initialized beforehand, i.e., key material of issuers (i.e., university), etc. have already been generated and setup.

4.1.1.4 Basic Flow

1. Use case begins;
2. Step 1
   The interested students physically visit CTI's office to declare her interest in the digital certification system. She fills in the relevant forms (including consent forms, etc.). The information is entered into the Degree Verification System, and the user receives a username one-time password (OTP) that can be used to activate her account;
3. Step 2
   The student visits CTI's Degree Verification System website and logs in using the OTP to finalize her registration;
4. Step 3
   The user is requested to change her OTP to a secure password for further usage;
5. Step 4 (optional)

For increased security, the user chooses a password which is needed to access any locally stored information, such as the user secret key generated before;

6. Step 5
   The user's secret key material is generated locally and stored on the user's device. The precise storage location (e.g., hard disk, browser add-in, mobile app) depends on the deployment scenario and still needs to be confirmed;
7. Use case ends.

The above flow is also illustrated in the following figure:

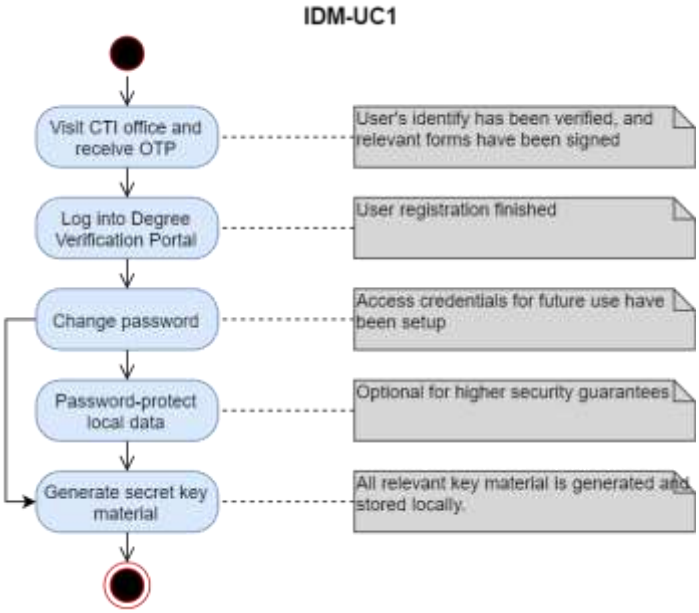

Figure 36: Privacy-Preserving Identity Management - IDM-UC1 Basic Flow

4.1.1.5 Postconditions

- The user has been subscribed to the system;
- The user has received all hardware and software tokens necessary to participate in the system, and all relevant key material has been initialized Included Use Cases.

4.1.2 Use case IDM-UC2: Issuance

To obtain a certificate on personal data, a user engages in an issuance session with a certificate issuer, which might be, e.g., a public authority, a university, or a service provider. In such an interaction, the user typically authenticates herself towards the issuer, and the two parties negotiate the specific attributes to be certified for the user (e.g., age, birth date, place of residence, nationality, expiration date, academic degrees, etc.). At the end of the interaction, the user receives a digital certificate (aka credential) attesting these attributes.

Specifically, within the domain of the degree certification use case, this step is needed for a graduate to receive a credential from the Degree Certification System. The attributes attest that she possesses a legible title.
The graduate access the Degree Certification System thought CTI's portal in order to request from it to certify that she has a legible academic degree/title/certificate.

Figure 37 shows the UML use case diagram for the IDM-UC2.

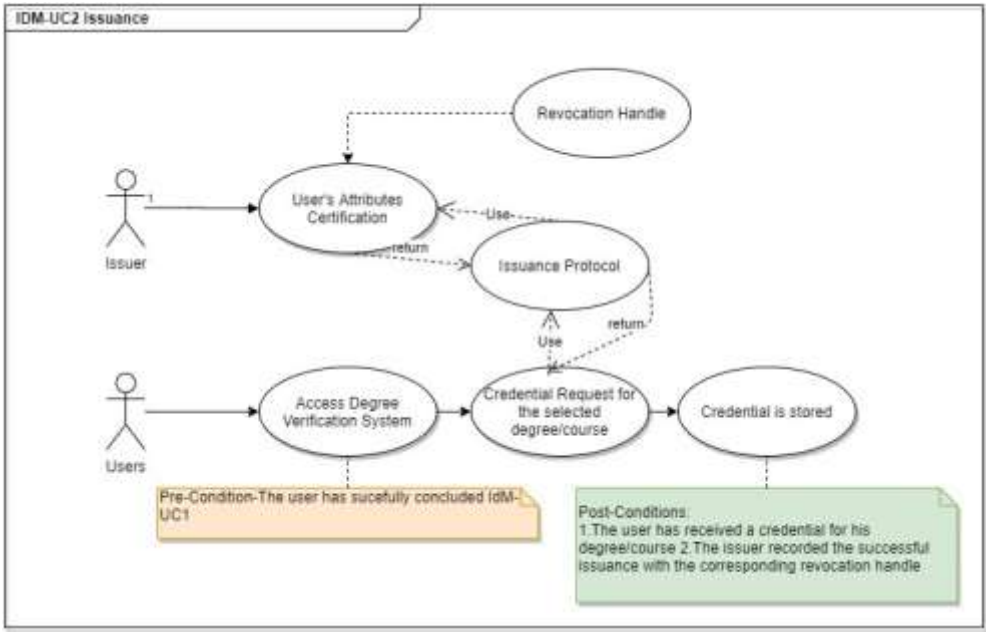

Figure 37: Privacy-Preserving Identity Management - IDM-UC2 Diagram

4.1.2.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.2.2 Actors

For more details on the actors, please refer to the previous use case (Section 4.1.1.2) as well as D5.1 [1].

Primary:

- Users;
- Issuers. Issuers are semi-trusted entities that certify a user's attributes upon her request after checking whether these attributes indeed belong to the user. In the context of our use case, education organizations may, e.g., certify that a user possesses a certain degree, passed certain courses, or applied for a certain job position. Relying parties accepting credentials issued by a certain issuer are willing to trust the issuer in the sense that it will not vouch for false attributes.

Secondary:

- Degree verification system;
- CTI's application portal. This is a web-based information portal. Through this portal, the job participants and researchers will get information about the pilot system and functionality as well as information about its usage. Moreover, this portal also contains the necessary links to the components of the system (Educational Certification System, Degree Verification System) that the participants should access;
- Educational certification system. This system lets graduates prove that they possess a certain degree or similar.

4.1.2.3 Preconditions

A subscribed user wishes to receive a certificate from the issuer (e.g., university).

4.1.2.4 Basic Flow

1. Use case begins;
2. Step 1
   The user who wished to receive a certificate from the issuer logs into the CTI Degree Verification System, using the username and password setup in IDM-UC1;
3. Step 2
   The Degree Verification System looks up the user's available degrees and passed courses. This information is then displayed to the user via the web interface, and the user choses the degree/course for which she wished to receive a digital credential;
4. Step 3 (optional)
   In the case that the credential shall be revocable, the System chooses a unique revocation handle for the credential, which will be embedded as an attribute. The revocation handle is stored by the System together with the user's identity, and the public revocation information is updated accordingly;
5. Step 4
   The Degree Verification System signs the certificate in interaction with the user, in particular embedding the user's secret key, the revocation handle (if any), and the certified qualification into the credential;
6. Step 5
   The user downloads her credential through the web interfaces and stores it locally;
7. Use case ends.

The above flow is also illustrated in the following figure:

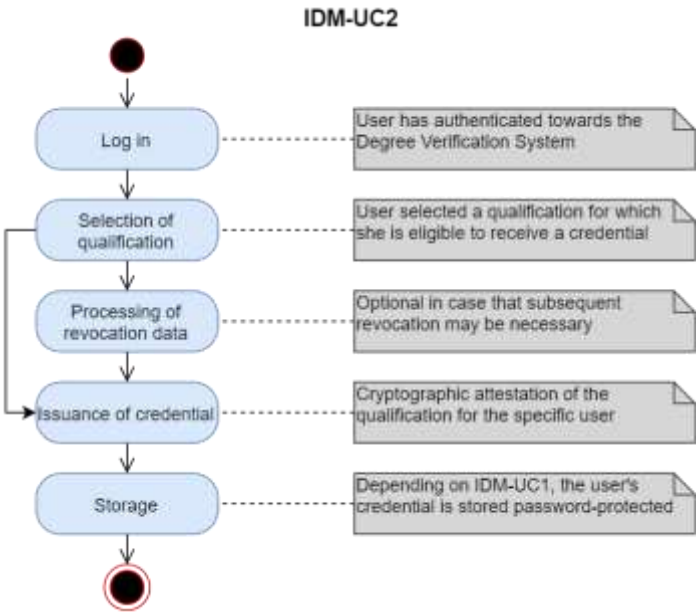

Figure 38: Privacy-Preserving Identity Management - IDM-UC2 Basic Flow

4.1.2.5 Postconditions

- The user received a credential for the requested attributes, stored in its application;
- The issuer recorded the successful issuance, potentially together with the corresponding revocation handle.

4.1.3 Use case IDM-UC3: Presentation

A user can prove possession of a credential certifying certain personal attributes to a service provider (aka relying party) by engaging in a presentation protocol. In this protocol, the two parties agree on which attributes the user needs to reveal, e.g., based on a policy of the service provider. At the end of the interaction the service provider receives these attributes with high authenticity guarantees, while the user is guaranteed that no other information was revealed to the service provider.

Specifically, within our demonstration case, this use case is performed when a student needs to generate a verifiable proof that she possesses a certain title or attended specific courses, e.g., to the application portal or a local authority.

Figure 39 shows the UML use case diagram for the IDM-UC3.

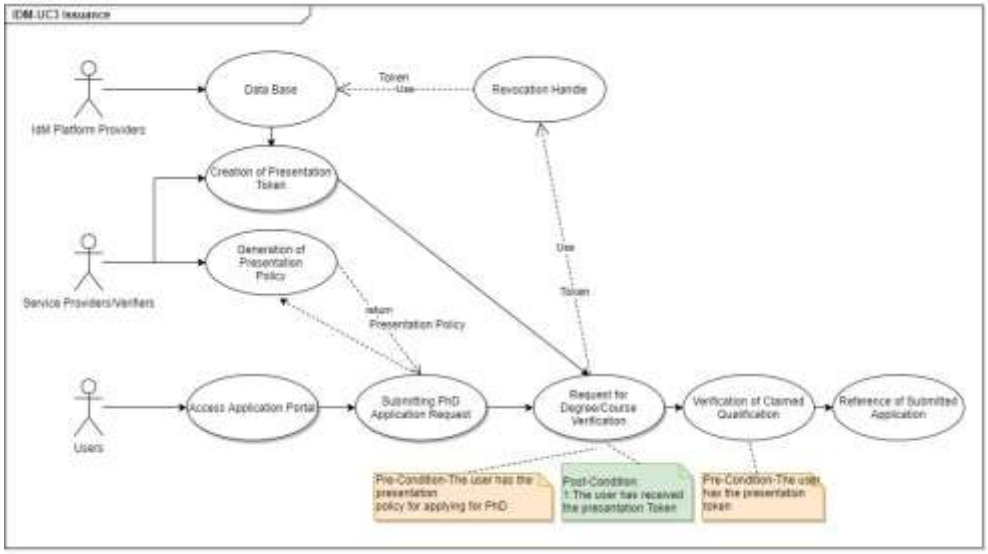

Figure 39: Privacy-Preserving Identity Management - IDM-UC3 Diagram

4.1.3.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.3.2 Actors

For more details on the actors, please refer to the previous use cases (Sections 4.1.1.2 and 4.1.2.2 respectively) as well as D5.1 [1].

Primary:

- Users
- Service providers / Verifiers. Such actors want to receive provably authentic information about a user to grant her access to a specific service. They also need to be able to define a (minimum) policy a user

must fulfill in order to be granted access. In the context of our use case, education organizations need be able to obtain verifiable claims on awards of applicants in order to accept them for a job position;

- IdM platform providers.

Secondary:

- CTI's application portal.

4.1.3.3 Preconditions

- The user wishes to prove possession of a certificate during a job application;
- A corresponding certificate has previously been issued to the user.

4.1.3.4 Basic Flow

1. Use case begins;
2. Step 1
   The user browses to the job application portal and identifies the position for which she would like to apply. At this point, no login or similar is required, as the job portal is publicly accessible;
3. Step 2
   The user adds her information and application data, such as, e.g., application letter and resume;
4. Step 3
   The job application portal offers the possibility to add academic degrees. Therefore, the user identifies the issuing university and type of degree. Using her locally stored credentials, the website then computes a cryptographic proof that the user indeed holds the specified degree and uploads it to the server; depending on the job profile, different information might be sufficient for the application (e.g., issuance date or certain grades might not be required). Note here that this computation is done fully on the user's side and no information about the credential is revealed to the portal.

   Furthermore, in case the system supports revocation, this so-called *presentation token* is computed relative to the revocation information published by the issuer, e.g., it is proven that the credential being used for the computation has not yet been revoked;
5. Step 4
   The job application portal verifies the received presentation token and adds the user's degree if the test was positive; otherwise, the claimed qualification is not accepted;
6. Step 5
   The user receives a high-entry unique identifier which she can later use to edit and update her application;
7. Use case ends.

The above flow is also illustrated in the following figure:

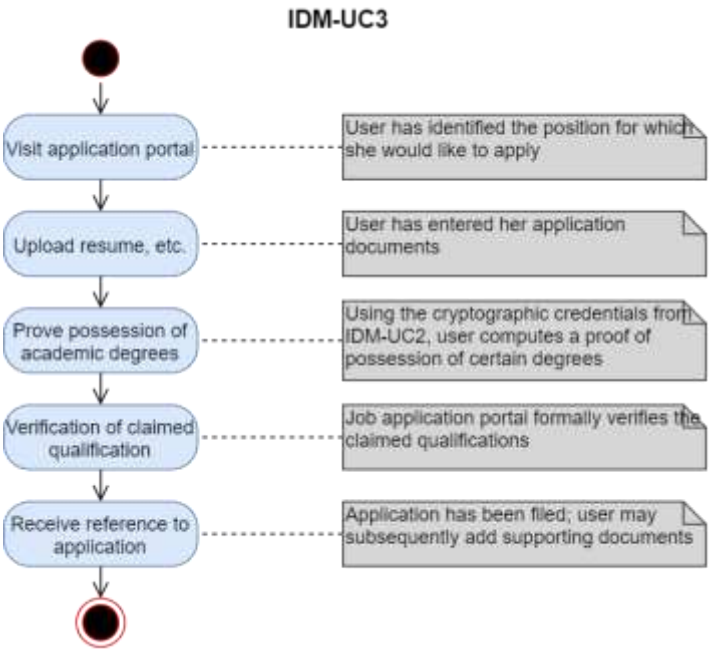

Figure 40: Privacy-Preserving Identity Management - IDM-UC3 Basic Flow

4.1.3.5 Alternate Flows

The following alternate flow is possible for IDM-UC3:

1. Use case begins;
2. Step 1 (as before).
3. Step 1a
   The user enters the unique identifier received during the application. The job application portal then displays the already added information, and enables the user to perform updates on her application;
4. Step 2-6 (as before);
5. Use case ends.

4.1.3.6 Postconditions

- The user has successfully applied for a position;
- The employer received high authenticity guarantees on the academic qualifications claimed by the user.

4.1.4 Use case IDM-UC4: Revocation

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

Within our demonstration domain, this use case will in particular be needed when attributes (e.g., names) change, or when unauthorized parties gained access to a user's secret credential.

Figure 41 shows the UML use case diagram for the IDM-UC4.

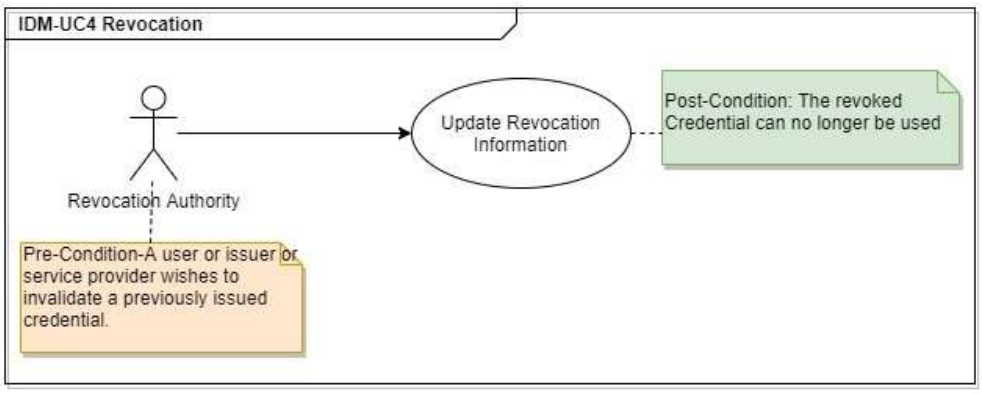

Figure 41: Privacy-Preserving Identity Management - IDM-UC4 Diagram

4.1.4.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.4.2 Actors

For more details on the actors, please refer to the previous use cases (Sections 4.1.1.2, 4.1.2.2, and 4.1.3.2 respectively) as well as D5.1 [1].

Several actors are labeled as "optional" in the following, as they are needed depending on the precise revocation model that is to be implemented. IDM-UC4 will not be covered by the first piloting round because further research is needed for an efficient realization, and the correct revocation approach has not yet been decided upon.

Primary:

- Users (optional);
- Service providers / Verifiers (optional);
- Issuers (optional);
- Revocation authorities. These parties provide publicly accessible revocation information such as white lists or black lists that may be used by service providers to decide whether or not to a accept a presentation based on a certain credential. Depending on the application scenario, revocation may be triggered by the issuer, a service provider, or the user herself. In our demonstrator case, the revocation authority and issuer coincide;
- IdM platform providers (optional).

Secondary:

- CTI's application portal (optional);
- Educational certification system (optional).

4.1.4.3 Preconditions

- At least one actor (user, issuer, service provider) wishes to invalidate a previously issued credential;
- The credential to be revoked has been clearly identified by the initiating party.

Even though the precise revocation model has not yet been decided upon, we will focus on issuer-centric revocation in the following, as this seems to be the most likely approach. In this case, the issuing university wishes to invalidate a certificate, e.g., because of abuse or because the legitimate owner reported that it was compromised and abuse is to be expected.

4.1.4.4 Basic Flow

1. Use case begins;
2. Step 1
   The Degree Verification System receives a description of the credential that shall be revoked, e.g., from the user by specifying the credentials that might have been compromised;
3. Step 2
   Using this information, the system looks up the unique revocation handle that was used when the credential was issued;
4. Step 3
   The Degree Verification System marks the corresponding entry as revoked, and updates the public revocation information accordingly;
5. Use case ends;

The above flow is also illustrated in the following figure:

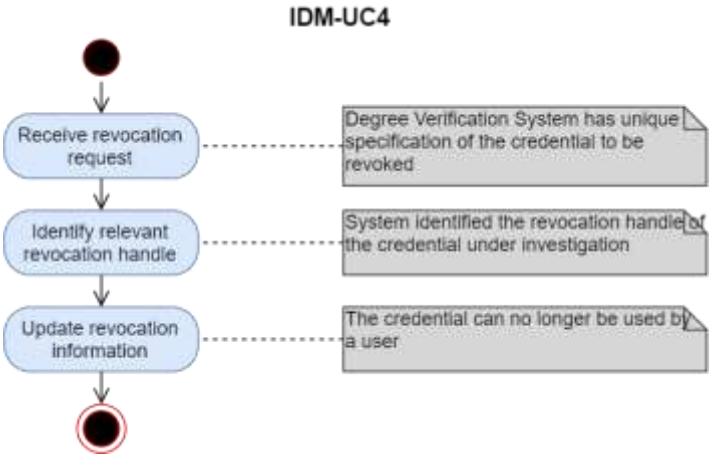

Figure 42: Privacy-Preserving Identity Management - IDM-UC4 basic flow

4.1.4.5 Postconditions

The credential can no longer be used for successful presentations.

4.1.5 Use case IDM-UC5: Inspection

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

While for the specific demonstrator scenario under consideration inspection might not be needed, we include it here because it might be needed when extending the technology beyond our demonstrator scenario, e.g., by involving additional stakeholders such as public authorities.

Figure 43 shows the UML use case diagram for the IDM-UC5.

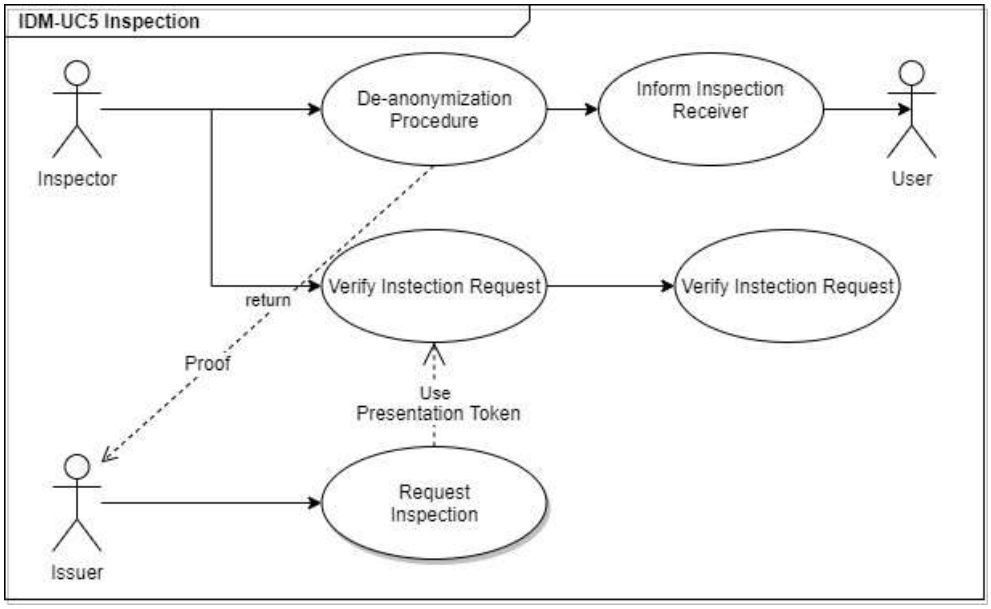

Figure 43: Privacy-Preserving Identity Management - IDM-UC5 diagram

4.1.5.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.5.2 Actors

For more details on the actors, please refer to the previous use cases (Sections 4.1.1.2, 4.1.2.2, 4.1.3.2, and 4.1.4.2 respectively) as well as D5.1 [1].

Primary:

- Service providers/Verifiers;
- Inspectors. Inspectors are able to revoke the anonymity of a certain presentation and unveil the identity of the user. We model inspectors as active actors as their actions are not triggered by another actor in the system. However, in reality, inspectors may typically become active, e.g., after a court order, i.e., after being triggered by an external entity;

  We will keep using the term "inspector" for the authority able to revoke the anonymity of a presentation, even though in our scenario the inspector and the issuer may likely collapse into a single entity; however, by having distinguished names and keeping them apart also in the implementation, we will obtain a more generic and modular demonstrator.

4.1.5.3 Preconditions

The anonymity of a performed presentation shall be revoked upon request, e.g., by the service provider.

4.1.5.4 Basic Flow

1. Use case begins;
2. Step 1
   The inspector receives the presentation token under consideration with the request to de-anonymize the holder of the underlying credential;
3. Step 2
   The inspector verifies that the requesting entity has the right to request this disclosure, e.g., based on terms and conditions, or by law;
4. Step 3
   The inspector executes the de-anonymization procedure locally, and returns the identity of the user together with a cryptographic proof that the de-anonymization has been performed correctly;
5. Step 4 (optional)
   Depending on the reason for the de-anonymization, the user is notified about the inspection process;
6. Step 5
   The requesting entity verifies the proof received from the inspector;
7. Use case ends.

The above flow is also illustrated in the following figure:

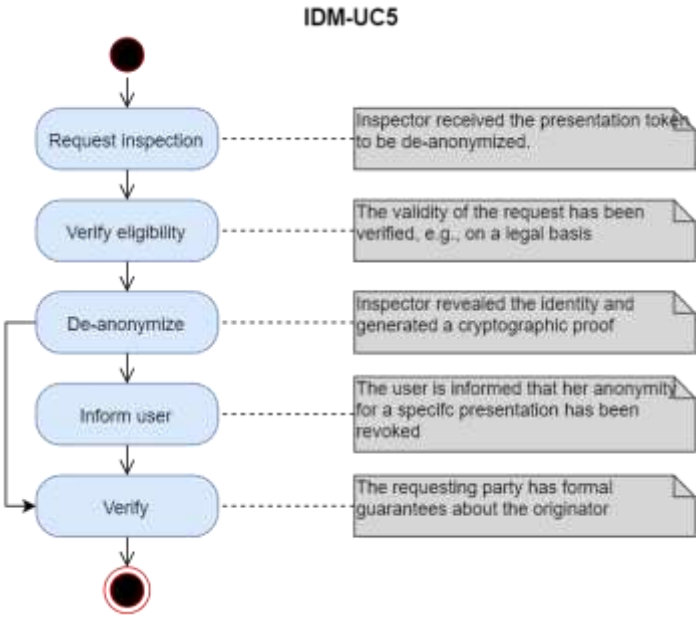

Figure 44: Privacy-Preserving Identity Management - IDM-UC5 basic flow

4.1.5.5 Postconditions

- The identity of the owner of the credential used for the presentation is revealed to the requesting entity;
- Depending on the application scenario, the user is notified about the inspection.

4.1.6 Use case IDM-UC6: Certificate Renewal

In this use case, a user can renew a credential that she already received earlier. This procedure may be triggered for different reasons, e.g., because the expiration date of a certificate has expired, or attributes such as name have changed. Also, the user may request a re-issuance of a credential that was previously revoked for some reason. The involved process is closely related to issuance (IDM-UC2, see Section 4.1.2), yet might be more lightweight and require less strict attribute assurance. Also, depending on the concrete type of credential, the use case may trigger revocation of the underlying original credential (IDM-C4, see Section 4.1.4) in order to avoid that a user has multiple credentials on the same data.

Figure 45 shows the UML use case diagram for the IDM-UC6.

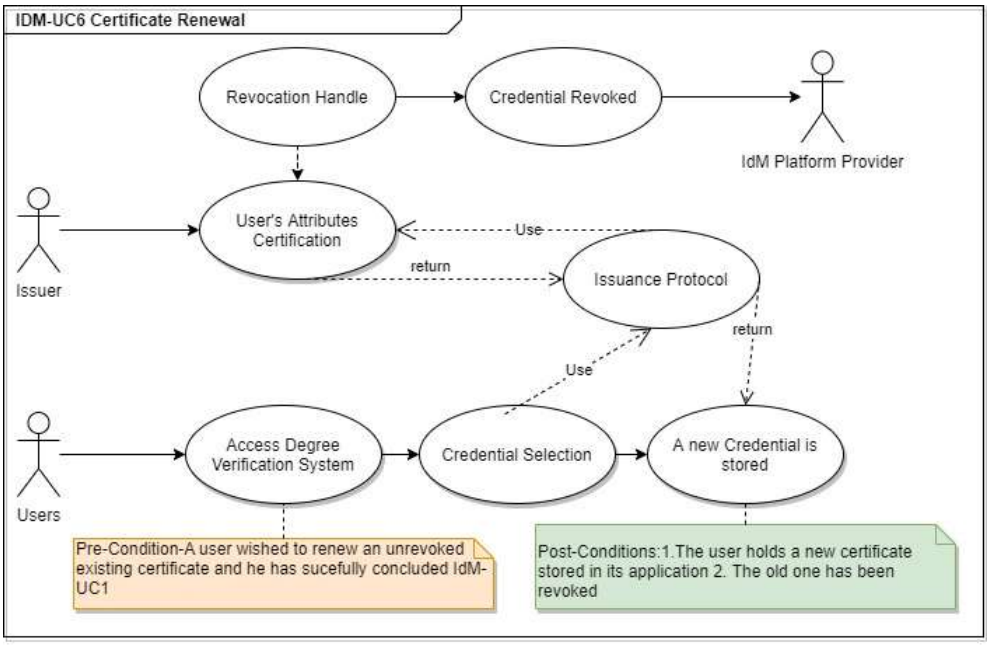

Figure 45: Privacy-Preserving Identity Management - IDM-UC6 diagram

4.1.6.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.6.2 Actors

For more details on the actors, please refer to the previous use cases (Sections 4.1.1.2, 4.1.2.2, 4.1.3.2, 4.1.4.2, and 4.1.5.2 respectively) as well as D5.1 [1].

Primary:

- Users;

- Issuers;
- IdM platform providers.

Secondary:

- Educational certification system.

4.1.6.3 Preconditions

A user wished to renew an unrevoked certificate that has already been issued, thereby updating certain attributes.

4.1.6.4 Basic Flow

1. Use case begins;
2. Step 1
   The user who wished to receive a renewed certificate from the issuer logs into the CTI Degree Verification System, using the username and password setup in IDM-UC1;
3. Step 2
   The user selects one of the previously issued credentials in the Degree Verification System;
4. Step 3
   The previously issued credential is revoked following IDM-UC4;
5. Step 4
   The user receives a new credential following IDM-UC2, thereby skipping Step 1;
6. Use case ends.

The above flow is also illustrated in the following figure:

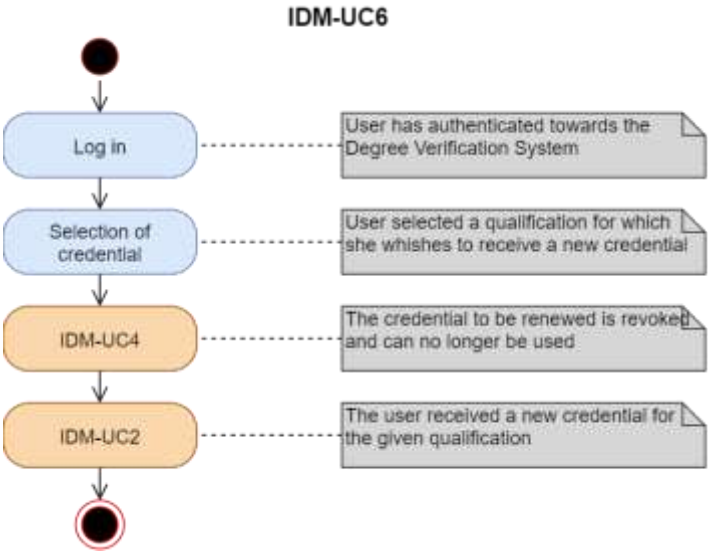

Figure 46: Privacy-Preserving Identity Management - IDM-UC6 basic flow

4.1.6.5 Postconditions

- The user holds a new certificate stored in its application;
- The old certificate has been invalidated.

4.1.6.6 Included Use Cases

- IDM-UC2: Issuance
- IDM-UC4: Revocation

4.1.7 Use case IDM-UC7: De-registration

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

Figure 47 shows the UML use case diagram for the IDM-UC7.

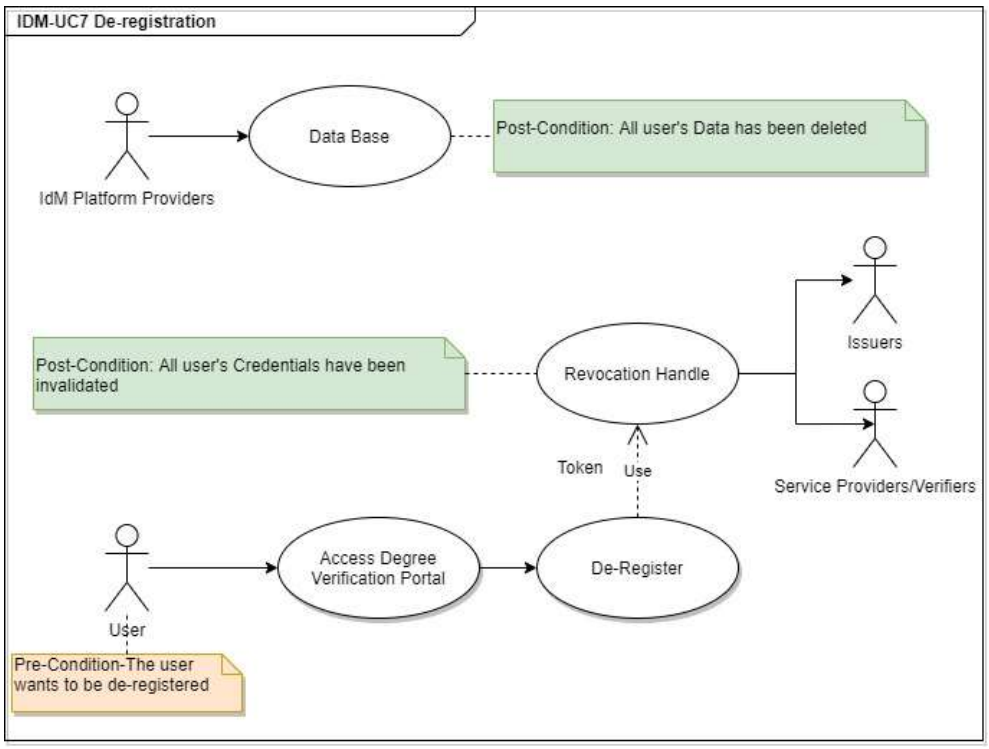

Figure 47: Privacy-Preserving Identity Management - IDM-UC7 diagram

4.1.7.1 Stakeholders

The relevant stakeholders are identical to those specified for use case IDM-UC1 (see Section 4.1.1.1).

4.1.7.2 Actors

For more details on the actors, please refer to the previous use cases (Sections 4.1.1.2, 4.1.2.2, 4.1.3.2, 4.1.4.2, 4.1.5.2, and 4.1.6.2 respectively) as well as D5.1 [1].

Primary:

- Users;
- Service providers / Verifiers;
- Issuers;
- Revocation authorities;
- IdM platform providers.

Secondary:

- Degree verification system;
- CTI's application portal;
- Educational certification system.

4.1.7.3 Preconditions

A subscribed user wishes to de-register from the ecosystem.

4.1.7.4 Basic Flow

1. Use case begins;
2. Step 1
   The user logs into the CTI Degree Verification Portal;
3. Step 2
   The user chooses to de-register from the platform, thereby consenting to the invalidation of all her credentials;
4. Step 3
   The Degree Verification Portal revokes all credentials that have previously been issued to the user, following IDM-UC4;
5. Step 4
   The Degree Verification Portal deletes all user specific data. Where this is not possible, the user is informed about retention periods and their legal basis;
6. Use case ends.

The above flow is also illustrated in the following figure:

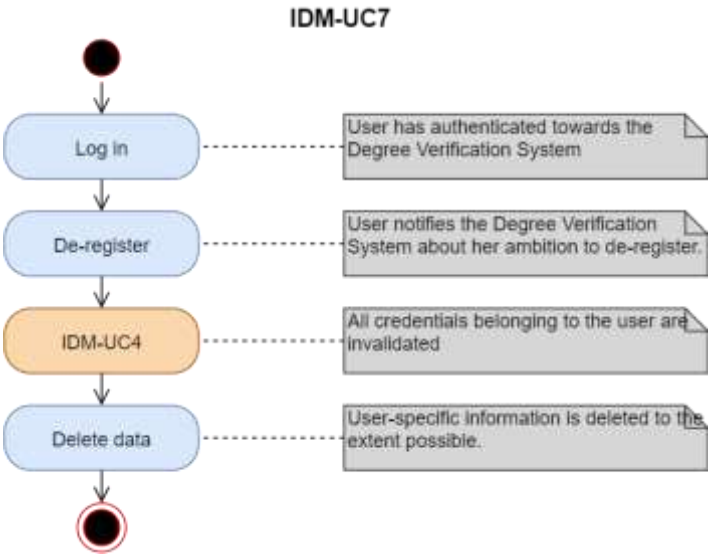

Figure 48: Privacy-Preserving Identity Management - IDM-UC7 basic flow

4.1.7.5 Postconditions

- The user has been deregistered from the system;
- All existing certificates have been invalidated;
- User-specific data has been deleted from the Degree Verification System.

4.1.7.6 Included Use Cases

IDM-UC4: Revocation

4.2 Demonstrator Set-up

Greece experienced an increase in cases where fake university degrees and diplomas were sold on the Internet without requiring the buyer to do anything but pay a fee; in particular, no academic qualification was required. In order to mitigate such fake university degrees, the demonstrator aims at providing a cryptographically secured alternative to the existing, paper-based process for certifying university degrees, passed courses, etc. Students can then later use these cryptographic tokens and present them to future employers, other universities (e.g., during exchange programs), public authorities, etc. in a way that gives high authenticity guarantees to the receiver, while still respecting the user's privacy. That is, the relying party will have cryptographic guarantees that the released information was authentic and indeed certified by an accredited university; on the other hand, the user will have full control over which information is revealed to whom. For instance, for certain scenarios it might not be necessary to release all information (e.g., when proving possession of a degree to an authority, it might not be necessary to reveal the overall grade). Furthermore, by providing digital equivalents of paper-based certificates and diplomas, usage and presentation of such degrees will be eased, while at the same time allowing for automatized verification.
While the demonstrator will be demonstrated in Greece, we note that the showcased technologies may also be used in a pan-European context, e.g., in order to de-materialize processes for students taking semesters abroad.

4.2.1 Relation to Use Cases

During the first phase of the demonstrator, the following use cases will be show-cased.

- IDM-UC1 – Registration
- IDM-UC2 – Issuance
- IDM-UC3 – Presentation

All other use-cases, in particular those depending on IDM-UC4 (Revocation), require additional developments and possibly research results from WP3 in order to be implemented efficiently.

4.2.2 Relation to WP3 Assets

In the first piloting phase, we are going to leverage the following assets from WP3:

- **Mobile pABCs.** The cryptographic technology underlying our privacy-preserving identity management solution will be based on building blocks of this primitive, especially those related to the ABC4Trust project. However, as job applications are typically not filed on mobile devices, the deployment will not involve mobile devices at this point.

For the further development of the demonstrator, several additional WP3 assets are envisioned to be included or serve as a baseline for further developments, including extensions and/or modifications to existing assets to make them suitable for our application domain. In particular:

- **SelfSovereign-PPIdM.** Using this asset, we envision to adapt self-sovereign privacy-preserving solutions in blockchains, following the outcomes of the Decentralized identity Foundation;
- **eABCs.** One potential direction for further development follows the concept of encrypted attribute-based credentials, where most of the computations can be outsourced to a cloud-service without negatively impacting the user's privacy. This might make our service more portable between devices (laptops, tablets, etc.) as less key material and credentials need to be duplicated among these devices.

4.2.3 Description and Workflow

Our demonstrator on privacy-preserving identity management will very closely follow the steps and actions that were already specified in the previous sections. That is, the relevant end points will be setup on CTI's Degree Verification Portal in order to support the issuance of digital credentials, as well as their Job Application Portal for applying for positions. Test users will be registered as described in IDM-UC1, after having consented to the participation. At the end of the pilot, all user specific data will be deleted.

4.2.3.1 High-Level Architecture

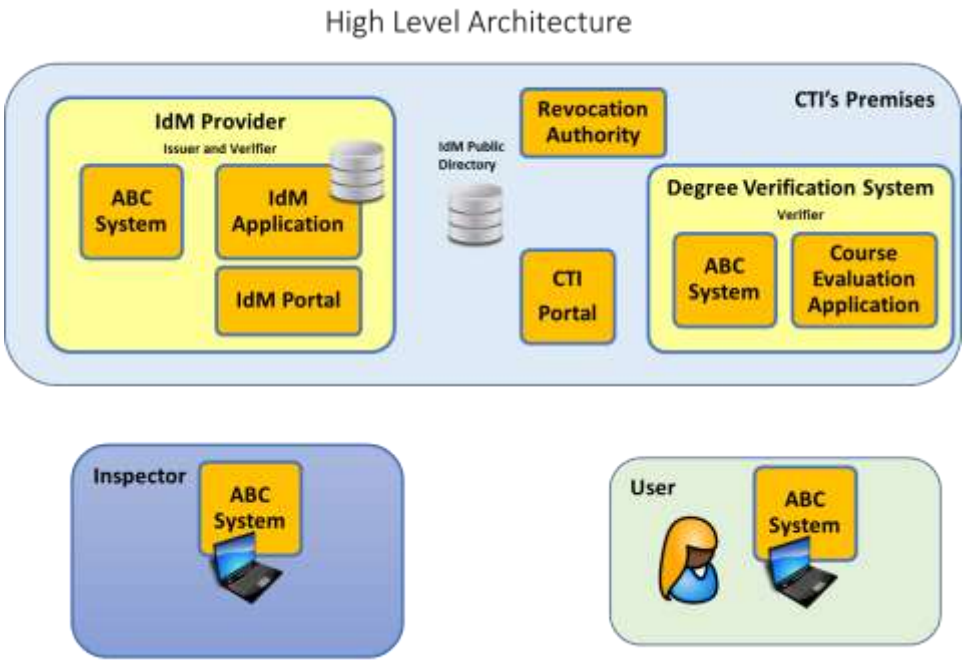

Figure 49: Privacy-Preserving Identity Management - Demonstrator's high-level architecture

As can be seen from the previous figure, the architecture of the IDM is based on various components. These components have different functionalities and roles based on the scenario and use case definition of this IDM. Next, we describe the functionality and the characteristics of each high-level component that is presented on the architecture figure. Note that the user interactions with the CTI Portal, IdM Provider and Degree Verification System are online.

CTI Portal: This component is an information web portal. Through this portal, the Users can be informed about the system's functionality and can be instructed on how to operate it. Thus, this page provides to the users the necessary links to the components of the system (e.g. Degree Verification System, Submitting Application) that are responsible for specific functionalities. Every time a user desires to interact with the system, his first action is to visit this portal and by following the instructions he can perform various operations (e.g. register, submit an application).

Degree Verification System: This component is mainly used for issuing Privacy-ABCs to the users of the system. Its sub-components are an ABC System, an IdM Application and the IdM portal.

When the IdM application is required to issue Privacy-ABCs to users (e.g. degree verification) it invokes the ABC System which is responsible for performing the issuing protocols. When a user wants to browse his personal information, the IdM application uses the IdM portal that supports this functionality.

As the Degree Verification System is the main issuer of the IdM, its parameters (system parameters, revocation information) should be stored in a public repository, so that all system components can access them. This repository is the IdM Public Directory that can be seen in the above figure.

4.2.3.2 Overview of the Software Layers

One basic software layer is the ABC engine, which is responsible for all lower layers, including handling credentials, policies etc. and if possible given the users credentials, providing access tokens fulfilling the requested policies. The User Client is supplying a user interface, making the user capable of choosing between

different credentials if more than one fulfils the requested policy. An overview of the can be seen below in Figure 50.

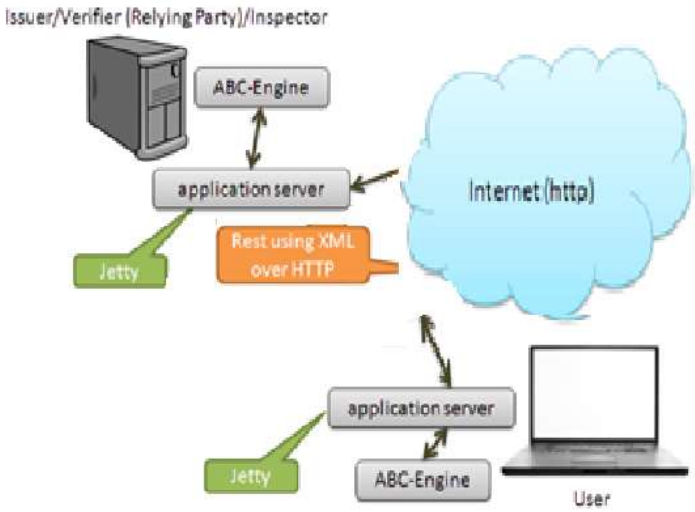

Figure 50: Privacy-Preserving Identity Management - Overview of the demonstrator's software layers

The ABC engine is implemented as a set of web components executed locally on the user's computer, using the Jetty webserver installed locally. For a description of the internal functionality of the ABC Engine.

The user side software is packed in on installable package including the Jetty server, the ABC engine, the user application and the Firefox plugin. The requirements for the installation: Firefox and Java 1.6.

4.2.3.3 Application Overview

The IdM provider runs on an Ubuntu Linux system, an open source operating system distributed under the GNU General Public License. The ABC Engine itself and IBM's Crypto-Engine are java-based applications, which can easily run in a Linux environment. The host 'idm.cti.gr' runs on a 32-bit Ubuntu Linux system.

Figure 51 presents an Application Overview of IdM provider.

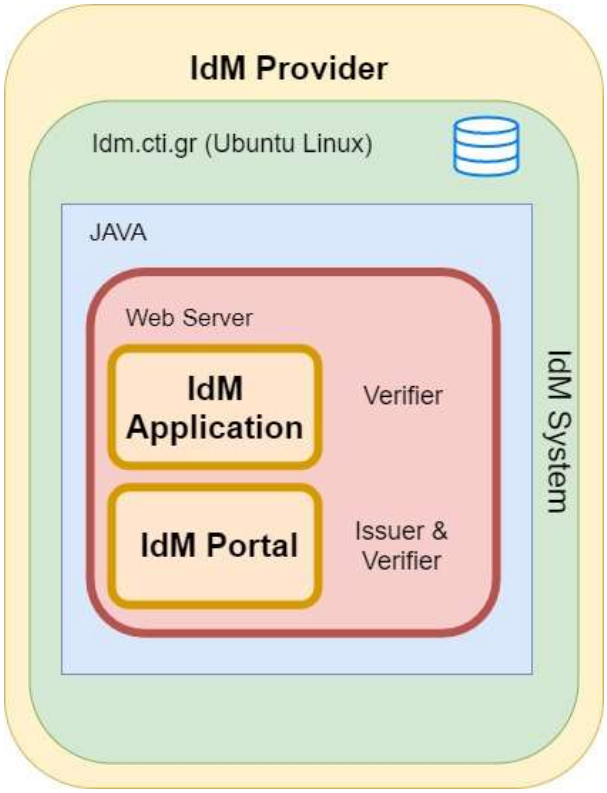

Figure 51: Privacy-Preserving Identity Management - Application overview of the IdM provider

4.2.4 Target Group

The first piloting round of this demonstrator will be hosted by CTI. Therefore, university students from the University of Patras, Greece, will be invited to test and evaluate the system. In order for representative feedback, a sufficiently large number of students will be included, and we will aim at a representative balance regarding age, gender, and IT-related background. On the issuer and verifier side, personnel from CTI will be in charge to also evaluate the relevant processes.

We want to stress that even though CTI is responsible for hosting the system and also acts as a data consumer, these will be disjoint groups of users with distinct responsibilities within CTI (IT Services and Human Resources), such that representative feedback from all relevant types of actors can be collected.

Besides the plain pilot execution, we plan to make the results available also to a wider public, and in particular to related initiatives.

5 Incident Reporting in the Financial Sector

In this section it is described the use cases related to the demonstration case for creating a smart incident reporting platform to address the common need for standardized and coordinated cybersecurity notification in case of significant cyber and operative incidents. This demonstrator will also tackle the lack of harmonization in the EU mandatory incident reporting process, which results from the different requirements defined by each supervisory authority at both, EU and national levels [2]. The demonstrator would pave the way towards public and private cooperation towards reaching the common goal of enhancing cyber resilience not only across Europe but also beyond the EU borders.

As it was described in D5.1, the current EU legal framework foresees the need "to comply with Mandatory Incident Reporting to different Supervisory Authorities respecting the relevant impact assessment criteria and thresholds, timing, data set, communication means as defined by each authority both at EU and national level. All these different criteria and patterns cause fragmentation into the overall incident reporting process and are to be managed along the critical path of managing the incident itself. These mandatory reporting requirements are particularly strong in the financial market. For instance, when a cyber incident impacts a multinational Financial Group, there is also the additional need for each entity impacted to eventually report to the National Competent Authority, and for the Parent Company Headquarter to gather all the information in a standardized way from each legal entity in order to assess the overall impact at Group level" [1].

5.1 Use Cases Specification

5.1.1 Use case IR-UC1: Data Collection, Enrichment, and Classification

Use case IR-UC1 begins with the Data Collection phase, which consists of gathering data regarding an incident detected in the entity, the enrichment of the data that has been gathered, and the event classification. These three steps aim at defining and quantifying the incident.

The EU Mandatory Incident Reporting regulatory requirements for financial sector considered in this first phase of development of the demonstrator are:

- Incident reporting according to the requirements established by the PSD2;[27]
- Incident reporting according to the requirements established by the ECB/SSM framework.[28]

In the second phase of development of the demonstrator, the scope will be extended to include other regulatory frameworks and/or additional or updated regulatory requirements, such as the GDPR, the NIS Directive, Target2, and eIDAS. Beyond the end of the project, the scope could be further extended to cover also the incident reporting requirements of other business sectors.

Figure 52 shows the UML use case diagram for the IR-UC1 that will be described with more detail in the next subsections.

[27] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

[28] European Central Bank (ECB), https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

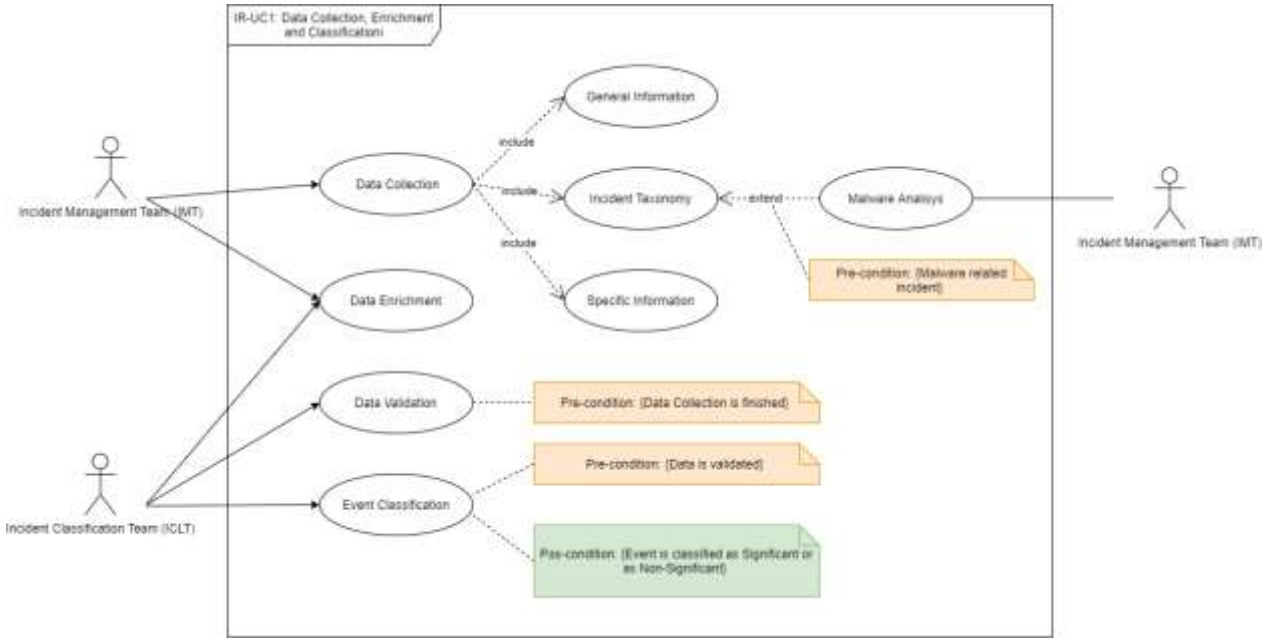

Figure 52: Incident Reporting – IR-UC1 Data Collection, Enrichment, and Classification Use Case Diagram

5.1.1.1 Stakeholders

Concerning the financial sector, the main stakeholders potentially involved in the first phase of development of the demonstrator are the ones already identified in section 7.3 of D4.3 [2]. We reproduce here the stakeholders described in that deliverable:

- **Financial Institutions**: financial institutions are subject to many regulations and frameworks that require mandatory incident reporting to several supervisory authorities and/or international financial market infrastructures, according to specific procedures and utilizing different templates. Within the financial market, mandatory incident reporting requirements apply to:
    - **Significant Institutions** (ECB SSM): The ECB classifies banks as significant or not significant based on the following criteria: size, economic importance, cross-border activities and direct public financial assistance.
    - **Payment Service Providers** (PSD2): Financial institutions operating as payment service providers (PSPs).
- **Regulators:** European or national legislative entities responsible for proposing and adopting the laws that regulate the functioning of specific areas of activity. At the European level, the main regulators are the European Commission, the European Parliament, and the Council of the European Union, as well as, for the financial sector, the European Central Bank (ECB). At the national level, the main regulators are national Parliaments. For the financial sector, national Central Banks and Securities Commissions (e.g., the Italian Consob) are entitled to define rules and guidelines applicable to national financial institutions.
- **EU/National Supervisory Authorities**: Entities responsible for direct supervision under EU normative or national transposition laws and regulations. The responsible authorities are defined at EU or at national level and will be the recipients of the corresponding mandatory incident reports. Each regulation defines one or more corresponding authorities and additional mandatory incident reporting requirements, such as the obligation to notify a national authority in addition to the EU authority specified in the EU law. The EU/National Supervisory Authorities foreseen in the first phase are:

- **PSD2**: National Central Authority (NCA)/European Central Bank (ECB)/European Banking Authority (EBA)
- **ECB/SSM**: ECB/Joint Supervisory Team

In a wider perspective, other stakeholders that might benefit from an automated process of incident reporting and an enhanced cooperative approach to information sharing are:

- **European Union agencies**
  - **ENISA**: ENISA supports Member States and European Union stakeholders in their response to large-scale cyber incidents that take place across borders, in cases where two or more EU Member States have been affected. Moreover, it also supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.
- **Law-enforcement agencies**
  - **Europol**: the Europol, in particular through the European Cybercrime Centre (EC3), strengthens the law enforcement response to cybercrime in the EU and helps to protect European citizens, businesses and governments from online crime also by leveraging the information voluntarily shared by the private sector.

European citizens: in a wider long-term perspective, the final beneficiaries of the deployment of smart incident reporting tools are the European citizens. They will indirectly benefit from enhanced resilience and security in the Digital Single Market, resulting from the increased information sharing on cyber vulnerabilities and threats.

5.1.1.2 Actors

External Providers are subjects contractually engaged with the entity. Sometimes external providers can intercept and refer occurrences of events potentially dangerous for the entity, because they become aware beforehand of some vulnerability related to their solutions or services they provide to the entity. They do not have direct access to the Incident Reporting Platform.

The Impacted or involved business office/function is an internal organizational units that can intercept and refer occurrences of events potentially dangerous for the entity. These units carry out a first screening of the event occurred and determine if it is a false positive, or if it is an issue that needs to be further analysed by specific agents appointed (Asset Owner / Incident Management Team). They do not have direct access to the Incident Reporting Platform.

The Asset Owner / Incident Management Team (IMT) is/are appointed operator/s of the internal organizational unit affected by the potentially dangerous event. They are in charge of carrying out a more detailed analysis in order to determine the necessity of the opening of an incident in the application or if it is an issue that can be solved internally. In case of an incident, the Asset Owner / Incident Management Team is responsible for the opening of the incident and for the collection of the main information related to the incident itself.

The Incident Classification Team (ICLT) is the internal organizational unit responsible for classifying all the incidents opened by the Asset Owners / Incident Management Teams. This includes the identification of the type of incident, the perimeter extension, the estimation of the economic impact. The result of the classification determines if the incident can be managed by the unit until its closure or if an escalation process is needed and if Mandatory Incident Reporting would be applicable.

An **Administrator** oversees the customization of the Incident Reporting Platform to adapt it to the particular needs of a FI or a given market. The Administrator shall create the user profiles providing the appropriate permissions that correspond to the scope of their functions. The Administrator is the demonstrator supervisor from the IT perspective.

Subject to the dynamic effects related to the incident and considering its extent, impact, and severity, an escalation process could be activated. The **Emergency & Crisis Management** is the internal organizational unit in charge of the management and reporting of the incident that has been classified as emergency or crisis since the beginning or during its lifetime. It must monitor the emergency/crisis and report its evolution to the competent authorities. In case of a crisis, a **Crisis Committee** is involved and is responsible for the official communication of the crisis status that could entail specific procedures towards the Supervisory Authority.

The actors directly involved in this use case are the following:

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

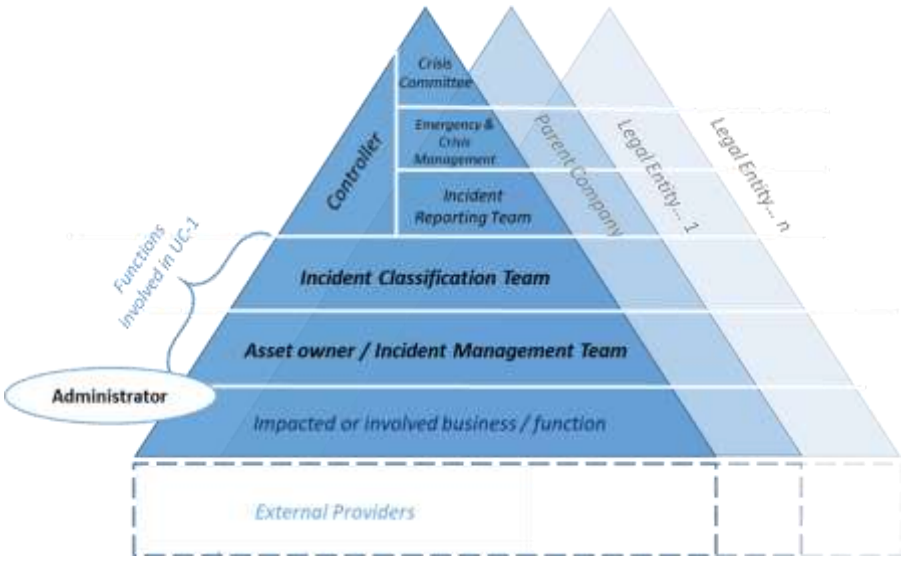

Figure 53: Incident Reporting - Actors involved in use case IR-UC1

5.1.1.3 Preconditions

We assume the security incident has occurred in a financial institution that has registered itself as a **Significant Institution** in the Incident Reporting Platform and is operating as a **Payment Service Provider** (PSP). Under ECB-SSM (Cyber Incident reporting Framework for Significant Banks) Framework if only one threshold has been reached, an Incident Report to the ECB is required. If the incident has occurred in a subsidiary or branch of the Group, the impact of the event has to be evaluated on a consolidated basis. The requirements established under the PSD2 cover financial institutions operating as Payment Service Providers.

The following components need to be enabled before the execution of this Use Case:

- TheHive[29] incident management and response open source software;
- HADES (Automatic analysis of malware samples) to analyse malware samples and perform the event

[29] https://thehive-project.org/

classification and event severity suggestion of the detected malware;

- AIRE Incident Reporting Engine designed to manage the incident reporting workflow and the collection of general information required for the configuration of the mandatory reporting;
- TheHive Responder for Dummy Incident Reporting Event Classifier: since currently there is no WP3 asset or open source application capable of classifying the security incident and calculating the severity of its impact for the purpose of mandatory incident reporting according to the regulatory requirements, a dummy asset will be provisionally included to be invoked from TheHive tool. This dummy asset will simulate the classification and the impact severity calculation for the specific test scenarios defined for the demonstrator. In case the incident is classified as "Significant", it will suggest the need for mandatory Incident Reporting as well as the Competent Authorities that need to be notified.

Using the demonstrator's GUI, the Administrator will register all the information related to the Entities involved in the incident (including the data about the Contacts and any other relevant information required for the mandatory reporting), as well as the users that can log in to the platform with their function, position, and permissions assigned.

The Administrator should also map and configure the criteria and thresholds necessary for the classification of the incidents into the demonstrator in an initial pre-configuration phase, ideally as soon as an entity starts using the demonstrator for Mandatory Incident Reporting purposes. In a later phase of development of the tool, the Administrator should be able to update the criteria and thresholds established by the Mandatory Incident Reporting normative requirements whenever necessary. However, this criteria and thresholds configuration step will be skipped in the demonstrator since there is no WP3 asset implementing this functionality. Consequently, all the criteria and thresholds illustrated below will not be included in the demonstration case and are included here just for completeness purposes. Only those ones required for validation purposes will be implemented in the dummy TheHive Responder for Incident Reporting Event Classifier and used by the demonstrator.

Under the ECB-SSM Cyber Incident Reporting Framework, all financial institutions from the 19 euro area countries identified as "Significant institutions" have to report "Significant" cyber incidents. The classification of whether a cyber incident is significant or not for reporting purposes is to be carried out by the institution itself on a consolidated basis, based on reaching one or more of the minimum thresholds as defined by the ECB.

If a cyber incident occurs, then the institution should assess the materiality of the incident on a consolidated basis, using the following criteria defined by the ECB:

- Threshold 1: Reputational impact;
- Threshold 2: Financial impact;
- Threshold 3: Internal Escalation;
- Threshold 4: Regulatory Compliance;
- Threshold 5: Crisis management;
- Threshold 6: External reporting;
- Threshold 7: Additional Criteria.

The following thresholds are relevant to evaluate the need for mandatory reporting under the PSD2 (Payment Service Directive 2) Framework. The thresholds shall be mapped and duly updated in advance by the Administrator in order to support the reporting under the PSD2 Framework.

Article 96 (1) of the PSD2 establishes that "In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the

payment service provider".[30] In addition, "Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident".[31]

The EBA Guidelines on major incident reporting under PSD2[32] specify the criteria for the classification of "Major" operational or security incidents by payment service providers: "*Payment service providers should classify as major those operational or security incidents that fulfil:*

- *one or more criteria at the 'Higher impact level'; or*
- *three or more criteria at the 'Lower impact level'*"[33].

The criteria and their thresholds are listed in the table below, provided by EBA Guidelines on major incident reporting under PSD2.

Thresholds	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **and** > EUR 100 000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 5 million
Payment service users affected	> 5 000 **and** > 10% of the payment service provider's payment service users	> 50 000 **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital, EUR 200 000) **or** > EUR 5 million
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

Table 1: Incident Reporting - Criteria for the classification of security incidents (source: EBA Guidelines on major incident reporting under PSD2, page 23)

Table 2: Incident Reporting - Criteria for the classification of security incidents (source: EBA Guidelines on major incident reporting under PSD2, page 23)

[30] DIRECTIVE (EU) 2015/2366, Art. 96(1)
[31] Ibid.
[32] European Banking Authority (EBA), Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)
[33] Ibid.

Both the ECB-SSM and the PSD2 Mandatory Incident Reporting requirements foresee 3 types of reports for each incident classified as "Significant" or "Major":

- a **First Report** requiring information regarding the impacted entity or entities and an initial description of the event. According to the requirements established in the ECB-SSM framework, the First Report must be sent within 2 hours of the cyber incident being classified as "Significant"; According to the requirements established by the PSD2, "the First Report must be sent within 4 hours from the moment the major operational or security incident was first detected".
- one or more **Intermediate (or Interim) Report(s)** requiring more detailed information about the event and its consequences in terms of e.g., economic impact, payment services affected, or the extent of the media coverage. If detailed information about the incident is not yet available, the affected entity can provide some estimates instead. The information provided in the Intermediate Report(s) can be updated and enhanced in the Final Report. According to the requirements established in the ECB-SSM framework, an Interim Report is required within 10 working days of submitting the first report; According to the requirements established by the PSD2, entities must submit Intermediate Reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report (either the Initial Report or the previous Intermediate Report, within a maximum of 3 days).
- a **Final Report** requiring detailed and updated information about the incident, such as the root cause of the event and a more accurate description. According to the requirements established in the ECB-SSM framework, the final report is required within 20 working days of the interim report; According to the requirements established by the PSD2, the final report must be sent within a maximum of 2 weeks after a business is deemed back to normal.

Following a Significant or Major Incident, the First and the Final Report are always mandatory, whereas the Interim Report can be omitted when the incident is resolved or re-classified as "not significant" before sending the Intermediate Report.

Given the obligations and timing requirements described above, entities impacted by significant or major incidents are required to gather information, update it, and fill in all the required fields several times during the reporting process and the management of the incident, in order to compile and send all the necessary reports. For this reason, the flow of operations that are included in the three Use Cases can recur multiple times, according to the characteristics of the incident being reported. In the demonstration case for phase 1, we will focus only on the generation of the First Report.

5.1.1.4 Basic Flow

1. Use case begins: Event 1
   The Asset Owner/Incident Management Team (IMT) receives a notification about an incident detected in the financial institution by the impacted or involved business/function, or by an external provider.

2. Event 2
   All the information required in the "Data Collection" phase should be gathered by the Asset Owner / Incident Management Team. First, the user belonging to the IMT needs to have been previously registered in the incident reporting platform by the Administrator. The information required in the First Report includes, for instance, the name of the affected entity and the details about its location. The Asset Owner / Incident Management Team (IMT) fills in all the general information related to the incident detected in the financial institution using a questionnaire through the platform's GUI**.** For the First Report, only a preliminary description of the event is mandatory.

3. Event 3
   In the case of a malware incident, the Asset Owner / Incident Management Team (IMT) will use the

HADES component to analyse the malware sample under suspicion, identifying the causes that generated the incident and its impacts on the financial institutions (incident severity). This component will provide the data necessary to complete the description of the incident for the classification of the incident.

4. Event 4
   Once the Incident Management Team has completed its tasks – the collection and filling in of all the information about the incident – the Incident Classification Team (ICLT) validates the information provided and continues with the categorization and identification of the cause that generated the incident. Should additional information regarding the incident become available during this phase, the Incident Classification Team will enrich the data already gathered by the IMT.
5. Event 5
   Once all the available information has been gathered and filled in, the demonstrator will proceed with the classification of the security event based on the gathered data and on the ground of the thresholds established by the Mandatory Incident Reporting framework. The classification of the incident should be done by a dedicated Incident Classification asset (currently unavailable). Due to the unavailability of this component, however, the functionality will be provisionally simulated by a dummy asset that will be manually invoked by a user of the Incident Classification Team (ICLT) from TheHive's GUI.
6. Use case ends.

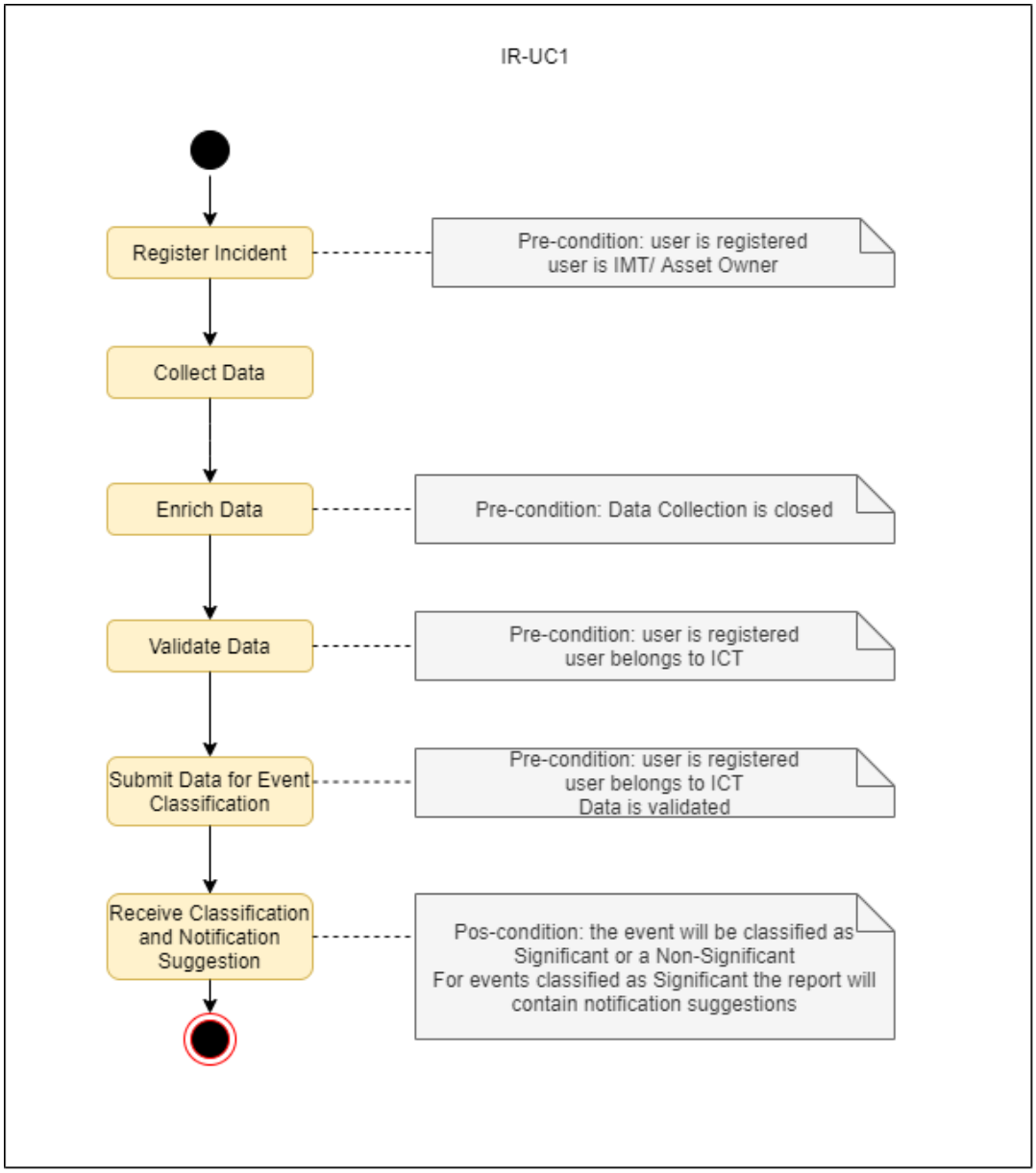

Figure 54: Incident Reporting - IR-UC1 Basic Flow

5.1.1.5 Postconditions

Following the end of use case IR-UC1, the demonstrator should classify the incident either “Significant” or “Not Significant”.

If the demonstrator classifies the incident as “Not Significant”, the incident will be stored in the incident register and no report will be required.

If the demonstrator classifies the incident as “Significant”, this will be notified to the Controller for confirmation and use case IR-UC2 will begin.

5.1.2 Use Case IR-UC2: Managerial Judgement

The goal of this Use Case is to introduce a human decision-making stage in the demonstrator’s Incident Classification and the Mandatory Incident Reporting process in order to guarantee an appropriate level of

quality of the reports and to prevent accidental or inaccurate reporting. Through the Managerial Judgement, the Controller can confirm or reject the result of the incident classification as well as the suggestion regarding to which authorities the reports must be submitted.

Figure 55 shows the UML use case diagram for the IR-UC2 that will be described with more details in the next subsections.

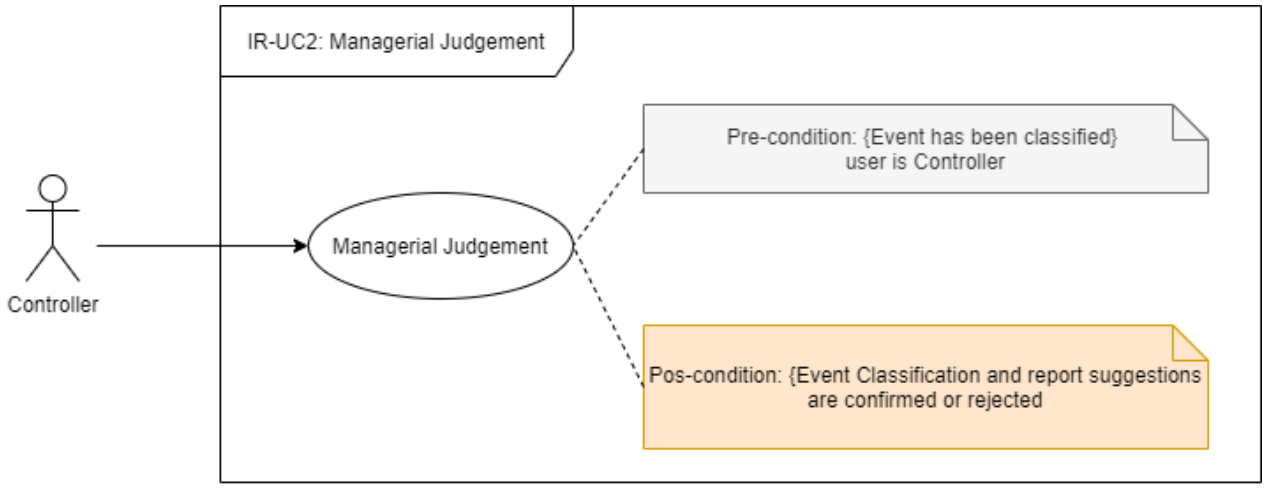

Figure 55: Incident Reporting – IR-UC2 Managerial Judgement Use Case Diagram

5.1.2.1 Stakeholders

This use case foresees the involvement of the same stakeholders involved in use case IR-UC1.

5.1.2.2 Actors

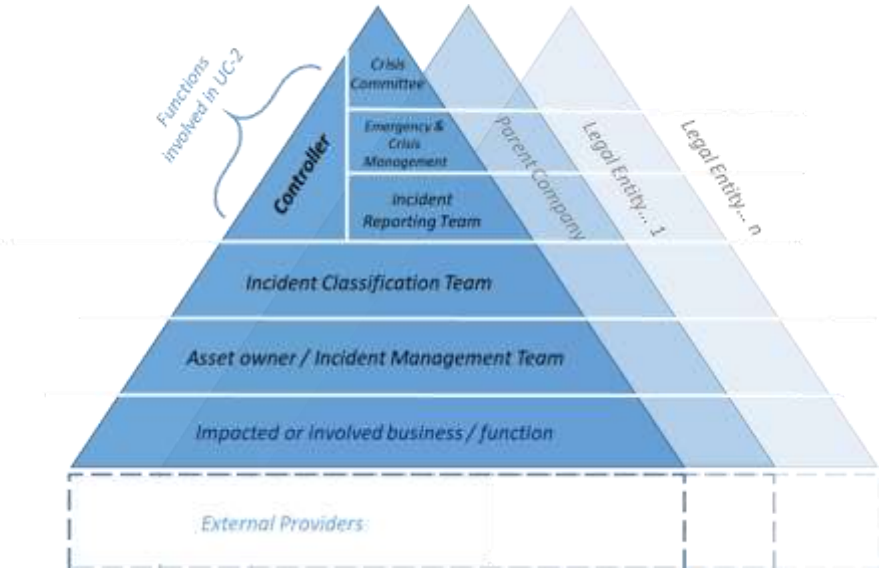

Figure 56: Incident Reporting - Actors involved in use case IR-UC2

Controller: This actor must perform the Managerial Judgement on the Incident Reporting suggestions given by the Incident Reporting Platform, which are the result of the analysis the Platform carries out on the information about the incident the IMT and the IRT provided. Through the Managerial Judgement, the

Controller gives the authorisation to proceed with the reporting process. The Controller is also the actor that authorizes the release of the report(s) that the Incident Reporting Platform has produced, in their appropriate templates, to the competent Authority/Authorities. Finally, the Controller oversees the whole incident reporting process from Classification to Reporting, and eventually manages the escalation to the Emergency and Crisis Management.

Subject to the dynamic effects related to the incident and considering its extent, impact, and severity, an escalation process could be activated. **The Emergency & Crisis Management** is the internal organizational unit in charge of the management and reporting of the incident that has been classified as emergency or crisis since the beginning or during its lifetime. It must monitor the emergency/crisis and report its evolution to the competent authorities. In case of a crisis, a **Crisis Committee** is involved and is responsible for the official communication of the crisis status that could entail specific procedures towards the Supervisory Authority.

The Controller is the actor normally involved in this use case.

5.1.2.3 Preconditions

The same preconditions of use case IR-UC1 apply to use case IR-UC2.

The following CyberSec4Europe components need to be enabled prior to the execution of this use case:

- TheHive incident management and response open source tool;
- AIRE Incident Reporting Engine to manage the incident reporting workflow. In addition, the incident must have been classified by the demonstrator following the Data Collection, Data Enrichment , and Incident Classification use case (IR-UC1).

5.1.2.4 Basic Flow

1. Use case begins: Event 1
   The Controller, based on the experience gained, the specificities of the incident and further considerations made, may confirm or reject the classification of the demonstrator, and thus confirm or not the need for Incident Reporting suggested by the Incident Reporting demonstrator. In case of rejection, the Controller must clearly specify the reasons that justify the choice. Every decision taken by the Controller shall be recorded in the logs register of the demonstrator for accountability purposes, including the reasons that justify the rejection of the incident classification.
2. Event 2
   The most appropriate action plan to be implemented to handle and respond to the incident will be determined according to the assigned Severity judgement (see Postconditions).
3. Use case ends.

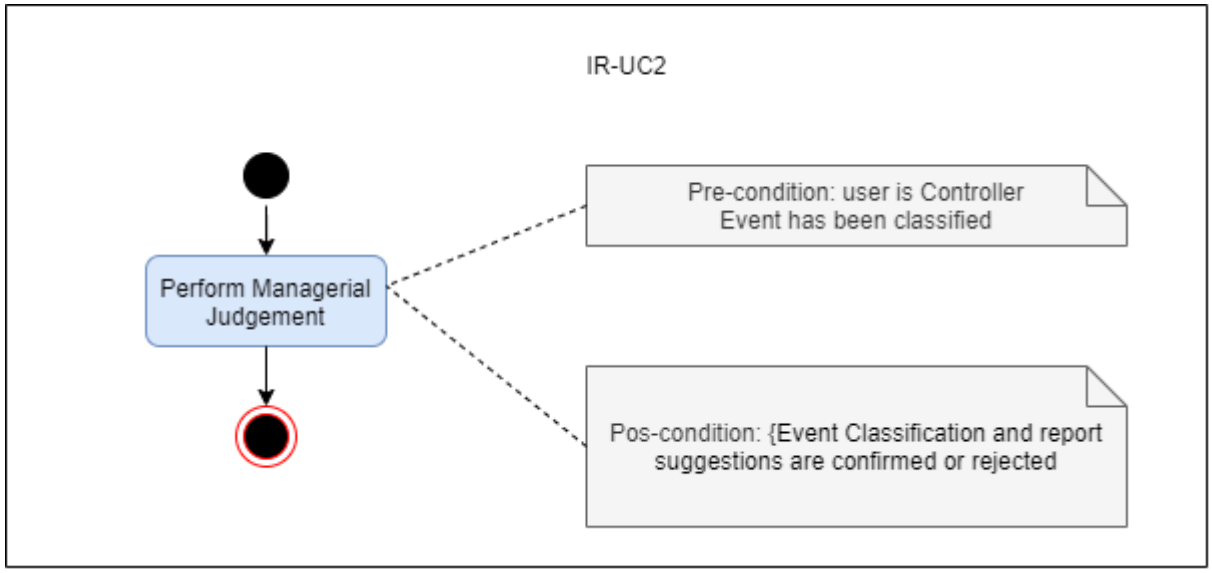

Figure 57: Incident Reporting - IR-UC2 Basic Flow

5.1.2.5 Postconditions

Based on the result of the Managerial Judgement, one of the following circumstances may occur:

1) The demonstrator classified the incident as **Not Significant** and the **Controller confirmed**:
    a. For a newly opened incident, the incident is closed and stored in a designated incident register. The incident does not need to be reported and no further action is required; or
    b. For an incident that has already been reported (in an Intermediate Report and/or in a First Report) and has now been re-classified as Not Significant: the reclassified incident must be reported to the same recipients by sending a Final Report containing the reasons for the re-classification in the designated field, thus proceeding to use case IR-UC3; This situation will not be implemented during phase 1.
2) The demonstrator classified the incident as **Not Significant** and the **Controller rejected** the classification:
    a. The incident must be sent back to the IMT and the ICLT to be re-analysed, thus restarting use case IR-UC1; or
    b. The Controller may decide to report the incident anyway, thus proceeding to use case IR-UC3;
3) The demonstrator classified the incident as **Significant** and the **Controller rejected** the classification:
    a. The incident can be sent back to the IMT and the ICLT to be re-analysed, thus restarting use case IR-UC1, for instance, when a mistake was committed during the Data Collection or the Data Enrichment phases; or
    b. If the incident has already been reported (in an Intermediate Report and/or in a First Report), it can now be re-classified as Not Significant: the re-classified incident must be reported to the same recipients by sending a Final Report containing the reasons for the reclassification in the designated field, thus proceeding to use case IR-UC3; this case will not be implemented during phase 1.

The demonstrator classified the incident as **Significant** and the **Controller confirmed** the classification: the incident must be reported to the Competent Authorities, thus use case IR-UC3 will begin.

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

Use case IR-UC3 consists of the conversion of the data gathered during use case IR-UC1 into the appropriate format or template required by the recipients of the reports. The demonstrator will perform the conversion only after confirmation in the Managerial Judgement and based on the data filled in during the Data Collection and/or Enrichment phases.

When preparing the First Report, the demonstrator will include only data that is mandatory for that report, while also giving the possibility to include other data that is normally mandatory starting from the Intermediate Report. While preparing the Intermediate or Final Report (not included in the demonstrator for phase 1), the demonstrator will include all available data in the appropriate format or template required by the recipients of the reports.

Figure 58 shows the UML use case diagram, which will be described with more details in the next subsections.

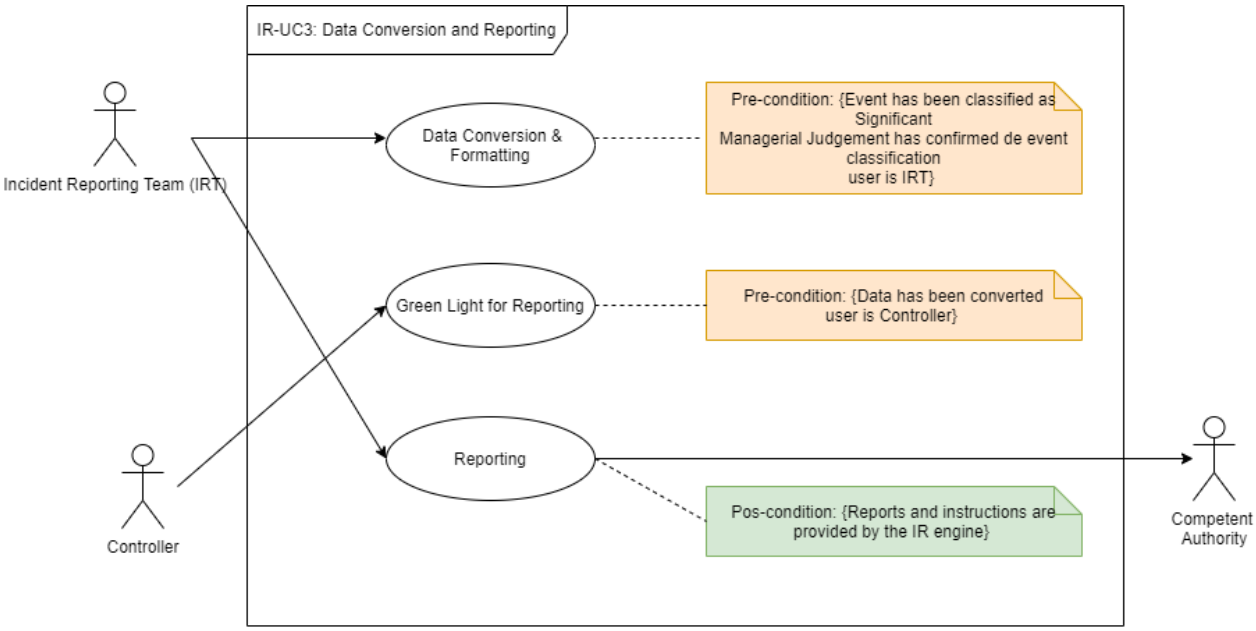

Figure 58: Incident Reporting - IR-UC3 Data Conversion and Reporting Use Case Diagram

5.1.3.1 Stakeholders

This use case foresees the involvement of the same stakeholders of use cases IR-UC1 and IR-UC2.

5.1.3.2 Actors

Incident Reporting Team (IRT): This actor must continuously monitor the evolution of the incident and, upon Controller authorization, needs to carry out the reporting processes to competent authorities until the closure of the incident, according to relevant regulation timelines. This actor can also be in charge of internal incident reporting, communication, and coordination.

Controller: This actor must perform the Managerial Judgement on the Incident Reporting suggestions given by the Incident Reporting Platform, which are the result of the analysis the Platform carries out on the information about the incident the IMT and the IRT provided. Through the Managerial Judgement, the Controller gives the authorisation to proceed with the reporting process. The Controller is also the actor that authorizes the release of the report(s) that the Incident Reporting Platform has produced, in their appropriate templates, to the competent Authority/Authorities. Finally, the Controller oversees the whole incident reporting

process from Classification to Reporting, and eventually manages the escalation to the Emergency and Crisis Management.

Subject to the dynamic effects related to the incident and considering its extent, impact, and severity, an escalation process could be activated. **The Emergency & Crisis Management** is the internal organizational unit in charge of the management and reporting of the incident that has been classified as emergency or crisis since the beginning or during its lifetime. It must monitor the emergency/crisis and report its evolution to the competent authorities. In case of a crisis, a **Crisis Committee** is involved and is responsible for the official communication of the crisis status that could entail specific procedures towards the Supervisory Authority.

The actors normally involved in this use case are the following:

- The Controller;
- The Incident Reporting Team (IRT).

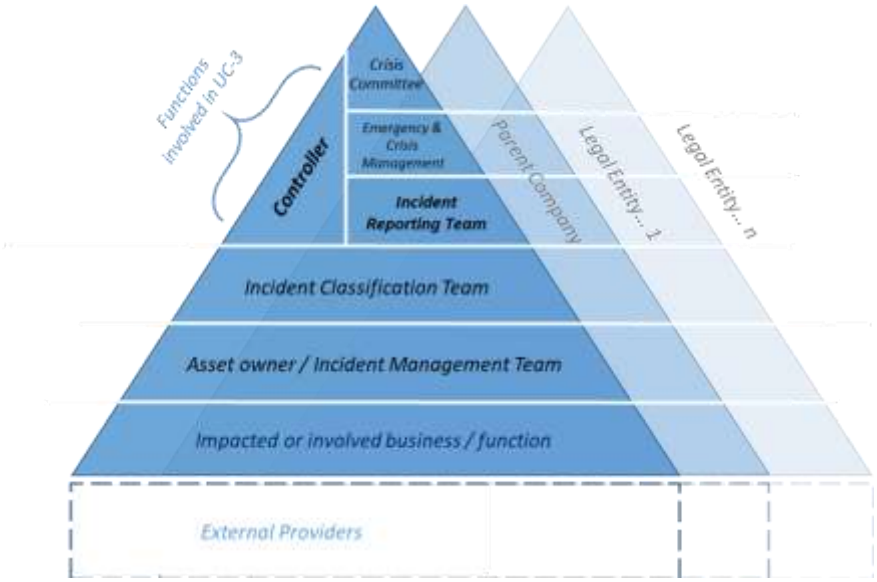

Figure 59: Incident Reporting - Actors involved in use case IR-UC3

5.1.3.3 Preconditions

The same preconditions of use cases IR-UC1 and IR-UC2 apply to this use case.

The following CyberSec4Europe components need to be enabled prior to the execution of this use case:

- TheHive Incident Management and Reporting open source tool
- AIRE Incident Reporting Engine to manage the incident reporting workflow and preparation of the report.

In addition, prior to the beginning of this use case, the event must have been classified as Significant and the Controller must have confirmed the classification and the reporting suggestion given by the demonstrator.

5.1.3.4 Basic Flow

- Use Case begins: Event 1
  Based on the information collected, the classification of the incident, and following the Controller's confirmation in the Managerial Judgement, the demonstrator shall appropriately convert all the available information into the appropriate template/communication(s). The conversion will be

performed by the **Incident Reporting Engine component** according to the requirements established by the regulators, as illustrated in the description of this Use Case.

- Event 2
  After a final authorization ("green light") given by the Controller, the Incident Reporting Team will manually send the report(s) produced by the demonstrator to the Competent Authority/Authorities. The demonstrator will suggest sending instructions to the user (email of the recipient, encryption measures, etc.).
- Use case ends
  After being sent to the Competent Authorities, the report(s) is/are stored in an Incident Register database along with the logs of the incident lifecycle.

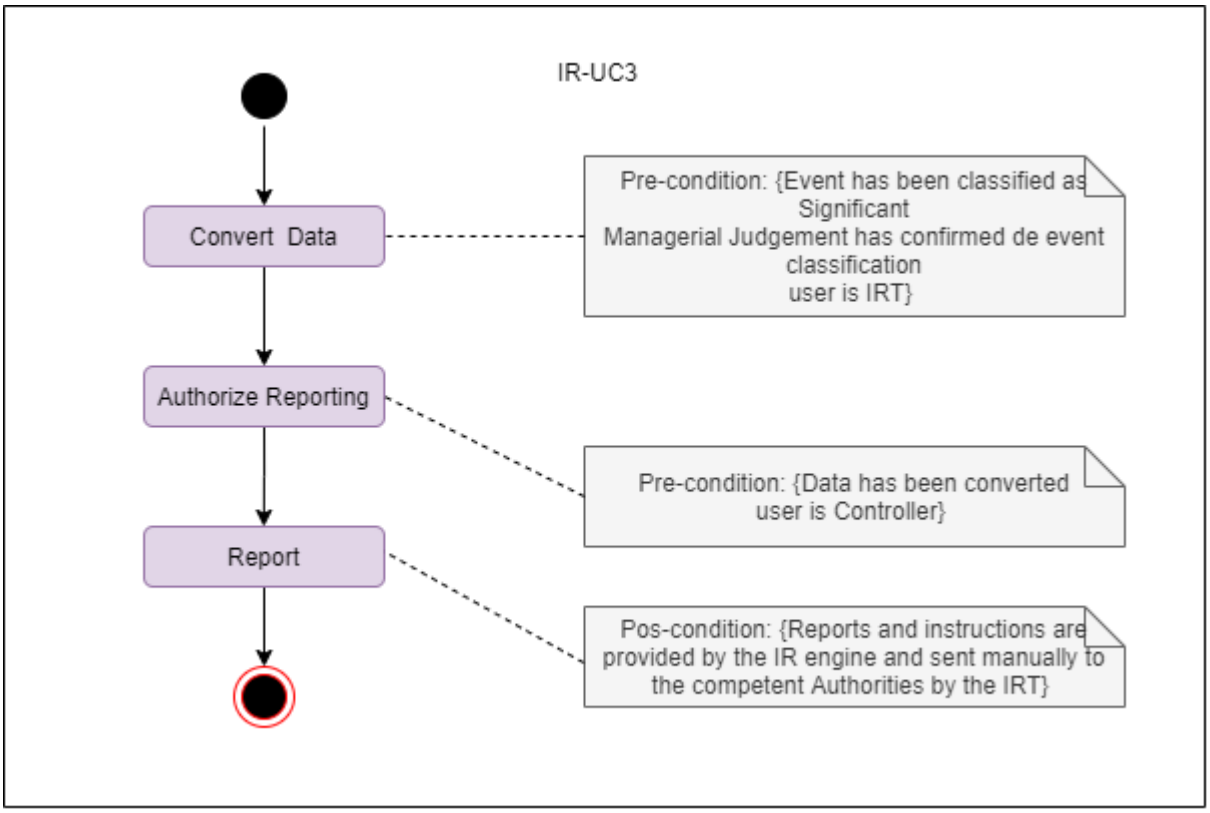

Figure 60: Incident Reporting - IR-UC3 Basic Flow

5.1.3.5 Alternate Flows

- Event 1
  If the First Report has already been sent and the incident is not yet resolved, an Intermediate (or Interim) report towards the Competent Authorities containing more detailed information about the incident is required. The Data Enrichment is carried out by the Incident Classification Team, which will gather and fill in the details regarding, e.g., the cause of the incident, the number of affected transactions (in case of an incident involving payment services), and the economic impact.
- Event 2
  In the case of a malware incident, the Asset Owner / Incident Management Team (IMT) will use the HADES component to analyse the malware sample under suspicion, identifying the causes that generated the incident and its impacts on the financial institutions (incident severity). This component will provide the data necessary for the classification of the incident.

- Event 3
  Once all the available information has been gathered and filled in, the demonstrator will proceed with the classification of the event based on the gathered data and on the ground of the thresholds established by the Mandatory Incident Reporting framework. The classification of the incident will be done by a dedicated Incident Classification asset (currently unavailable). Due to the unavailability of this component, however, the functionality will be provisionally simulated by a dummy asset.

- Use case ends.

5.1.3.6 Postconditions

The flow of operations described in use cases IR-UC1, IR-UC2, and IR-UC3 repeats itself in a cyclical order each time an incident needs to be analysed and to be reported (First, Intermediate, or Final Reports).
Each time a report is sent, it will be stored in the Incident Repository along with the information regarding the incident lifecycle, the outcome of the Managerial Judgement and, should the latter result in a rejection of the classification of the incident, the motivations that led to that decision. The demonstrator in phase 1 will focus only on the generation of the First Report.

5.2 Demonstrator Set-up

The demonstrator for Mandatory Incident Reporting aims at filling the gap left by the absence of a common methodology and an automated tool in the mandatory cyber and operative incident reporting process. The demonstrator will offer a simple way to report significant security incidents through a user-friendly graphical interface.

The Incident Reporting Smart Engine demonstrator will provide support to the different actors of the financial institutions that participate in the mandatory incident reporting process (in particular, the members of the Incident Management Team, the Incident Classification Team, The Controller and the Incident Reporting Team) enabling them to perform their tasks more easily and effectively. Through its user-friendly graphical interface, the demonstrator will cover the different steps of the incident reporting and event management workflow, from the collection of all the information about the incident to the generation of the mandatory reports requested by the Competent Authorities by the 4-eyes principle described in Deliverable D5.1 [1].

5.2.1 Relation to Use Cases

The demonstrator will implement all three use cases since they are all required in the mandatory incident reporting process. The first phase of development will see the deployment of use case IR-UC1, save for the Incident Classification and reporting suggestion functionalities that are currently uncovered. Use cases IR-UC2 and IR-UC3 will be integrated into the second phase of development.

5.2.2 Relation to WP3 Assets

To cover the requirements listed in Deliverable D5.1 [1] and to enforce the workflow described above, the demonstrator will integrate open source tools and a set of components currently developed by WP3. In particular, the following WP3 assets will be integrated in the Incident Reporting demonstrator during the first phase of the development:

- **Automatic Analysis of Malware Samples (HADES)**
  The asset HADES will be included in the context of the Incident Reporting demonstration case as an analyser that can be invoked by the members of the Incident Management Team from the incident

reporting platform when they are performing the collection of all the main information about a security incident to determine the necessity of opening an incident in the reporting platform. In particular, and since HADES is a platform for the orchestration of sandboxes for malware execution, in the demonstration case it has been assumed that the security incident is related to a potential malware detected in the infrastructure of a financial institution. Consequently, a malware sample file will be sent to HADES from the incident reporting platform and a report will be returned by this asset with the result of the analysis carried out.

- **ATOS Incident Reporting Engine (AIRE)**

  The asset AIRE will be included in the Incident Reporting demonstration case to cover the requirements related to incident reporting workflow enforcement, data conversion and reporting preparation. Through the integration with an incident and response management tool (in particular, with the open source tool TheHive),[34] this asset will enforce the different steps in the incident reporting process ensuring a Controller performs the Managerial Judgement (once done the incident classification by the Incident Classification Team) in order to proceed with the preparation of the templates containing the information to be reported. This asset will also support the Incident Reporting Team in the preparation of the templates filling in all the required information about security incidents in the appropriate format required for mandatory incident reporting according to the different regulatory frameworks and, once the Controller has given the green light for reporting, by suggesting the communication channels to be used to send the report to the different Competent Authorities.

Other WP3 assets which have been analysed to be integrated into the demonstrator for phase 1 are:

- **JSON Users and Device analysis tool (JUDAS)**
  The asset JUDAS could be also included in the Incident Reporting demonstration case during the data collection and enrichment phase. This asset could be used by the members of the Incident Management Team to get a report containing information about users and devices affected by an incident. This report could help operators to obtain some additional information about the security incident they are analysing, in order to determine, for instance, its extension and the users or devices affected. Although this WP3 asset was initially mapped in the incident reporting demonstration case's requirements by its owner, it will not be available for integration in the demonstrator during phase1.

It is worth noting, however, that there is no WP3 asset or open source tool available which is capable of automatizing the data collection through a "smart" questionnaire. This asset or open source tool should adapt the questions asked to the operators according to the information they gradually fill in and to the requirements established by the regulators.

In addition, there is no WP3 asset or open source tool capable of evaluating the data regarding the incident that is provided by the operators through the smart questionnaire while also being able to classify the incident in terms of severity and to suggest the authorities that need to be notified.

Below, we describe the approach followed in each of those cases to cover (at least partially) the gaps in the main requirements with open source tools and some development in the context of the WP5, in order to have a complete demonstrator for the first phase:

- **Missing WP3 asset for Data Collection**
  The Data Collection phase of the incident reporting workflow in the demonstration case (requirement IR-F02 in D5.1) consists in "*collect all the information required related to the cyber incident through different questionnaires*" [1]. The open source Incident Management and Response tool TheHive will be used to fulfil this requirement. The main advantages of using this tool are:
    - It can be integrated with the WP3 asset AIRE to enforce the incident reporting workflow;

[34] https://thehive-project.org/

- It allows the management and customization of the templates used for the creation of new incidents in the incident reporting platform. A default incident template will be defined in CyberSec4Europefor the collection of all the information about a security incident. Such information will be used to fill in the report templates that need to be produced and sent to the Competent Authorities;
- It supports the creation of "Custom Fields" that will allow to directly insert information in a field that can be latter be processed (e.g., for event classification or report template preparation).

However, the incident templates that can be created using TheHive have some limitations:

- It does not have a smart questionnaire. This means that all the questions will be shown to the user, who should skip those that are not relevant (e.g., in case of an operational incident some field related to cyber incidents should not be completed). In these cases, the field will have a note in the description that will indicate in which conditions it needs to be compiled.
- The current version of TheHive does not support multi-choice fields in the custom fields.[35] This is an important limitation since many of the fields that are present in the notification templates established by regulators sometimes require the user to select more than one option. In order to solve this issue, for the first phase of development of the demonstrator, focused on the generation of the First Report (see the use case specification in section 5.1), those fields that are needed to perform the classification of the incident – which, in the first place, determines whether the incident must be notified or not – will be included in the questionnaire and will be divided into multiple fields (one by each option). The remaining ones will be included in the General Description of the incident to be selected by the user.
- The tool does not support the registration and storage of the details about entities and the related contacts, which is a type of information that is requested each time an incident is notified. Since the storage of this information in the demonstrator could accelerate the compilation of the questionnaires considering that more than one incident could affect a single entity during its lifetime, this feature will be integrated in the ATOS Incident Reporting Engine dashboard together with the information required to configure the mandatory incident reporting preparation.

- **Missing WP3 asset for Event Classification**
  The Event Classification and the suggestion about the need for mandatory incident reporting according to the different EU/National regulatory frameworks is a crucial phase in the incident reporting workflow as it is performed through this demonstration case. Being the Event Classification asset missing, we will provisionally skip this functionality and integrate a dummy asset within the open source Incident Management & Response Tool TheHive. This dummy asset will provide an event classification and a suggestion for mandatory incident reporting, but without implementing the classification and assessment methodologies defined in the sections above. Just some specific fields will be checked for the test scenarios that will be defined. The result will be included automatically in the same incident template used for the data collection through TheHive.

Figure 61 summarizes the architecture for the incident reporting demonstrator with the WP3 assets and open source tools described above involved.

[35] There is a feature request in TheHive GitHub project to support multi-select custom fields but it has not yet been implemented yet.

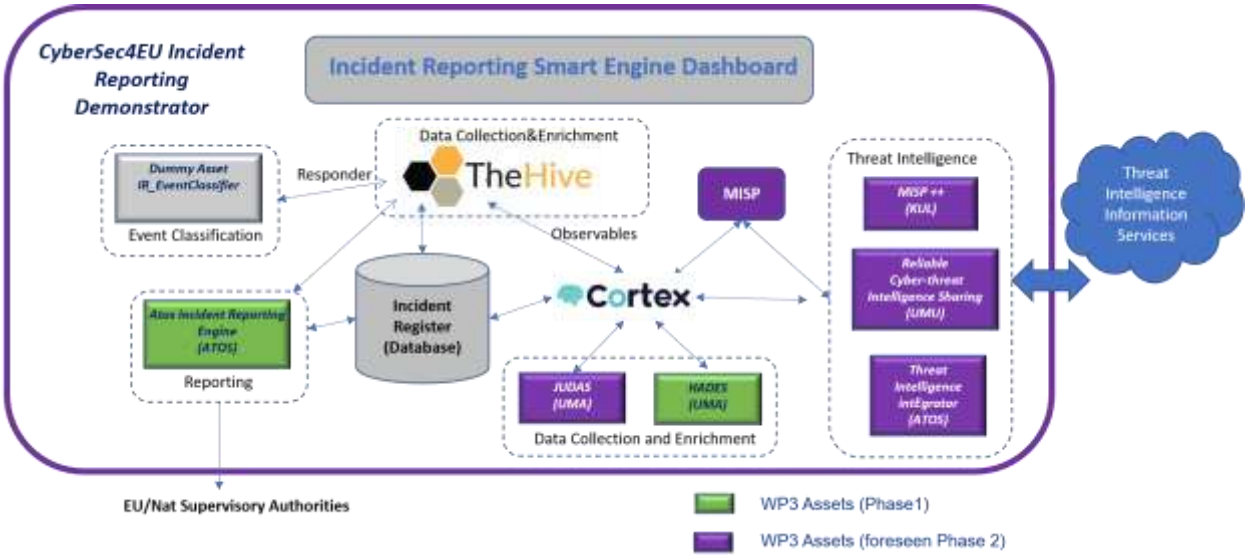

Figure 61: Incident Reporting - Demonstrator's Architecture

5.2.3 Description and Workflow

The demonstrator will be made available through a web page that will give access to the Incident Reporting Smart Engine graphical interface. In the background, the WP3 assets and the open source Incident Management and Response tool TheHive described in the previous subsection will be running in a Virtual Machine.

Firstly, the Administrator user will need to log into the demonstrator to register all the information about the entities and users that can use the Incident Reporting Smart Engine. The administrator will be responsible for the assignation of the roles and the respective permissions of the different users involved in the incident reporting process. He/she will also be in charge of configuring the demonstrator with all the information about the different regulatory frameworks required to deal with the mandatory incident reporting process. This includes, for example, the configuration of the contacts for the entities and the channels to be used for the reporting in each case.

Once the Incident Reporting Smart Engine has been correctly configured, the different users can log into the web page. The graphical interface of TheHive will be integrated into the Incident Reporting Smart Engine and will be used to manage the different security incidents under analysis in a collaborative way. Thanks to the workflow enforcement performed by the AIRE asset, each time a new incident is created in TheHive a new incident reporting process will start. Only users belonging to the Incident Management Team (IMT) will have the possibility of registering new incidents. A specific TheHive “case template” will be developed in CyberSec4Europe to harmonize the collection of all the information about the incidents that will be required later to perform the mandatory reporting according to the different regulatory frameworks supported by the Incident Reporting Platform. This template will be selected by the users when a new incident is created using TheHive graphical interface.

The user permissions in TheHive (allowing only reading or also writing during the reporting process) and the tasks that are assigned to each user will depend on the stage of the incident in the incident reporting workflow. This control will be done transparently for the users using the AIRE asset.

The workflow foreseen in this demonstrator can be divided in three macro-phases that have a direct correspondence with the three Use Cases described in the previous section: a first Data Collection, Data Enrichment and Incident Classification and reporting suggestion phase; a second, evaluative phase in which a designated officer (the Controller) of the affected entity confirms or rejects the outcomes of the first phase (the

so-called "Managerial Judgement"); a third phase called "Data Conversion and reporting preparation" in which the demonstrator will convert the available data and automatically fill in the mandatory incident reporting templates to be manually sent to the appropriate competent authorities. Figure 62 below shows the complete flowchart foreseen for the demonstrator. During the first phase of development of the demonstrator, we will focus only in the generation of the First Report which includes the "Incident Detection and Triage" and "Incident Analysis" phases.

One of the key features included in the open source tool TheHive is the possibility of adding what they call "Observables" (such as IP addresses, domains, URLs, files, emails, etc) and send them to different analysers that provide additional information about an incident. This is done using the observable analysis and active response engine called Cortex,[36] which is fully integrated with TheHive. The WP3 asset HADES will be integrated in the Incident Reporting Smart Engine as a new analyser that can be invoked using the same Cortex engine. In the demonstration case, the HADES asset will be used by the Incident Management Team to analyse a malware sample file in order to determine the severity of a cyber incident detected in a financial institution.

Once the task of Data Collection assigned to the group of users in the IMT (it will be assigned to the person registered as IMT responsible by the administrator) is closed by one of them, the users in the Incident Classification Team (ICTL) will have permissions to complete the information about the incident working in the task "Data Enrichment". The users in the ICTL will have also assigned a task for "Event Classification" and enabled the possibility to invoke from TheHive graphical interface a "Responder" (in the terminology used in TheHive) called "Incident Reporting Event Classifier". This classifier which returns a report in JSON format with the result of the event impact severity classification (Significant or Not Significant) after the analysis done on the information introduced about the incident and if it is suggested to submit the incident to the different competent authorities in base to ECB/SSM and PSD2 regulations.

The result of the suggestions done by the Event Classifier will need to be confirmed by the Controller. The Controller will have an assigned task "Managerial Judgement" that will be enabled and a notification "ReadyForManagerialJudgement" will be shown through TheHive graphical interface when all the information about the incident is already available in the tool and the previous tasks have been closed by the Incident Management and Classification Teams. The Controller, after checking the incident information and the suggestions provided by the Incident Reporting Platform, will have the possibility to change the classification of the event and the need for reporting to the different authorities. Depending on the Controller's decision, the task related to data enrichment will be reopened (so the users in the ICLT can continue working on it to provide more information about the incident or update it) or the incident reporting workflow will move on to the next stage.

If the Controller determines that the security incident is "Not Significant" and can be closed, then all the information about the incident is registered in the database and the reporting workflow for that specific incident ends.

If the Controller determines that the security incident is "Significant" and can be reported, then the Incident Reporting Team (IRT) will start the "Data Conversion" task. In this task, they will need to complete any additional information required for the preparation of the mandatory reports that will be sent. The users in the IRT will have available a new Responder through TheHive graphical interface to invoke the WP3 asset AIRE to prepare the report templates with the information about the incident in the different formats (e.g., Excel) required by the competent authorities. Once these reports have been generated and the IRT considers they are ready for submission, they can close the Data Conversion task.

However, a final authorization from the Controller is necessary to perform the submission. At this stage, the Controller will be notified through TheHive graphical interface that the incident is "ReadyForFinalAuthorization" and he/she will have a new task "Green-light for Reporting" assigned. Again,

[36] https://github.com/TheHive-Project/Cortex

depending on the Controller's decision the reporting workflow for that specific incident ends or a new task for "Reporting & Release" is assigned to the IRT. In this task, the users will do manually the submission of the mandatory incident reports to the different Competent Authorities.

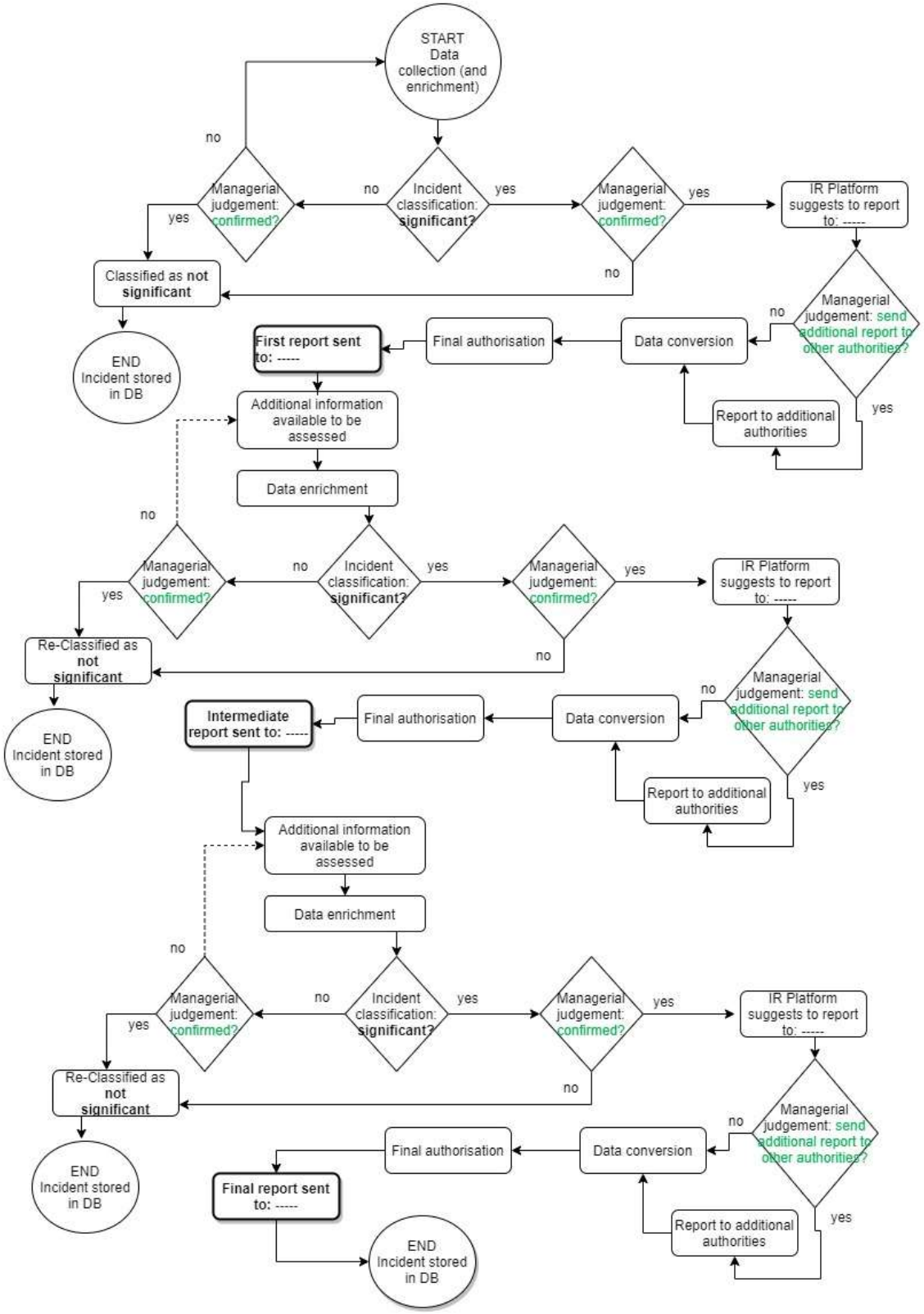

Figure 62: Incident Reporting - Flowchart foreseen in the use cases of the Mandatory Incident Reporting demonstrator

5.2.4 Target Group

Considering the current EU mandatory incident reporting framework, and the mandatory reporting requirements it imposes on financial institutions, the European Financial Sector shall be the main target group of the smart incident reporting platform. More specifically, since the incident reporting engine would provide a standardized and coordinated cybersecurity notification tool, its main target group shall include all European financial institutions qualified as:

- **Significant institutions (**ECB-SSM): Financial institutions from European countries, which are qualified as significant under the ECB-SSM Cyber Incident Reporting Framework.
- **Payment Services Providers** (PSD2): FIs operating as Payment Service Providers (PSPs).
- **Operators of Essential Services** (NIS): FIs classified as OESs under the requirements established by the NIS directive.
- **Personal Data Processors/Controllers** (GDPR): FIs that operate as Processors, which process personal data on behalf of a controller, and those that operate as Controllers, which determine the purposes and means of the processing of personal data.
- **Trust Service Providers** (eIDAS): FIs that operate either as Qualified or as Non-qualified trust service providers.

Furthermore, all other entities from other business or public sectors qualified as OES, Personal Data Processors/Controllers and Trust Service Providers shall be considered as part of a secondary target group of the smart incident reporting engine:

- **Operators of Essential Services** (NIS): Entities belonging to various economic sectors considered as OES by the respective national government, considering the specific criteria defined by the normative.

- **Personal Data Processors/Controllers** (GDPR): The Data Controllers are natural or legal persons, public authorities, agencies or other bodies which, alone or jointly with others, determine the purposes and means of the processing of personal data. The Data Processors are natural or legal persons, public authorities, agencies or other bodies which process (e.g., collects, records, organises, stores, uses, etc.) personal data on behalf of the Controller.

- **Trust Service Providers** (eIDAS): Trust services providers classified as Qualified or as Non-qualified trust service providers.

The smart incident reporting platform could provide to such target groups a tool that would simplify their mandatory incident reporting processes, allowing its centralization under the same management structure. It would also enable such institutions to standardize its incident management and reporting procedures, defining the roles and responsibilities of the actors involved in those processes and improving their effectiveness.

Additionally, the incident reporting tool would provide to such entities an objective and effective solution to the current legal uncertainty regarding mandatory incident reporting procedures that arises from the existing heterogenic mandatory incident reporting setting.

Therefore, summing up, the smart engine could resolve the common need of the entities belonging to those two target groups of having a standardized and coordinated cybersecurity notification process in case of significant cyber and operative incidents.

6 Maritime Transport

In this section, we describe the use cases for the CyberSec4Europe project which are applied in the demonstration case titled “Maritime Transport”. We provide a structured view utilizing use cases, which are structured in processes and events. Finally, we present a description and the workflow of three demonstration cases along with their relationships with WP3 assets, their specific relationship to use cases and finally the target groups they are aiming for.

6.1 Use Cases Specification

6.1.1 Use Case MT-UC1: Threat Modelling and Risk Analysis for Maritime Transport Services

This use case describes the threat modeling and risk analysis service for maritime transport. It includes various other use cases which describe the distinctive phases of asset identification (MT-UC1.1), maritime services analysis and representation (MT-UC1.2), Vulnerability Management (MT-UC1.3), Threats and Controls Management (MT-UC1.4), Threat Scenarios Specification (MT-UC1.5), Maritime Transport Risk Analysis (MT-UC1.6), Attack paths Generation and Representation (MT-UC1.7) and Maritime Transport Risk Management (MT-UC1.8).

6.1.1.1 Stakeholders

This use case comprises the following stakeholders:

- Port Authorities
- Ship-owner
- Cruise Operators
- Public Administrations
- Customs Authorities
- Importer
- Industry
- Insurance Company

These stakeholders apply to all the sub-use cases we will present. If a sub-use case includes additional stakeholders, we will report them it the sub-use case section.

For an exhaustive description of these stakeholders, please refer to [1].

6.1.1.2 Actors

This use case comprises the following actors:

- Security Officer
- Administrator
- End User

These actors apply to all the sub-use cases we will present. If a sub-use case includes additional actors, we will report them in the sub-use case section.

For an exhaustive description of these actors, please refer to [1].

6.1.1.3 Preconditions

This use case has no preconditions.

6.1.1.4 Basic Flow

We describe each step of this use case's basic flow in the relevant sub-use cases:

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

6.1.1.5 Alternate Flows

We describe this use case's alternate flows in the relevant sub-use cases' sections.

6.1.1.6 Postconditions

- A successful risk assessment procedure has been completed;
- A complete map of all the assets is drawn.

6.1.1.7 Included Use Cases

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

6.1.1.8 Use Case MT-UC1.1: Assets Identification and IT Infrastructure Representation

CyberSec4Europe Maritime Transport RA adopts an integrated intra and inter organization asset management approach that allows the creation of an IT asset inventory of all computing and networking related devices owned, managed, or otherwise used by the Security Officer. The use case on Assets Identification and IT Infrastructure Representation can be implemented through the following processes:

1. Asset Declaration: A list of all the existing assets is written down, along with some information on their location, which will later assist in the mapping process;
2. Networks Management / Association of Assets with Networks: A list of all the existing networks is written down;
3. Assets Customization: Existing Assets are connected with vulnerabilities and threats;
4. Assets Visualization: A Graph depicting distances and connectivity amongst devices is drawn.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

See Section 6.1.1.2 for a complete list of actors.

Preconditions

- An existing list of all the components that substantiate the system under scrutiny, along with interaction characteristics, is available to aid the risk assessment procedure;
- The Vulnerability list is up to date with current standards and customized based on special products and issues introduced to the asset map;
- The Threat list is up to date with current standards and customized based on special products and issues introduced to the asset map.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Asset Declaration

The Asset Declaration process is initiated by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A new Asset is created and a unique name for it is declared.
2. An Asset Type is selected from the available options: Hardware, OS and Application.
3. For Applications, the Run Privilege attribute must be set.
4. For Hardware, an installation Site must be selected from the available list.
5. After the asset is connected to a vendor, the specific product name and product version attributes can be inserted (either manually, or chosen through the existing list).
6. The last step is to define where this particular asset is installed on, there are certain rules for the declaration of this particular asset relationship:
    a. A Hardware can only be installed on hardware.
    b. An operating system can only be installed on hardware or another operating system.
    c. An application can only be installed on Operating systems or other applications.

This process is repeated for all of the assets contained on the system under duress.

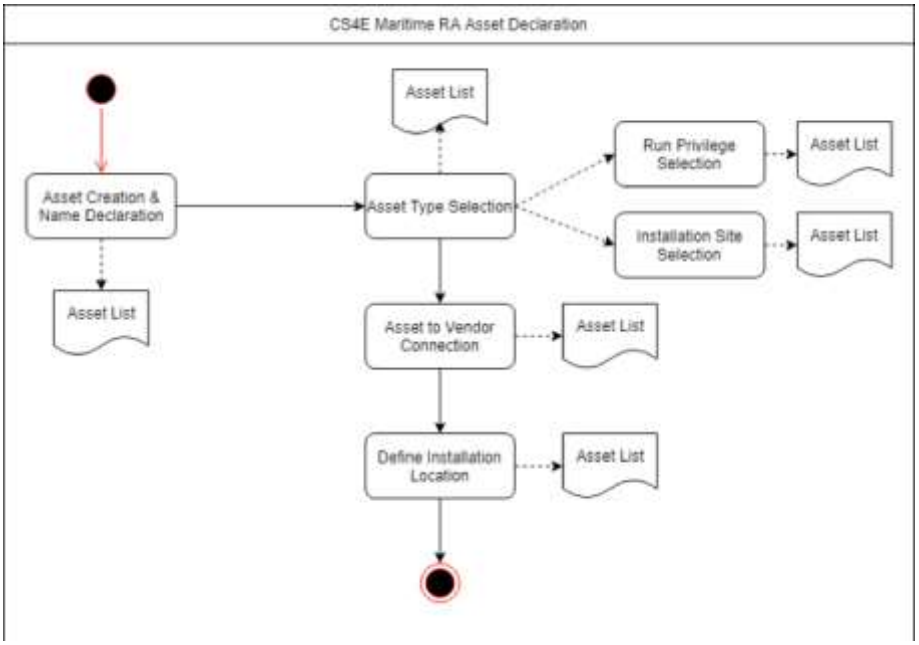

Figure 63: Maritime Transport - Basic Flow of the Asset Declaration Process

Process 2: Networks Management / Association of Assets with Networks

Having completed the Asset Declaration process the Security Officer must once again collaborate with actors familiar with the corporate IT Infrastructure and realize the following events:

1. A new Network is created, a unique name for it is declared;
2. A Network Type is selected from the available options;
3. An identifier for the network is inserted and the Network is saved;
4. The Security officer can now connect the list of Existing Network to the previously declared Assets.

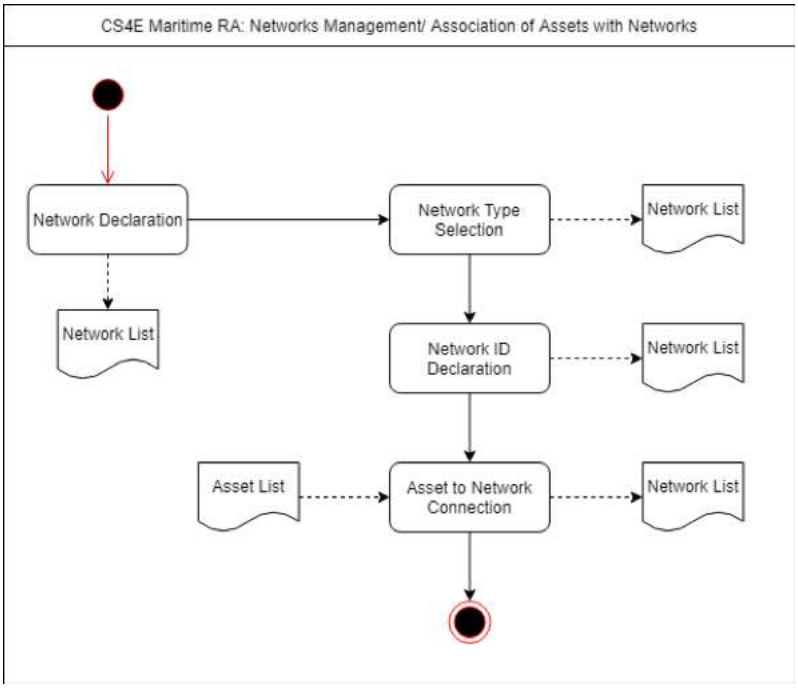

Figure 64: Maritime Transport - Basic Flow of the Networks Management/Association of Assets with Networks Process

Process 3: Assets Customization

With a list of all the existing assets the Security Officer can now proceed to connect assets with the corresponding vulnerabilities, threats and controls.

Flow of the Events:

1. Finding the Asset that is to be Customized;
2. Fill the Confirmed Vulnerabilities tab, either manually or from an existing list;
3. Fill the Threat tab, either manually or from an existing list;
4. Add and remove controls in order to mitigate existing threats.

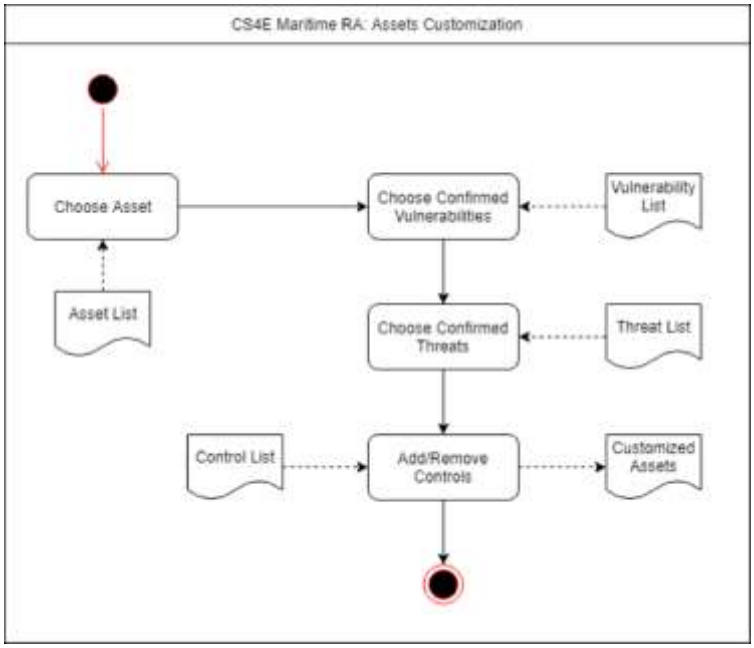

Figure 65: Maritime Transport - Basic Flow of the Assets Customization Process

Process 4: Assets Visualization

With a list of all the existing assets and further attributes, the Security Officer can now proceed to create a map containing the entire system under duress.

Flow of the events:

1. The Asset Map is created based on the existing information;
2. Class distances are set based on the actual distances amongst assets;
3. Node Scaling is used in order to depict the size of each individual asset.

Alternate Flows

The Security Officer can start by declaring the available Networks first, then proceed to declare the Assets.

Postconditions

- All of the Assets are listed along with their characteristics;
- All of the Assets are linked with their confirmed vulnerabilities and threats;
- Security Controls have been set for the vulnerable assets;
- All of the Networks are listed along with their interconnections with assets;
- A Map of all the existing Assets and Networks is created.

Extended Use Cases

- MT-UC1.1 is an extension of MT-UC1.3, since the asset customization process requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.3 refer to chapter 6.1.1.10;
- MT-UC1.1 is an extension of MT-UC1.4, since the asset customization process requires a complete list of threats in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11.

Included Use Cases

- MT-UC1.1 is included in MT-UC1.5, since the threat scenario specification use case, which requires a complete list of assets in order to be successful. For further information on MT-UC1.5 refer to chapter 6.1.1.12;
- MT-UC1.1 is included in MT-UC1.6, since the Maritime Transport Risk Analysis use case, which requires a complete list of assets in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.1 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case, which requires a complete list of assets in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;
- MT-UC1.1 is included in MT-UC1.8, since the Maritime Transport Risk Management use case, which requires a complete list of assets in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.9 Use Case MT-UC1.2: Maritime Services Analysis and Representation

CyberSec4Europe Maritime Transport RA provides a collaborative, business-centric approach, which aims to facilitate knowledge sharing among inter-organizational or extra organizational business partnerships of the maritime industry. The proposed knowledge-based method explores both process-based and asset-based views of knowledge within the Maritime sector. It focuses on both knowledge flows and knowledge content – its creation, storage and reusability and in providing support for the representation and retrieval of articulated, documented knowledge. The use case on Maritime Services Analysis and Representation can be implemented through the following processes:

1. Service Initiation;
2. Service Process Declaration;
3. Business Partner Invitation;
4. Association of Assets with Business Process;
5. Business Partners Cyber-Dependencies Declaration.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actor:

- Business Partners.

Preconditions

A verified list of all the legitimate Business Partners exists.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Service Initiation

The Service Initiation process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A new Maritime Service is created;
2. The desired name for the Maritime Service is set.

Process 2: Service Process Declaration

The Service Process Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A Maritime Service is chosen;
2. A corresponding process is created;
3. The desired name for the process is set;
4. The process is saved.

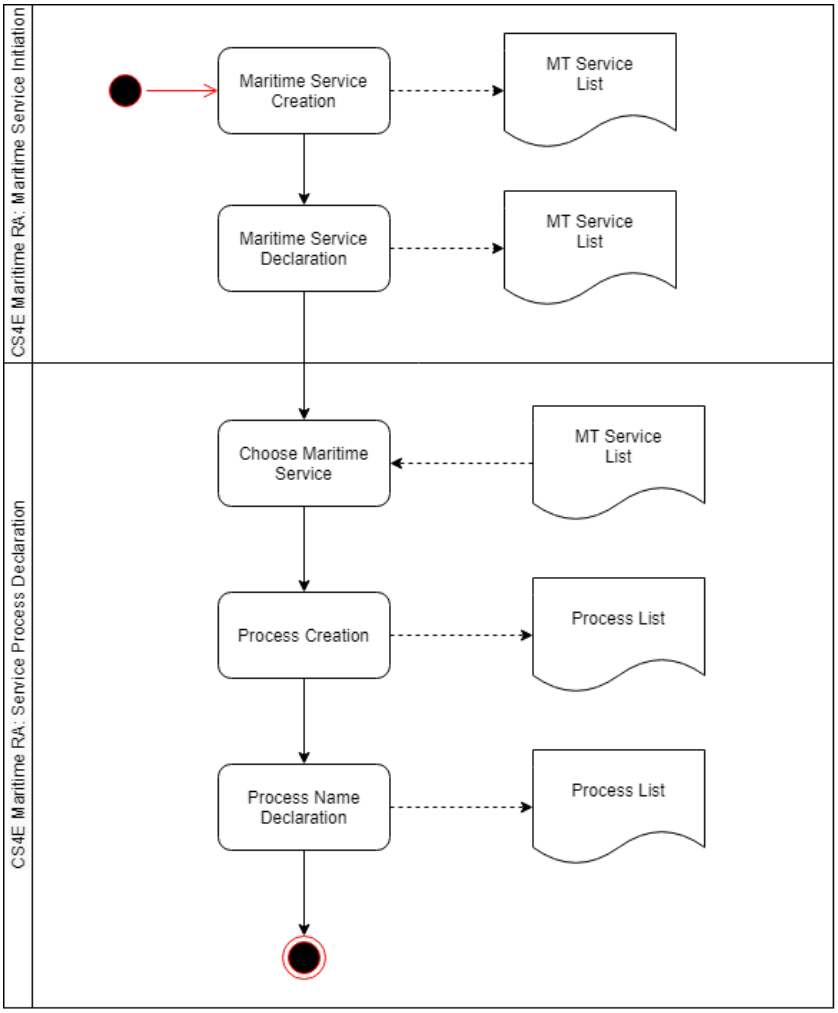

Figure 66: Maritime Transport - Basic Flow of the Maritime Service Initiation and the Service Process Declaration Processes

Process 3: Business Partner Invitation

The Business Partner Invitation process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, in this specific process the Business Partners are involved in the context of handling the incoming invitations, this process can be analysed in the following events:

1. Invitations are sent to the corresponding business partners by other business partners or by administrators;
2. Accept incoming invitations from business partners.

Process 4: Association of Assets with Business Process

The Association of Assets with Business Process process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, in this specific process the Business Partner knowledge about business processes may also be utilized, while realizing the following events:

1. The available Service Processes are listed and a desired process is chosen;
2. The available business partners for the corresponding Service Process are listed and a desired partner is chosen;

3. Based on the asset list of the corresponding partner, an asset is chosen and then connected to a process;

Process 5: Business Partners Cyber-Dependencies Declaration

Cyber dependencies are used to declare cyber interconnections amongst different business partners within a process of a maritime service. The Business Partners Cyber-Dependencies Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, in this specific process the Business Partners are involved in the context of handling the incoming invitations, this process can be analysed in the following events:

1. A process is chosen and the participating business partners are listed;
2. A partner is chosen for the cyber dependency to be declared;
3. A name for the cyber dependency is declared;
4. An invitation is sent to the business partner.

Alternate Flows

There are no alternate flows for this use-case

Postconditions

- A list of all the existing Business Partners has been created;
- A list of all the existing Maritime Services has been created;
- For every Maritime Service a list of existing processes has been created;
- The corresponding Business Partners and their assets are connected to each process.

Extended Use Cases

- MT-UC1.2 is an extension of MT-UC1.1, since the Maritime Services Analysis and Representation use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;
- MT-UC1.2 is an extension of MT-UC1.3, since the Maritime Services Analysis and Representation use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.3 refer to chapter 6.1.1.10;
- MT-UC1.2 is an extension of MT-UC1.4, since the Maritime Services Analysis and Representation Stakeholders use case requires a complete list of threats in order to be successful. For further information on MT-UC1.3 refer to chapter 6.1.1.11.

Included Use Cases

- MT-UC1.2 is included in use case MT-UC1.5, since the threat scenario specification use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.5 refer to chapter 6.1.1.12;
- MT-UC1.2 is included in use case MT-UC1.6, since the Maritime Transport Risk Analysis use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.2 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;

- MT-UC1.2 is included in MT-UC1.8, since the Maritime Transport Risk Management use case, which requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.10 Use Case MT-UC1.3: Vulnerability Management

The organizations should be aware of the vulnerabilities that the assets comprising their IT infrastructure may have. The CyberSec4Europe Maritime Transport RA system makes use of open data sources where these vulnerabilities have been disclosed replicating all the vulnerabilities. In this way, the proposed system can act as a central repository for all custom and known vulnerabilities.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

See Section 6.1.1.2 for a complete list of actors.

Preconditions

- A list of custom Vulnerabilities referring to unique assets exists;
- Access to Open Vulnerability Databases is Enabled in order to synchronize with them.

Basic Flow

This use case can be organized and presented through several processes, which we describe in what follows.

Process 1: Vulnerabilities Declaration

The Vulnerabilities Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A new Vulnerability is declared;
2. A unique ID is chosen;
3. A CVSS score is determined for the vulnerability;
4. Access complexity, authentication and exploitability are set on the appropriate level.

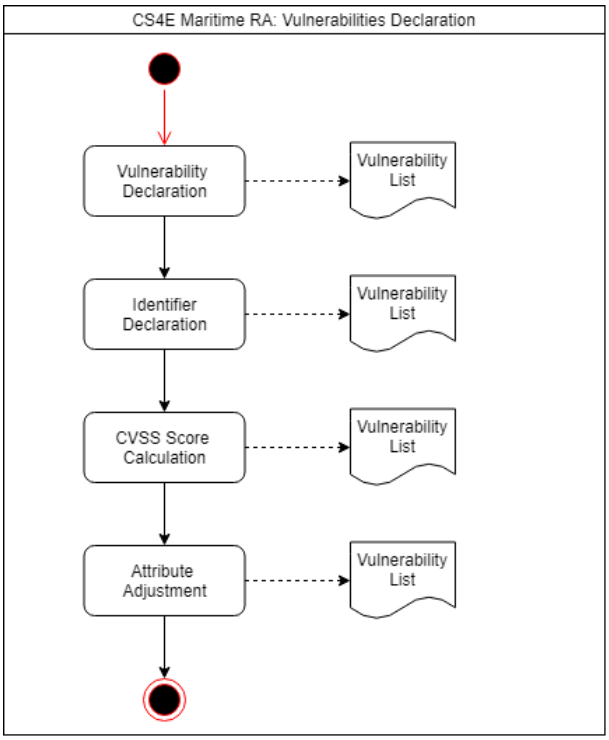

Figure 67: Maritime Transport - Basic Flow of the Vulnerabilities Declaration Process

Process 2: Vulnerabilities Synchronization and Management

The Vulnerabilities Synchronization and Management process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. The list of the existing custom vulnerabilities can be extending by synchronizing it with the list provided by CVE Details[37];
2. Existing vulnerabilities are altered;
3. Vulnerabilities that are not required can be deleted.

[37] (https://www.cvedetails.com/)

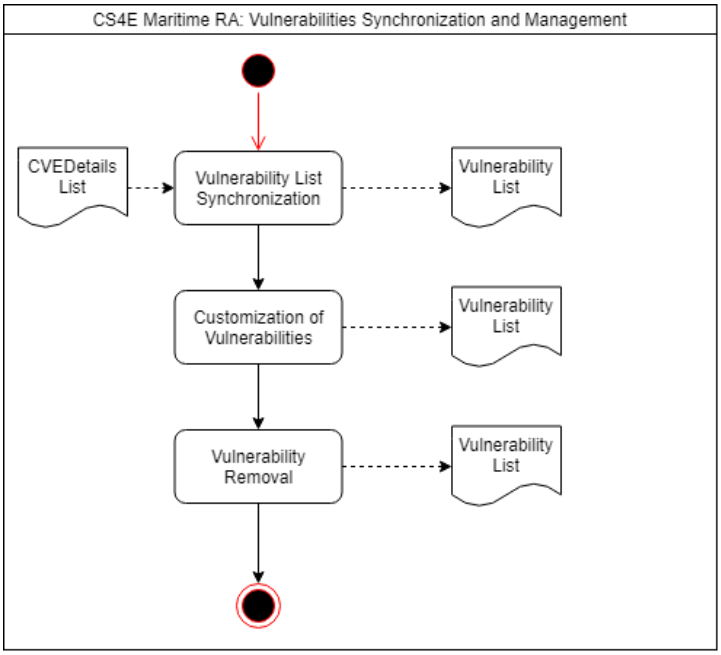

Figure 68: Maritime Transport - Basic Flow of the Vulnerabilities Synchronization and Management Process

Alternate Flows

There are no alternate flows for this use-case

Postconditions

This use case has no postconditions.

Included Use Cases

- MT-UC1.3 is included in MT-UC1.1, since the Assets Identification and IT Infrastructure Representation use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;
- MT-UC1.3 is included in MT-UC1.4, since the Threats and Controls Management use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11;
- MT-UC1.3 is included in MT-UC1.5, since the Threat Scenarios Specification use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11;
- MT-UC1.3 is included in MT-UC1.6, since the Maritime Transport Risk Analysis use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.3 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;
- MT-UC1.3 is included in MT-UC1.8, since the Maritime Transport Risk Management use case requires the complete list of vulnerabilities in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.11 Use Case MT-UC1.4: Threats and Controls Management

The digital era forces the Security Officers as well as all the organizations involved in the Maritime industry under pressure to be aware of the threat landscape that their IT infrastructure is exposed to. Therefore, they should be armed with appropriate tools and solutions that will help them familiarize themselves with threats that may affect their organizations and the security controls that can be deployed or can be applied in order to mitigate the risks and deal with their defined threats and weaknesses.
In this context, the CyberSec4Europe Maritime RA system can act as a comprehensive dictionary of known threats as well as the corresponding mitigation controls that can be used to advance the understanding of Security Officers and enhance their defences.
Therefore, in order for the Security Officers of the maritime industry to enhance their awareness of the threat landscape, have to perform the following processes:

1. Threats Declaration;
2. Threats Synchronization and Management;
3. Security Controls Declaration;
4. Security Controls Customization.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actor:

- Maritime Transport Security Officer.

Preconditions

- A list of Threats that can be inserted to the system exists;
- Access to Open Vulnerability Databases is enabled.
- MT-UC1.3 is completed and therefore there is an available complete Vulnerability list.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Threats Declaration

The Threats Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A new threat is declared;
2. A name and a unique identifier are set for the new threat;
3. A short description is added for the inserted threat.

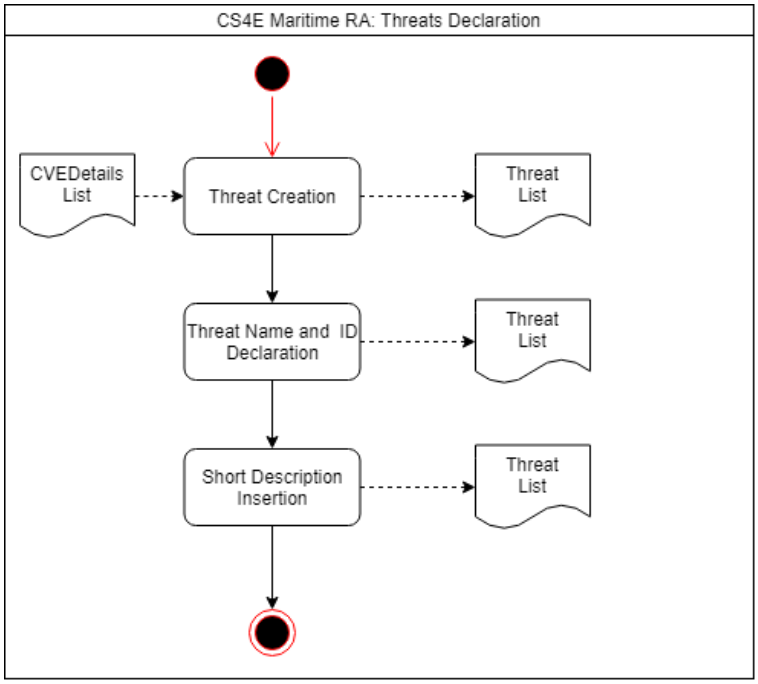

Figure 69: Maritime Transport - Basic Flow of the Threats Declaration Process

Process 2: Threats Synchronization and Management

The Threats Synchronization and Management process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. The threat list is synchronized and extended with the list of threats provided by MITRE (CWE) and applied by CVE Details;
2. Based on the threat CWE identifier connections between vulnerabilities and threats are created.

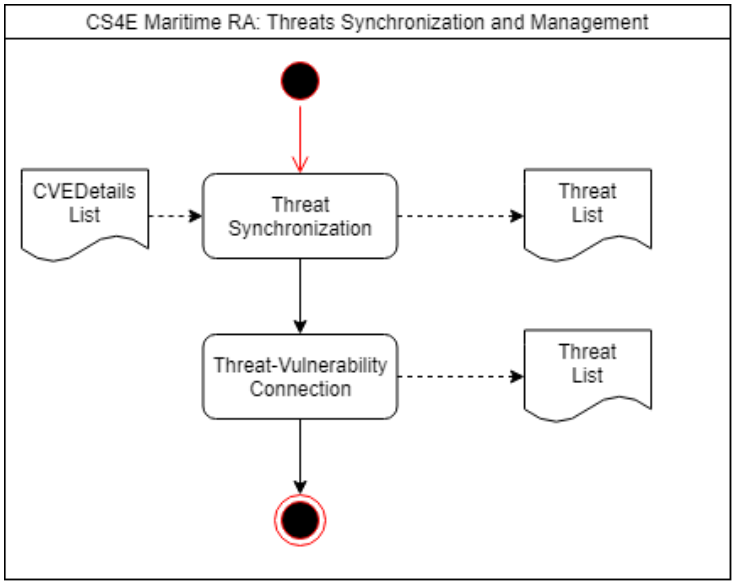

Figure 70: Maritime Transport - Basic Flow of the Threats Synchronization and Management Process

Process 3: Security Controls Declaration

The Security Controls Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. A new Control is created;
2. A name for the Control is declared;
3. A Control type is chosen between Mitigate Threat and Mitigate Vulnerability;
4. The Control is added and saved to the existing list.

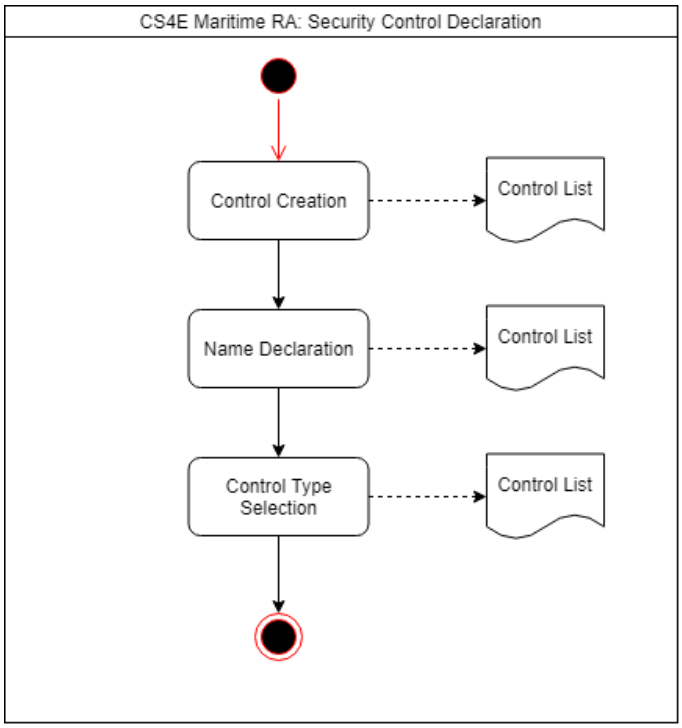

Figure 71: Maritime Transport - Basic Flow of the Security Controls Declaration Process.

Process 4: Security Controls Customization

The Security Controls process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. The available Controls are listed and viewed;
2. Depending on the Control Type, the Control can be associated with further Vulnerabilities or Threats.

Postconditions

- A List is created containing all the manually and automatically inserted threats;
- All of the threats are connected to the corresponding vulnerabilities;
- Security Controls are created for the listed threats.

Extended Use Cases

- MT-UC1.4 is an extension of MT-UC1.1, since the Threats and Controls Management use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;
- MT-UC1.4 is an extension of MT-UC1.3, since the Threats and Controls Management use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.3 refer to chapter 6.1.1.10.

Included Use Cases

- MT-UC1.4 is included in MT-UC1.1, since the Assets Identification and IT Infrastructure Representation requires a complete list of threats in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;
- MT-UC1.4 is included in MT-UC1.5, since the Threat Scenario Specification use case requires a complete list of threats in order to be successful. For further information on MT-UC1.5 refer to chapter 6.1.1.12;
- MT-UC1.4 is included in MT-UC1.6, since the Maritime Transport Risk Analysis use case requires a complete list of threats in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.4 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case requires a complete list of threats in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;
- MT-UC1.4 is included in MT-UC1.8, since the Maritime Transport Risk Management use case requires a complete list of threats in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.12 Use Case MT-UC1.5: Threat Scenarios Specification

The CyberSec4Europe Maritime RA system aims to provide guidance to the maritime industry operators on how to assess and organize the security issues associated with the processes in which they are involved. In this context, the CyberSec4Europe Maritime RA system encompasses and executes an evaluation process that implements the main steps of the proposed collaborative evidence-driven Maritime Service Risk Assessment.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actors:

- Maritime Transport Security Officer;
- Business Partners.

Preconditions

- MT-UC1.1 is completed and therefore there is an available complete Asset list;
- MT-UC1.3 is completed and therefore there is an available complete Vulnerability list;
- MT-UC1.4 is completed and therefore there are available complete Threat and Security Control lists.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Attack Scenario Declaration

The Attack Scenario Declaration process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A unique name for the scenario is declared;
2. The affected asset is selected;
3. The corresponding vulnerability is selected;
4. The threat that can enable the chosen vulnerability is selected.

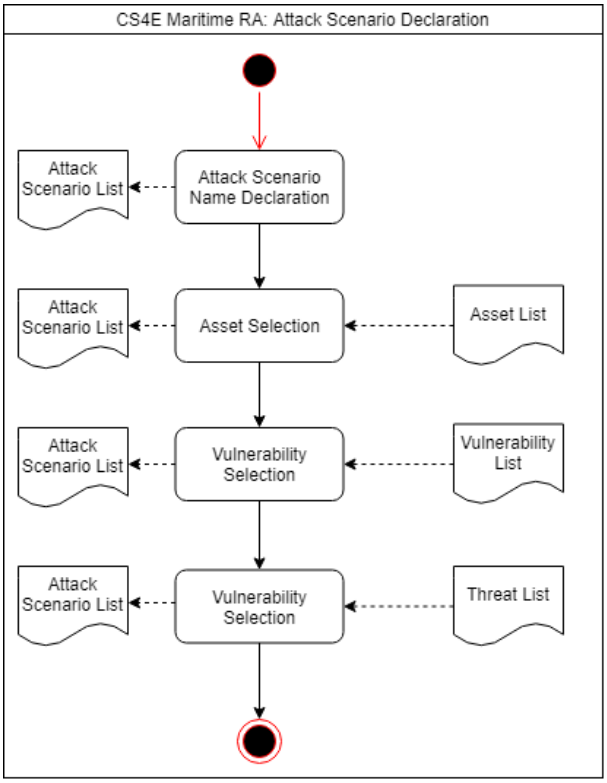

Figure 72: Maritime Transport - Basic Flow of the Attack Scenario Declaration Process

Postconditions

A complete list of the attack scenarios and their required attributes is created.

Extended Use Cases

- MT-UC1.5 is an extension of MT-UC1.1, since the Threat Scenarios Specification use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;

- MT-UC1.5 is an extension of MT-UC1.2, since the Threat Scenarios Specification use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.2 refer to chapter 6.1.1.9;
- MT-UC1.5 is an extension of MT-UC1.3, since the Threat Scenarios Specification use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.10;
- MT-UC1.5 is an extension of MT-UC1.4, since the Threat Scenarios Specification use case requires a complete list of threats in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11.

Included Use Cases

- MT-UC1.5 is included in MT-UC1.6, since the Maritime Transport Risk Analysis use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.5 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;
- MT-UC1.5 is included in MT-UC1.8, since the Maritime Transport Risk Management use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.13 Use Case MT-UC1.6: Maritime Transport Risk Analysis

The CyberSec4Europe Maritime RA system aims to guide the operators on how to assess and organize the security issues associated with the Maritime Services in which they involved. In this context, the system encompasses and executes an evaluation process that implements a collaborative evidence-driven Maritime Supply Chain Risk Assessment procedure.
The processes that should be performed to measure the risks, threats and vulnerabilities of ICT-based maritime services are the following:

1. Risk Assessment Initiation;
2. RA Involved Assets Preview;
3. RA Summary Preview;
4. RA Reports (Risk Analysis, Threat Analysis diagrams) Preview.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actors:

- Maritime Transport Security Officer;
- Business Partners.

Preconditions

- MT-UC1.1 is completed and therefore there is an available complete Asset list;

- MT-UC1.2 is completed and therefore there is an available complete Business Partner, Maritime Service and Process list;
- MT-UC1.3 is completed and therefore there is an available complete Vulnerability list;
- MT-UC1.4 is completed and therefore there are available complete Threat and Security Control lists;
- MT-UC1.5 is completed and therefore the possible attack scenarios have been calculated.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Risk Assessment Initiation

The Risk Assessment Initiation process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A Risk Assessment Procedure is initiated;
2. A process is selected to be assessed;
3. A short name for the Risk Assessment is declared;
4. A Risk Assessment Type is Chosen between Real and Simulation;
5. For the Simulation Type Vulnerabilities can be edited and further controls can be added or removed;
6. Once all of the steps are completed the Risk Assessment is saved.

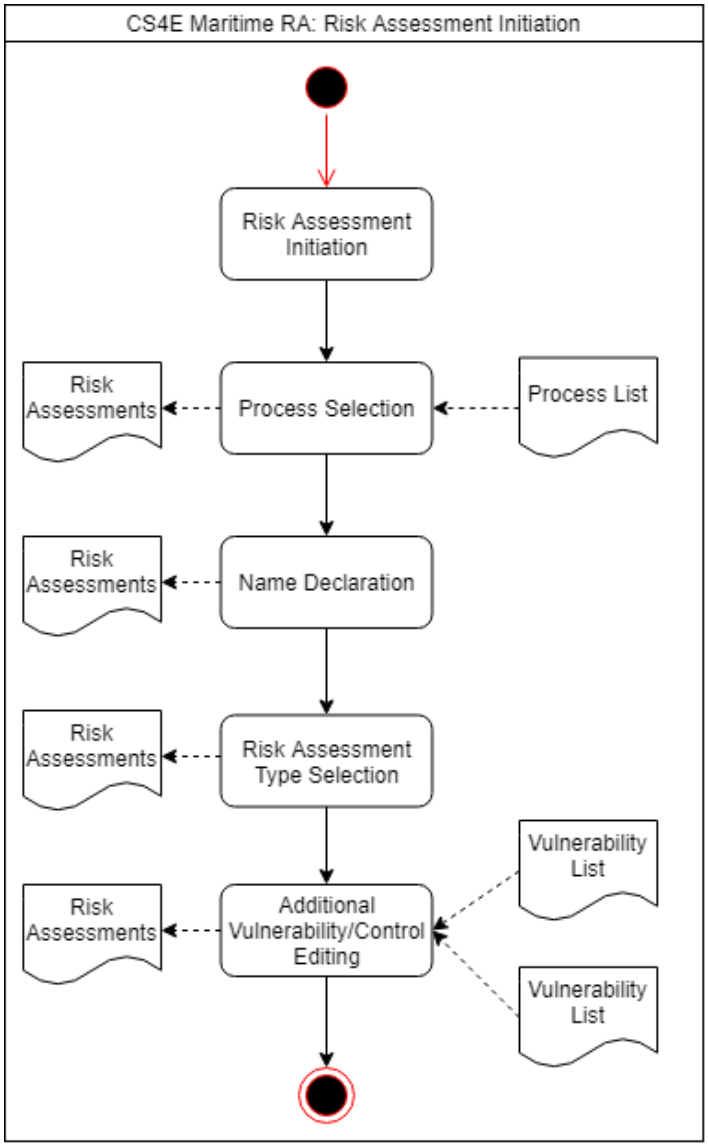

Figure 73: Maritime Transport - Basic Flow of the Risk Assessment Initiation Process

Process 2: RA Involved Assets Preview

The RA Involved Assets Preview process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A Risk Assessment is chosen and the Assets that take part in this procedure are viewed;
2. Risk Assessments of the type Simulation, which have not been executed can still be adjusted;
3. Risk Assessment of the type Real, after executed can be viewed in order to provide a better understanding over the options that were set.

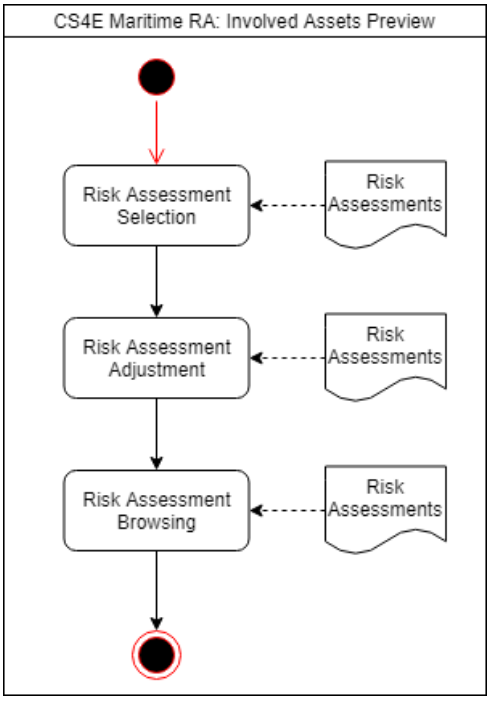

Figure 74: Maritime Transport - Basic Flow of the Involved Assets Preview Process

Process 3: RA Summary Preview

The RA Summary Preview process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A detailed summary of the calculated risk for each asset is created;
2. The risk per individual vulnerability per asset, is calculated. Threats are considered;
3. The Dominant Individual Risk Level is calculated.

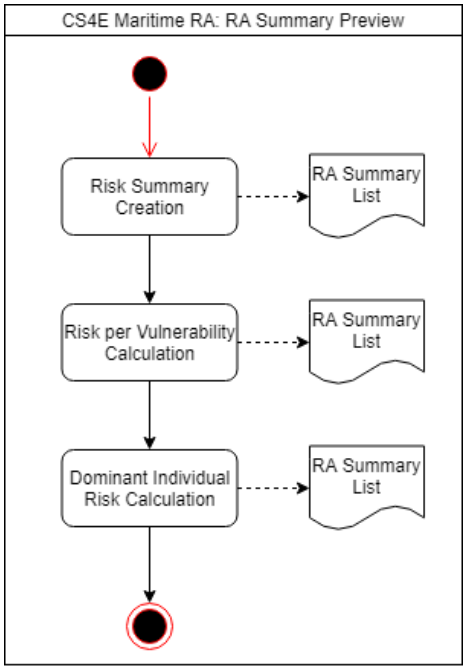

Figure 75: Maritime Transport - Basic Flow of the RA Summary Preview Process

Process 4: RA Reports (Risk Analysis, Threat Analysis diagrams) Preview

The RA Reports (Risk Analysis, Threat Analysis diagrams) Preview process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A Specific Risk Assessment is chosen;
2. A "Risk Analysis" diagram is drawn, where the dominant individual risk level for all the assets participating in the risk assessments depicted;
3. A "Threat Analysis" diagram is drawn, where a count of the threats associated with a specific asset based on their dominant risk level is depicted.

Postconditions

- The Risk Assessment process has been initiated and connected to the data procured by the previous use-cases;
- A summary based on the Risk Assessment is created and previewed;
- Reports based on the Risk Assessment are created and previewed.

Extended Use Cases

- MT-UC1.6 is an extension of MT-UC1.1, since the Maritime Transport Risk Analysis use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;

- MT-UC1.6 is an extension of MT-UC1.2, since the Maritime Transport Risk Analysis use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.2 refer to chapter 6.1.1.9;
- MT-UC1.6 is an extension of MT-UC1.3, since the Maritime Transport Risk Analysis use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.10;
- MT-UC1.6 is an extension of MT-UC1.4, since the Maritime Transport Risk Analysis use case requires a complete list of threats in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11;
- MT-UC1.6 is an extension of MT-UC1.5, since the Maritime Transport Risk Analysis use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.12.

Included Use Cases

- MT-UC1.6 is included in MT-UC1.7, since the Attack Paths Generation and Representation use case requires the Maritime Transport Risk Analysis procedure to be completed first in order to be successful. For further information on MT-UC1.7 refer to chapter 6.1.1.14;
- MT-UC1.5 is included in MT-UC1.8, since the Maritime Transport Risk Management use case requires the Maritime Transport Risk Analysis procedure to be completed first in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.14 Use Case MT-UC1.7: Attack paths Generation and Representation

The CyberSec4Europe Maritime RA provides an attack path discovery method that relies on unique characteristics, such as the attacker location, the attacker capability, assets interdependencies and which the entry and target points are to return all attack paths that exist in the examined supply chains. The business partners should perform the following actions to identify the attack paths associated with the Maritime Services in which they are involved.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actors:

- Maritime Transport Security Officer;
- Business Partners.

Preconditions

- MT-UC1.1 is completed and therefore there is an available complete Asset list;
- MT-UC1.2 is completed and therefore there is an available complete Business Partner, Maritime Service and Process list;
- MT-UC1.3 is completed and therefore there is an available complete Vulnerability list;
- MT-UC1.4 is completed and therefore there are available complete Threat and Security Control lists;
- MT-UC1.5 is completed and therefore the possible attack scenarios have been calculated;

- MT-UC1.6 is completed and therefore the Risk Assessment results are available (Reports, Summary).

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: RA Involved Assets Preview

The RA Involved Assets Preview process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A Risk Assessment is chosen and the Assets that take part in this procedure are viewed;
2. The Attack Path calculation procedure can now be initiated.

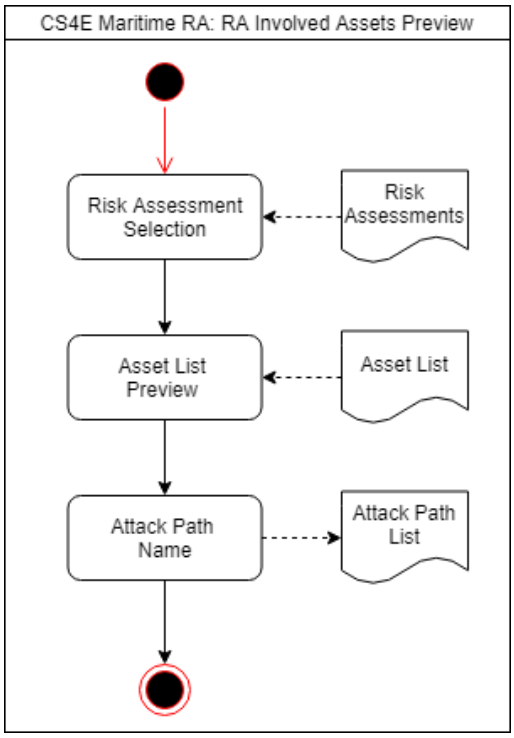

Figure 76: Maritime Transport - Basic Flow of the RA Involved Assets Preview Process

Process 2: Attack Paths Generation and Visualization

The Attack Paths Generation and Visualization process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure:

1. The Entry points of the system under duress are listed;
2. The Target points of the system under duress are listed;
3. Attacker Profile is set;
4. Attacker Location is set;
5. Maximum Length of chains is set;

6. The Attack Paths based on the Characteristics set by the user are calculated automatically.

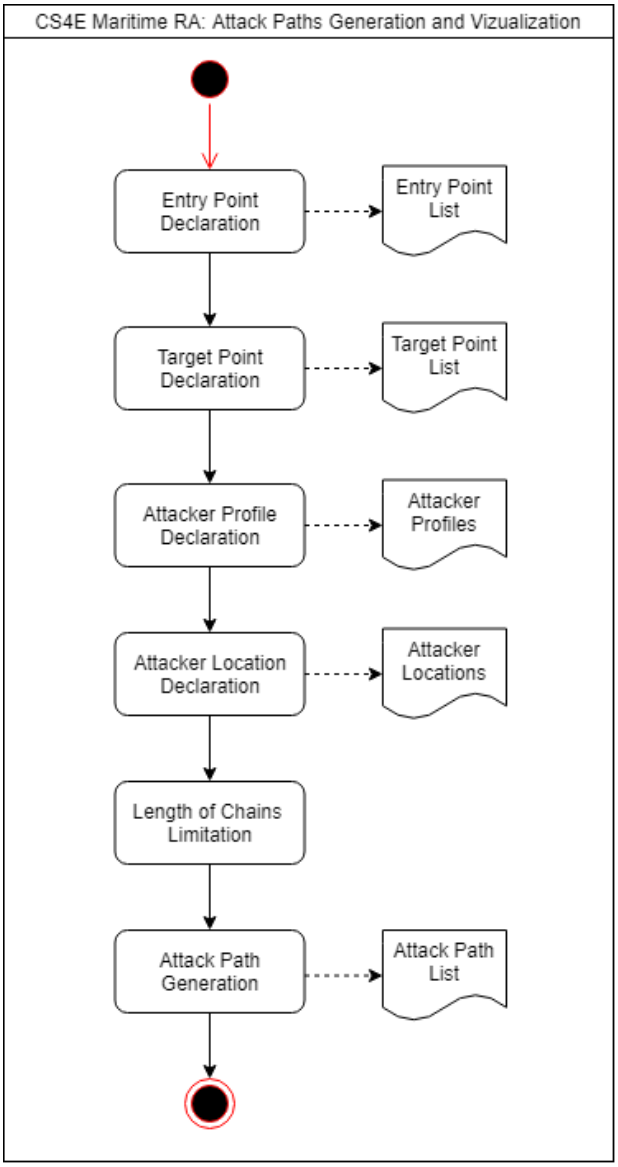

Figure 77: Maritime Transport - Basic Flow of the Attack Paths Generation and Visualization Process

Postconditions

- Through the procured asset list and risk assessment documents possible attack paths for connected assets are revealed;
- By setting entry/target points and attacker characteristics the attack paths that can be utilized are calculated;
- A list with all the possible attack paths the inserted attributes allow has been created.

Extended Use Cases

- MT-UC1.7 is an extension of MT-UC1.1, since the Attack Paths Generation and Representation use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;

- MT-UC1.7 is an extension of MT-UC1.2, since the Attack Paths Generation and Representation use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.2 refer to chapter 6.1.1.9;
- MT-UC1.7 is an extension of MT-UC1.3, since the Attack Paths Generation and Representation use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.10;
- MT-UC1.7 is an extension of MT-UC1.4, since the Attack Paths Generation and Representation use case requires a complete list of threats in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11;
- MT-UC1.7 is an extension of MT-UC1.5, since the Attack Paths Generation and Representation use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.12;
- MT-UC1.7 is an extension of MT-UC1.6, since the Attack Paths Generation and Representation use case requires the Maritime Transport Risk Analysis procedure to be completed first in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.12.

Included Use Cases

MT-UC1.7 is included in MT-UC1.8, since the Maritime Transport Risk Management use case requires the generated Attack Paths in order to be successful. For further information on MT-UC1.8 refer to chapter 6.1.1.15.

6.1.1.15 Use Case MT-UC1.8: Maritime Transport Risk Management

The CyberSec4Europe Maritime RA system shows how an attacker can take advantage of the weaknesses and limitations that exist in the IT infrastructures involved in the Maritime Services, conducting a sequence of attacks and exploiting multiple vulnerabilities in order to reach a specific target. These vulnerability trees, when produced they expose the risks that are embedded in the IT systems as well as the risks that a combination of threat scenarios pose to the Maritime Industry as a whole.
To fulfil this goal, the CyberSec4Europe Maritime RA system implements the following processes:

- Review Risk Assessment Results;
- Attack Path Analysis Scenarios Execution;
- Mitigation Strategy Selection.

Stakeholders

See Section 6.1.1.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.1.2 this use case comprises the following additional actors:

- Maritime Transport Security Officer;
- Business Partners.

Preconditions

- MT-UC1.1 is completed and therefore there is an available complete Asset list;
- MT-UC1.2 is completed and therefore there is an available complete Business Partner, Maritime Service and Process list;

- MT-UC1.3 is completed and therefore there is an available complete Vulnerability list;
- MT-UC1.4 is completed and therefore there are available complete Threat and Security Control lists;
- MT-UC1.5 is completed and therefore the possible attack scenarios have been calculated;
- MT-UC1.6 is completed and therefore the Risk Assessment results are available (Reports, Summary);
- MT-UC1.7 is completed and therefore all of the attack graphs have been calculated beforehand.

Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Review Risk Assessment Results

The Review of Risk Assessment Results process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure. Furthermore, business partners are considered actors for this use case because of their knowledge on the existing assets, this process is realized through the following events:

1. A Risk Assessment is chosen;
2. The Results are reviewed, with focus on assets that have high individual risk;
3. The vulnerabilities responsible for the resulting risk along with the applicable security controls are highlighted.

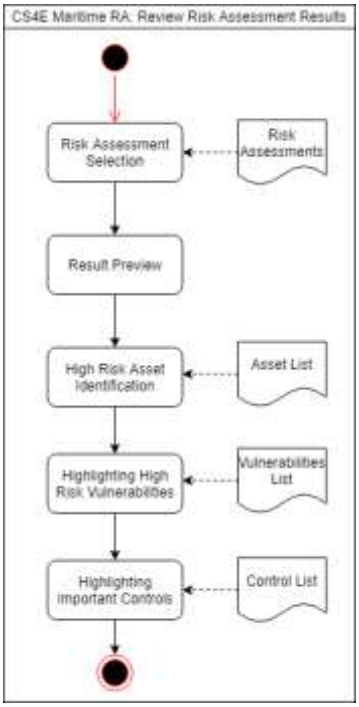

Figure 78: Maritime Transport - Basic Flow of the Review Risk Assessment Results Process

Process 2: Attack Path Analysis Scenarios Execution

The Attack Path Analysis Scenarios Execution process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. An attack path analysis procedure is executed using high-risk assets as entry points and cyber dependencies as targets;
2. The paths and vulnerabilities that contribute more to the cumulative risk on cyber dependencies are investigated further;
3. Attack path analysis can be rerun using cyber dependencies as entry points and studied through the produced sub-graph.

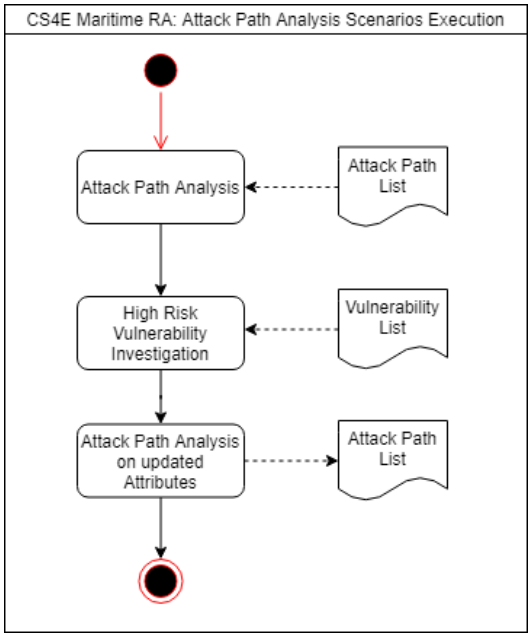

Figure 79: Maritime Transport - Basic Flow of the Attack Path Analysis Scenarios Execution Process

Process 3: Mitigation Strategy Selection

The Mitigation Strategy Selection process is implemented by the Security Officer of a Maritime Transport Organization, with the support of other actors like Administrators, End Users who are familiar with the corporate IT Infrastructure, by realizing the following events:

1. Security Controls are set;
2. Multiple defensive strategies are built;
3. The defensive strategies are evaluated using game theory.

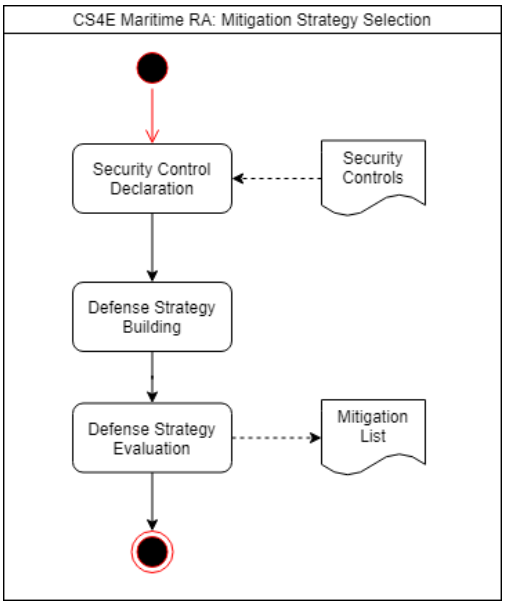

Figure 80: Maritime Transport - Basic Flow of the Mitigation Strategy Selection Process

Postconditions

- High Risk Assets have been identified through the review of the Risk Assessment Results;
- High Risk Vulnerabilities have been highlighted through the review of the Risk Assessment Results;
- Important Controls Have Been Highlighted;
- Attack Path Analysis is executed again with the updated variables;
- Further Security Controls have been declared;
- A defense strategy is built and evaluated;
- Mitigation controls are finalized.

Extended Use Cases

- MT-UC1.8 is an extension of MT-UC1.1, since the Maritime Transport Risk Management use case requires a complete list of assets in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.8;
- MT-UC1.8 is an extension of MT-UC1.2, since the Maritime Transport Risk Management use case requires the complete lists of Business Partners, Maritime Services and Processes in order to be successful. For further information on MT-UC1.2 refer to chapter 6.1.1.9;
- MT-UC1.8 is an extension of MT-UC1.3, since the Maritime Transport Risk Management use case requires a complete list of vulnerabilities in order to be successful. For further information on MT-UC1.1 refer to chapter 6.1.1.10;
- MT-UC1.8 is an extension of MT-UC1.4, since the Maritime Transport Risk Management use case requires a complete list of threats in order to be successful. For further information on MT-UC1.4 refer to chapter 6.1.1.11;
- MT-UC1.8 is an extension of MT-UC1.5, since the Maritime Transport Risk Management use case requires a complete list of threat scenarios in order to be successful. For further information on MT-UC1.5 refer to chapter 6.1.1.12;

- MT-UC1.8 is an extension of MT-UC1.6, since the Maritime Transport Risk Management use case requires the Maritime Transport Risk Analysis procedure to be completed first in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.13;
- MT-UC1.8 is an extension of MT-UC1.7, since the Maritime Transport Risk Management use case requires the generated Attack Paths in order to be successful. For further information on MT-UC1.6 refer to chapter 6.1.1.14.

6.1.2 Use Case MT-UC2: Maritime System Software Hardening

Applications used in the maritime domain, such as software that runs on a moving vessel or on the ground base usually utilize legacy code. With legacy code, we refer to software that is written in unmanaged programming systems and which is hard to update. A typical example is C/C++ code which was developed in the past and is now hard to replace with more advanced, and security-oriented, systems. A possible replacement could be a similar application written in a memory-safe programming system (e.g., Rust or managed code). However, the specifics on the maritime domain makes software replacement hard. Since such code is hard to be replaced with a memory-safe version, software hardening is an attractive option. With software hardening, we refer to the process where a particular code is re-written in order to contain memory-related vulnerabilities. Re-writing the code can be done either by re-compiling the source (where possible) or by reconstructing the binary. Notice that this re-writing is focused on the security properties of software and not on its base functionality. Hardening can be applied much easier than a total replacement of the code.

6.1.2.1 Stakeholders

This use case comprises the following stakeholders:

- Port Authorities
- Ship-owner
- Cruise Operators
- Public Administrations
- Customs Authorities
- Importer
- Industry
- Insurance Company

For an exhaustive description of these stakeholders, please refer to [1].

6.1.2.2 Actors

The only actor in this use case is the Administrator/Security Analyst.

6.1.2.3 Preconditions

An existing list of all software components operating on a vessel or ground station.

6.1.2.4 Basic Flow

This use case can be organized and presented through a number of processes, which we describe in what follows.

Process 1: Identify unsafe software components

This process is initiated by an administrator/security analyst, which identifies all software components that are developed in an unsafe programming system. The output of this process is a list of software that is considered unsafe and can be hardened. For instance, an analyst may indicate that the communication application is linked with a memory-unsafe cryptographic shared library, such as OpenSSL, while the communication application itself is a memory unmanaged binary, itself.

Process 2: Analyze all identified components.

Once unsafe components have been identified, further analysis is required in order to characterize possible vulnerability classes and existing resources that may facilitate hardening. For instance, if an analyst has identified that an open-source library is used, such as OpenSSL, then hardening can be applied directly to the source code. For other binaries, where code is not available, binary re-writing should be used. Finally, during this process, depending on the actual software, possible vulnerability classes and exact vulnerabilities can be identified.

Process 3: Apply software hardening.

During this process, based on the aforementioned identified information, the actual hardening takes place by re-constructing all recorded software components.

Process 4 (optional): Leverage possible hardware features.

Software hardening can degrade software performance, since it is based on additional code that checks memory for inconsistencies. In most cases, these checks can incur practical overheads. Nevertheless, particular hardware features can speed up checks. In this process, possible hardware features that can accelerate hardening are identified.

6.1.2.5 Postconditions

Successful hardening procedure.

6.1.3 Use Case MT-UC3: Secure Maritime Communications

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

- VDES frequencies (to be used for VTS information services);
- AIS information: Maritime Mobile Service Identity (MMSI), time, ship position, speed, rate of turn, length, course etc.;
- Vessel voyage information: Route plans and mandatory ship reports;
- Maritime Single Window reporting information: Ship certificates, single window reports (notifications, declarations, certifications, requests and service orders), log books, passengers' lists and crew lists;
- Port to vessel information: Weather reports, passenger or cargo manifestos, etc.

6.1.3.1 Stakeholders

This use case comprises the following stakeholders:

- Port Authorities;
- Ship-owner;
- Cruise Operators;

- Public Administrations;
- Customs Authorities;
- Ministries.

These stakeholders apply to all the sub-use cases of MT-UC3. If a sub-use case includes additional stakeholders, we will report them it the sub-use case section.

For an exhaustive description of these stakeholders, please refer to [1].

6.1.3.2 Actors

This use case includes the following actors:

- Vessel;
- VTS;
- Port.

For an exhaustive description of the actors, please refer to [1].

6.1.3.3 Preconditions

The Vessel or VTS needs to send information to VTS, Port or another Vessel.

6.1.3.4 Basic Flow

Secure maritime communications contain different sub-use cases. These are differentiated by who sends what to whom. They do not form a single continuous use case, but can instead be used in any order. For specific use-case flows, please refer to the relevant included use cases:

- Use case MT-UC3.1: VTS Transmits to Vessels;
- Use case MT-UC3.2: Vessels Broadcast to Vessels;
- Use case MT-UC3.3: Vessel Transmits Vessel Voyage Information to VTS;
- Use case MT-UC3.4: Maritime Single Window Reporting.

6.1.3.5 Alternate Flows

We describe this use case's alternate flows in the relevant sub-use case sections.

6.1.3.6 Postconditions

The information has been received and the sender's identity has been verified.

6.1.3.7 Included Use Cases

As mentioned in Section **Error! Reference source not found.**, this use case is described through its sub use cases. These are compiled based on the actors (VTS, Vessel) and nature of communication (transmission or broadcast). The included use cases are the following:

1. Use case MT-UC3.1: VTS Transmits to Vessels;
2. Use case MT-UC3.2: Vessels Broadcast to Vessels;
3. Use case MT-UC3.3: Vessel Transmits Vessel Voyage Information to VTS;

4. Use case MT-UC3.4: Maritime Single Window Reporting;

6.1.3.8 Use Case MT-UC3.1: VTS Transmits to Vessels

VTS transmits information to vessels.

Stakeholders

See Section 6.1.3.1 for a complete list of stakeholders.

Actors

This use case includes the following actors:

- Vessel Traffic Service (VTS);
- Vessel.

Preconditions

VTS needs to send information to the vessel(s).

Basic Flow

1. VTS chooses what information to send:
    a. General VTS to vessels communication;
    b. Transmission of VDES bulletin board;
    c. Transmission of DGPS corrections;
    d. Transmission of weather reports;
    e. Transmission of manifestos.
2. Depending on the type of information, VTS determines whether this is sent directly to the receiver (3) or broadcast (3a);
3. VTS encrypts cargo and passenger manifestos;
4. VTS adds its signature to the information;
5. VTS sends the transmission to the vessel;
6. The vessel receives the transmission and checks that the signature is from the right VTS;
7. The vessel decrypts the transmission if it is encrypted.

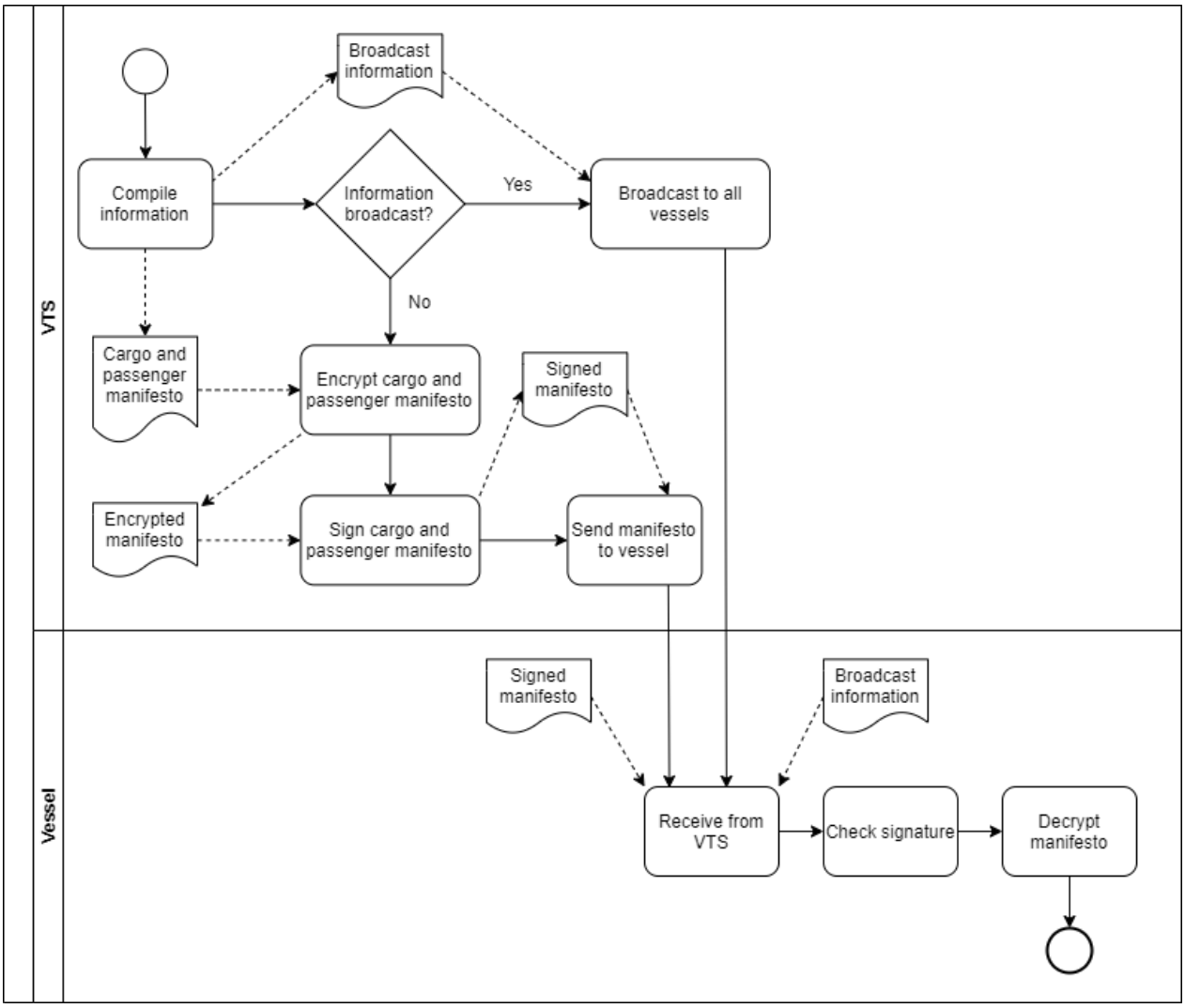

Figure 81: Maritime Transport – Use case MT-UC3.1: VTS transmits to Vessels.

Alternate Flows

1a. VTS signs the transmission;
2b. VTS broadcasts the transmission to all vessels;
3c. Return to Basic Flow 6.

Postconditions

The vessel has received the information and knows that it is from the right VTS.

6.1.3.9 Use Case MT-UC3.2: Vessels Broadcast to Vessels

Vessels broadcast information to vessels.

Stakeholders

See Section 6.1.3.1 for a complete list of stakeholders.

Actors

This use case has only one type of actor: Vessel.

Preconditions

Vessels need to send information to other vessels.

Basic Flow

1. The vessel chooses what information to send:
    a. General communication;
    b. AIS broadcasting.
2. The vessel adds its signature to the information;
3. The vessel broadcasts the information to other vessels;
4. The vessel receives the transmission and checks which vessel the signature is from.

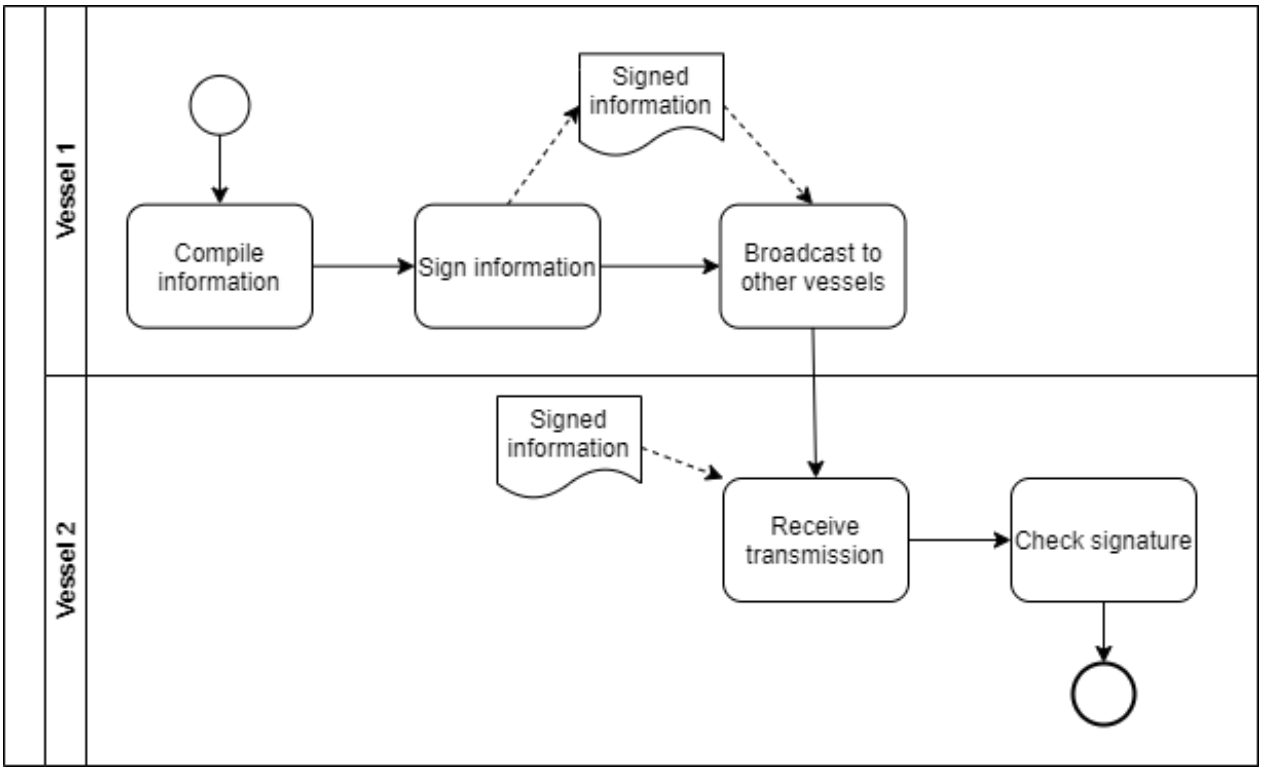

Figure 82: Maritime Transport - Use case MT-UC3.2: Vessels broadcast to vessels.

Postconditions

The vessel has received the information and knows which vessel it is from.

6.1.3.10 Use case MT-UC3.3: Vessel Transmits Vessel Voyage Information to VTS

Vessel transmits vessel voyage information to VTS.

Stakeholders

See Section 6.1.3.1 for a complete list of stakeholders.

Actors

This use case includes the following actors:

- Vessel Traffic Service (VTS);
- Vessel.

Preconditions

The vessel needs to send information to VTS.

Basic Flow

1. The vessel encrypts the route plans and mandatory SRS (Ship Reporting System) reports;
2. The vessel adds its signature to the information;
3. The vessel transmits the information to VTS;
4. VTS receives the transmission and checks which vessel the signature is from;
5. VTS decrypts the information.

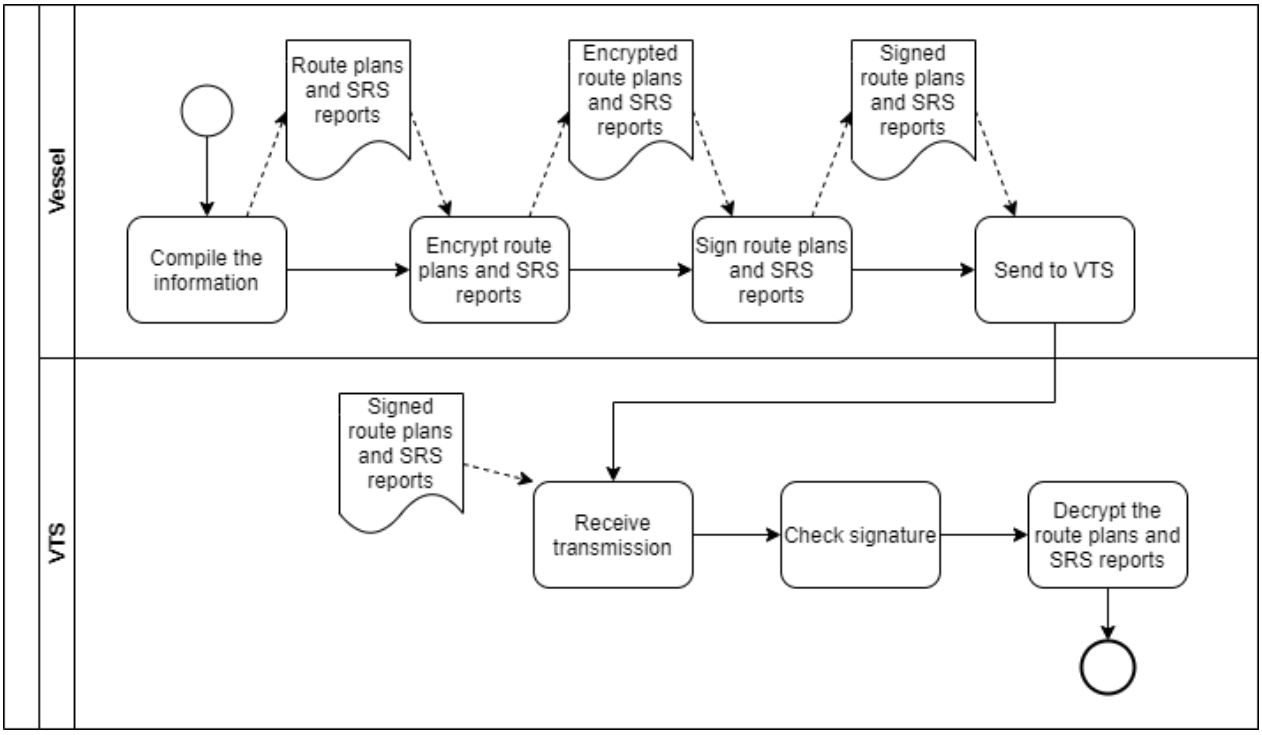

Figure 83: Maritime Transport - Use case MT-UC3.3: Vessel transmits vessel voyage information to VTS

Postconditions

VTS has received the information and knows which vessel it is from.

6.1.3.11 Use Case MT-UC3.4: Maritime Single Window Reporting

The vessel sends a report to the port.

Stakeholders

See Section 6.1.3.1 for a complete list of stakeholders.

Actors

This use case includes the following actors:

- Vessel;
- Port.

Preconditions

The vessel needs to send a report to the port.

Basic Flow

1. The vessel generates the report;
2. The vessel encrypts the report;
3. The vessel adds its signature to the report;
4. The vessel sends the transmission through the National Single Window;
5. The port receives the transmission and checks that the signature is from the right vessel;
6. The port decrypts the report.

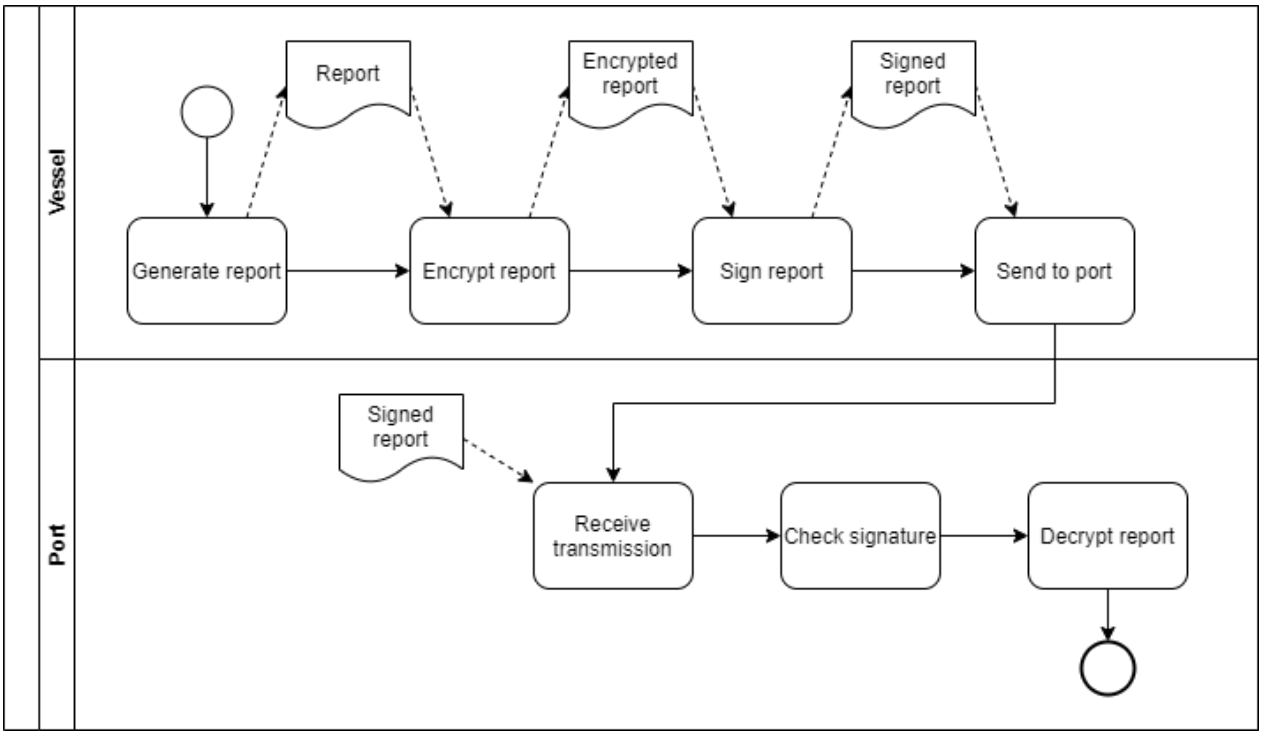

Figure 84: Maritime Transport - Use case MT-UC3.4: Maritime Single Window Reporting

Postconditions

The port has received the information and knows which vessel it is from.

6.1.4 Use Case MT-UC4: Trust Infrastructure for Secure Maritime Communication

Various types of information will be exchanged/transmitted between different maritime stakeholders and actors at sea and on-shore, using any of the existing or future communication systems (WiFi, VDES, SATCOM, etc.). Setting up and operating a trust infrastructure will enable these actors to authenticate themselves and securely exchange information. However, it is not straightforward to simply just set up and operate a security service for maritime communication, since there are a number of constraints associated with this particular domain. First, the solution has to be adapted to the large number of actors involved, which are owned and operation by many types of different organizations. For example, at the time of writing the International Maritime Organization (IMO) has 171 member states (flag states and port states) and there are between 100 000 and 150 000 ships that are sailing in international waters today. Second, the communication capacities of the different networks that ships use will need to be taken into account. In particular, the SATCOM component of VDES is

expected to become a bottleneck in ship communication, due to its low capacity. Also, ship often sail for long periods of time without any Internet connectivity at all. Third, shipping is a low cost business and this imposes strict limitations on what solutions that will be acceptable to the industry. Together, these constraints call for further research on the design and processes to operate the security solution and for demonstrations to show the feasibility of the proposed approach. This use case demonstrates the establishment and operation of a Public Key Infrastructure (PKI) service specifically adapted to fit the needs of the maritime domain.
As outlined in Figure 85, we will establish a three-level trust hierarchy in which the top-level Root CA and the intermediate CA will be operated by the PKI service provider. The PKI service can be used by a number of different actors that need to communicate securely; notably vessels, Vessel Traffic Services (VTS) and ports (in the next round, we may also choose to include other types of actors in the demonstrations). These actors are referred to as "end entities" in PKI terminology.

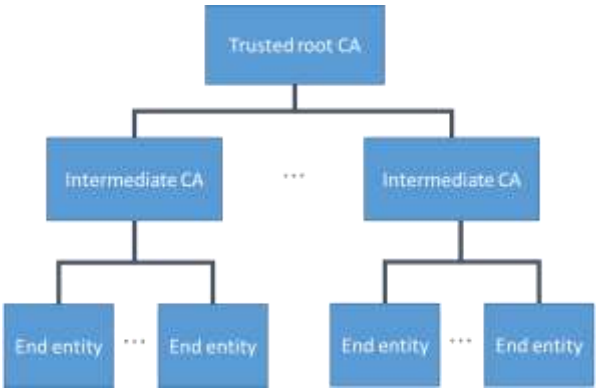

Figure 85: Maritime Transport - The Public Key Infrastructure (PKI) to be used in the demonstrations.

More details of the PKI can be found in the paper "*Protecting Future Maritime Communication*" [16] and in the CySiMS Service Evolution project deliverable "*D4.1 PKI Prototype Specification*" [17], which contain the design of the PKI service and a specification of its intended physical and logical realization.
The use case will be implemented and demonstrated through the following sub-use cases:

- Use case MT-UC4-1: Establishing the PKI;
- Use case MT-UC4-2: Operating the PKI.

6.1.4.1 Stakeholders

This use case comprises the following stakeholders:

- Port Authorities;
- Ship-owner;
- Cruise Operators;
- Public Administrations;
- Customs Authorities;
- Ministries.

These stakeholders apply to all the sub-use cases of MT-UC4. If a sub-use case includes additional stakeholders, we will report them it the sub-use case section.

For an exhaustive description of these stakeholders, please refer to [1].

6.1.4.2 Actors

This use case comprises one actor: the PKI Service Provider.

All the sub-use cases we will present leverage this actor. If a sub-use case includes additional, or different, actors, we will report them in the sub-use case's section.

For an exhaustive description of these actors, please refer to [1].

6.1.4.3 Basic Flow

The flow of this use case is presented through the sub-use cases presented below.

6.1.4.4 Postconditions

The PKI Service Provider is ready to enroll end entities. This means that the Intermediate CA is ready to receive Certificate Signing Requests (CSRs) from end entities.

6.1.4.5 Use Case MT-UC4.1: Establishing the PKI

This sub-use case shows how to establish the PKI and it contains the following processes:

1. Root CA establishment;
2. Intermediate CA establishment.

Stakeholders

See Section 6.1.4.1 for a complete list of stakeholders.

Actors

See Section 6.1.4.2 for a complete list of actors.

Basic Flow

Process 1: Root CA Establishment

This process will be realized by the following events:

- Event 1: The PKI service provider generates a private-public key pair for the Root CA;
- Event 2: The PKI service provider generates a self-signed Root CA certificate;
- Event 3: The PKI service provider stores the Root CA private key in a secure (offline) location;
- Event 4: The PKI service provider stores the Root CA certificate in the Intermediate CA webserver.

This process will only be done once.

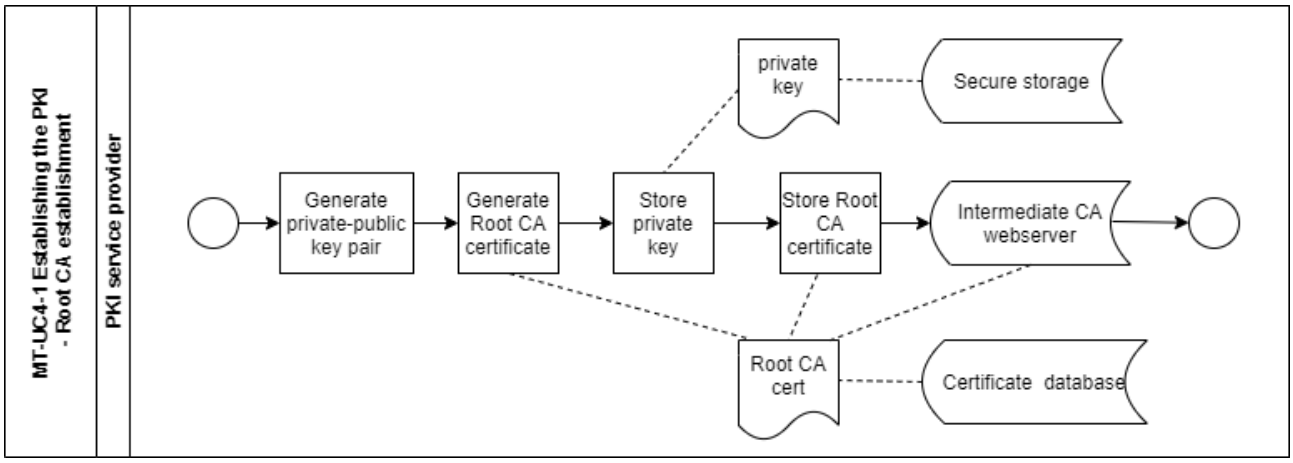

Figure 86: Maritime Transport - Use case MT-UC4.1: Establishing the PKI – Root CA establishment (Process 1)

Process 2: Intermediate CA Establishment

This process will be realized by the following events:

- Event 1: The PKI service provider generates a private-public key pair for the Intermediate CA;
- Event 2: The PKI service provider generates a certificate signing request (CSR) for the Intermediate CA;
- Event 3: The PKI service provider transfers the CSR to the secure (offline) location;
- Event 4: The PKI service provider uses the Root CA private key to sign the CSR;
- Event 5: The PKI service provider stores the signed Intermediate CA certificate in the Intermediate CA webserver.

This process will be done once for each intermediate CA that will be used in the demonstrators.

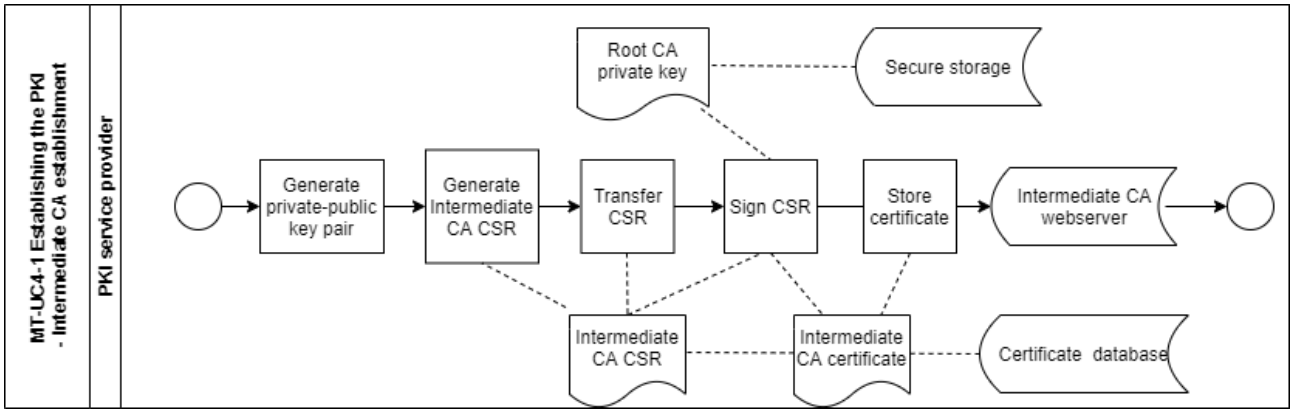

Figure 87: Maritime Transport - Use case MT-UC4.1: Establishing the PKI – Intermediate CA etsablishment (Process 2)

Postconditions

There are no postconditions to this use case.

6.1.4.6 Use Case MT-UC4.2: Operating the PKI

This sub-use case shows how to operate the PKI and it contains the following processes:

1. Enrolment of new end entities into the PKI;

2. Renewal of certificates for existing end entities in the PKI;
3. Revocation of end entity certificates from the PKI.

Stakeholders

See Section 6.1.4.1 for a complete list of stakeholders.

Actors

In addition to those listed in Section 6.1.4.2, this use case comprises the following additional actors:

- End Entities (Vessels/VTS/Ports, etc).

Preconditions

The use case MT-UC4.2: Establishing the PKI has been executed. This means that the Root CA and the Intermediate CA have been established and that the Intermediate CA is ready to receive Certificate Signing Requests (CSRs) from end entities.

Basic Flow

Process 1: Enrolment of new end entities into the PKI.

This process will be realized by the following events:

1. The end entity generates a private-public key pair;
2. The end entity generates a certificate signing request (CSR);
3. The end entity submits the CSR to the Intermediate CA webserver;
4. The PKI service provider fetches the CSR;
5. The PKI service provider verifies that the end entity belongs to its flag state;
6. The PKI service provider uses the Intermediate CA to sign the CSR;
7. The PKI service provider stores the signed certificate in the Certificate database;
8. The end entity fetches the certificate from the Intermediate CA webserver.

This process is repeated for all of the end entities that will be part of the trust infrastructure.

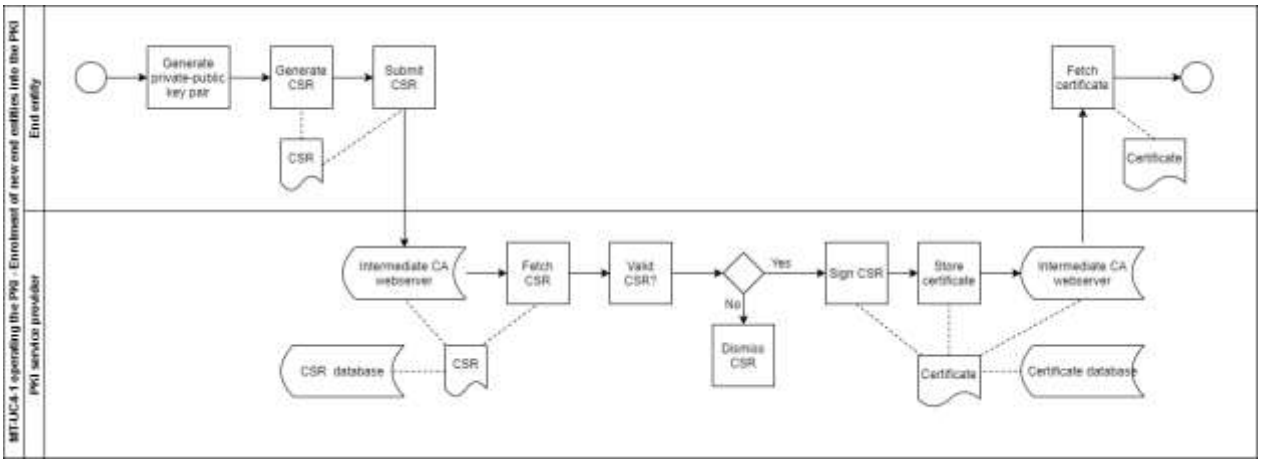

Figure 88: Maritime Transport - Use case MT-UC4.2: Operating the PKI – Enrolment of new end entities into the PKI (Process 1 and 2)

Process 2: Renewal of certificates for existing end entities in the PKI.
This process will be triggered when the current end entity certificate is about to expire. The process will be realized by similar events as Process 1 described above.

Process 3: Revocation of end entity certificates from the PKI.
This process will be realized by the following events:

1. The PKI service provider is notified that an end entity certificate needs to be revoked;
2. The PKI service provider uses the Intermediate CA to generate and sign a certificate revocation list (CRL);
3. The PKI service provider stores the CRL in the Intermediate CA webserver;
4. End entities fetch the CRL from the Intermediate CA webserver.

This process is repeated every time an entity needs to be revoked from the PKI.

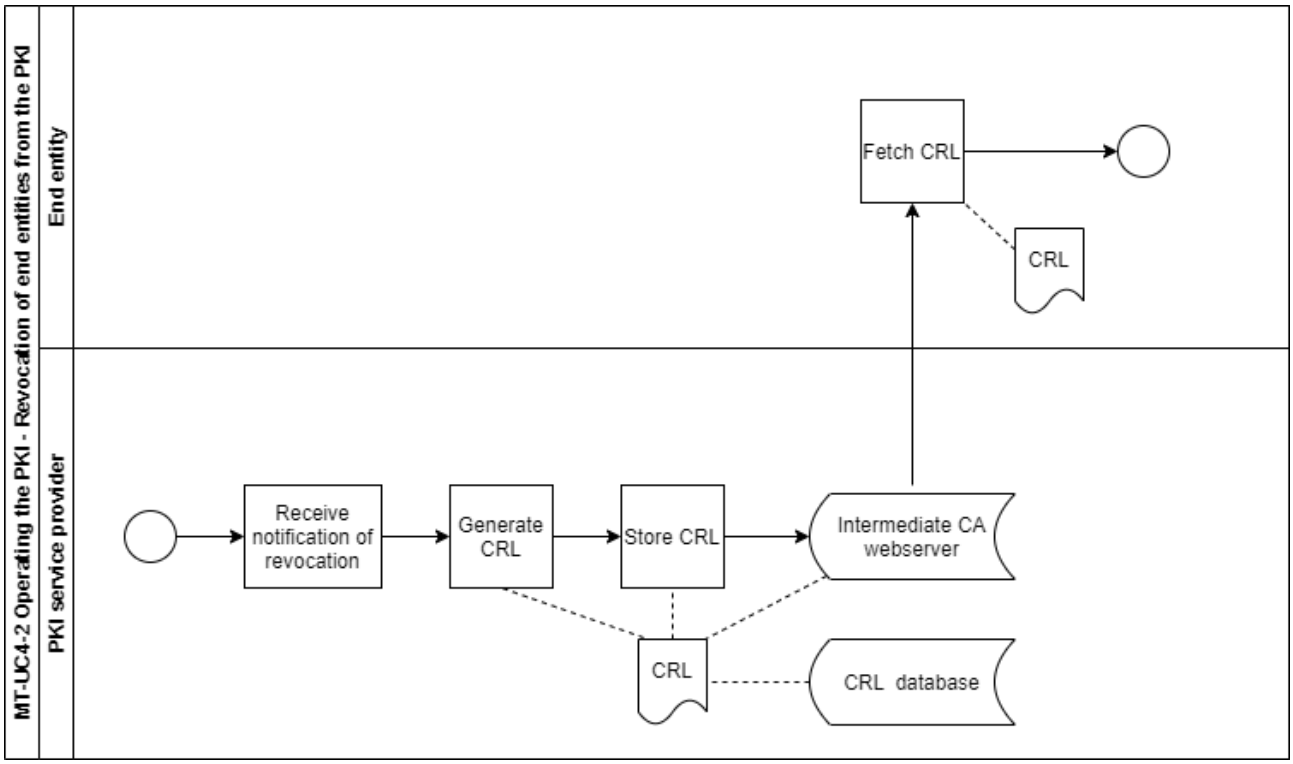

Figure 89: Maritime Transport - Use case MT-UC4.2: Operating the PKI – Revocation of end entities from the PKI (Process 3)

Postconditions
All end entities in the PKI (Vessel/VTS/Port) have private keys and valid signed certificates that can be used for secure communication.

6.2 Demonstrator Set-up

For the Maritime Transport vertical, three demonstrators will be presented:

- MT-D1: Threat modelling and risk analysis for maritime transport services;
- MT-D2: Maritime system software hardening;

- MT-D3: Secure maritime communications and Trust infrastructure for secure maritime communication.

6.2.1 Demonstrator MT- D1: Threat Modeling and Risk Analysis for Maritime Transport Services

6.2.1.1 Relation to Use Cases

During the first phase of the demonstrator, the sub-use cases contained in MT-UC1 will be show-cased:

- MT-UC1.1: Assets Identification and IT infrastructure Representation;
- MT-UC1.2: Maritime Services Analysis and Representation;
- MT-UC1.3: Vulnerabilities Management;
- MT-UC1.4: Threat Scenarios Specification;
- MT-UC1.5: Maritime Transport Risk Analysis;
- MT-UC1.6: Attack Paths Generation and Representation;

MT-UC1.7: Maritime Transport Risk Management.

6.2.1.2 Relation to WP3 Assets

The current demonstrator is built based on multiple assets from work package 3, which we list in what follows.

MITIGATE

MITIGATE aims at realizing a radical shift in risk management for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment approach. To this end, MITIGATE has integrated an effective, collaborative, standards-based risk management system for port's CIIs, which shall consider all threats arising from the SC, including threats associated with port-CIIs interdependencies and associated cascading effects. The proposed system enables port operators to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from the ports' SC. In this way, port operators can to predict potential security risks, but also to mitigate and minimize the consequences of divergent security threats and their cascading effects in the most cost-effective way, i.e., based on information associated with simulation scenarios and data acquired from online sources and repositories (e.g., National Institute of Standards and Technology (NIST) Repositories).

The MITIGATE system incorporates a bundle of automated processes and routines and integrates a wide range of ICT tools which enable port operators in structuring, organizing and managing assets and threats, as well as in executing simulation scenarios and deriving evidence-based knowledge that will be used for the identification, classification, assessment, simulation and mitigation of risks associated with port CIIs. Hence, these concepts can also be used for CyberSec4Europe to facilitate the analysis and propagation of a threat and risk in a structured and well-defined way. In this context, the MITIGATE system is a good candidate tool to be used in order to design and develop the proposed CyberSec4Europe Maritime RA system.

MEDUSA

The MEDUSA Risk Assessment methodology aims to provide a systematic approach to evaluate the security

risks affecting the supply chain business partners within a Supply Chain Service (SCS). In particular, Medusa can be applied to assess the overall risk of a SCS, as well as the risk associates with each individual business partner within an SCS. The derived overall risk values are used in order to generate a baseline SCS security policy, identifying the least necessary security controls for each participant in the SCS. In addition, Medusa allows the risk assessor to assess the risk of cascading threat scenarios which may be realized within an SCS. The study of the cascading scenarios takes into consideration the graph relations of a potential source of a threat as well as the business role of each participant by utilizing weights of business importance. Medusa enables all the SCS participants to fine-tune their security policies according to their business role in the examined SCS. The main goal of MEDUSA methodology is to increase the preparedness of the business partners, while at the same time enables the coordination of their efforts towards effectively identifying and treating their risks.

The proposed CyberSec4Europe Maritime RA system will take advantage of the multi-order risk assessment and impact assessment capabilities (based on graph-theory algorithms) for identifying/assessing risks, threats and security events and estimate their impact in interdependent infrastructures.

6.2.1.3 Description and Workflow

The demonstrator MT-D1 will be illustrated through a web application utilizing multiple modules that aim in a complete risk assessment process. User accounts will be provided to the users, through which they will gain access to the system and start the risk assessment procedure. There will be a walkthrough and a set of instructions concerning the sequence of information insertion which will ultimately lead to a complete Asset Map and multiple informative Risk Assessment Result output forms. In the context of the Risk Assessment Results MT-D2 will act as an enabler for MT-D1, since the hardening services will be considered as mitigation measures for certain threats.

CyberSec4EuropeMaritime System is an innovative web application that encourages maritime stakeholders, security operators and involving participants (i.e., ICT experts, SCADA operators, etc) to collaborate, in order to identify, analyse, assess and prevent or mitigate risks associated with cyber assets of the maritime transport. To accomplish this, the maritime system adopts and implements a bouquet of flexible and configurable self-driven services (CyberSec4Europe Maritime RA Services): *Maritime Transport Service Modelling, Vulnerabilities Management and Open Intelligence, Threats/Controls Management and Open Intelligence, Threat Scenarios Specification, Supply Chain Risk Analysis. Attack Paths Simulation and Risk Management.* These services will operate to conduct a thorough risk analysis of the cyber assets involved in the maritime transport case. The CyberSec4Europe Maritime RA Services are presented below.

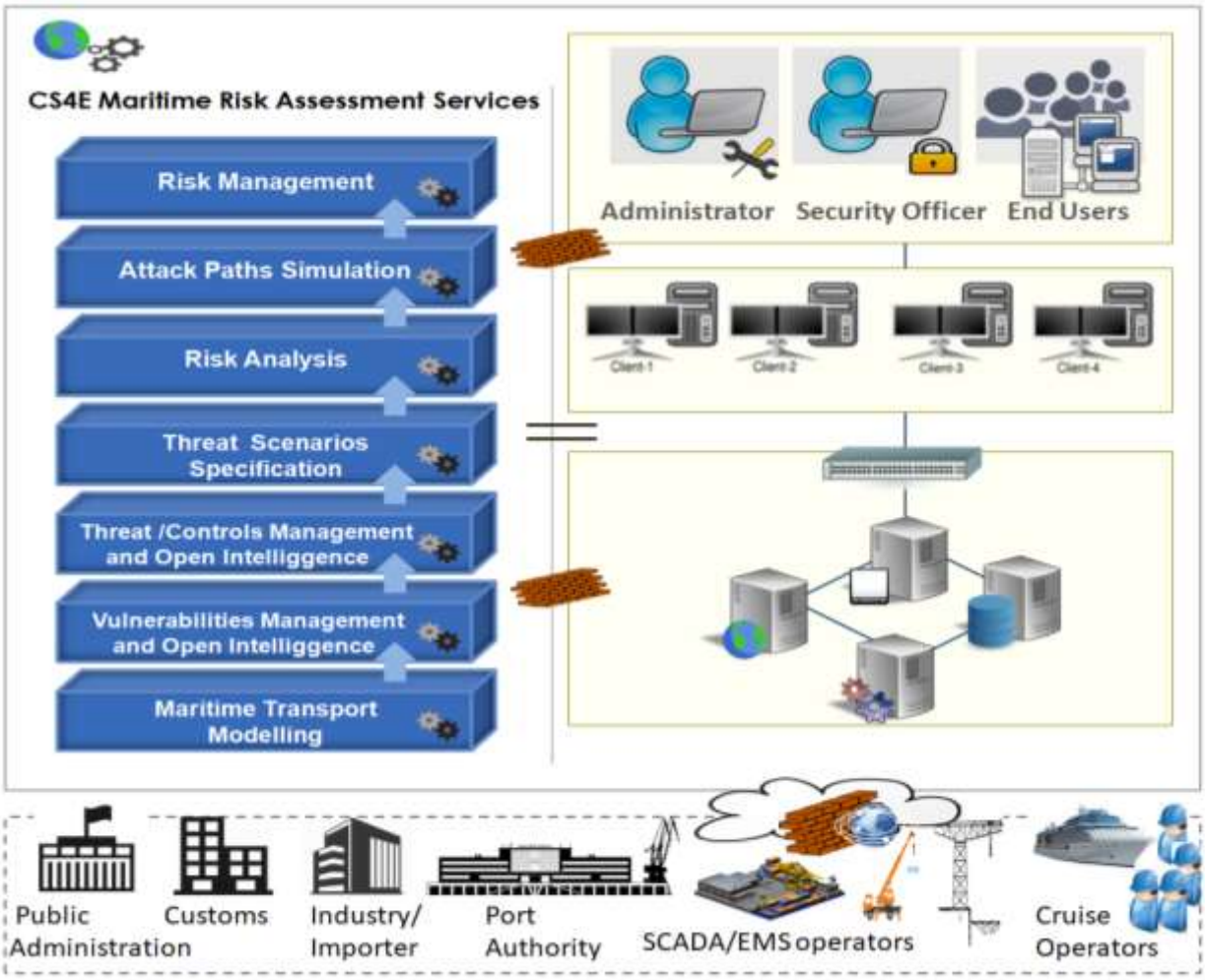

Figure 90: The Risk Assessment Services of the CyberSec4Europe Maritime Transport System

Maritime Transport Service Modelling Service

The current service aims to identify, analyse and model key-assets/infrastructures that operating within the maritime transport case along with the involving key-participants (maritime transport stakeholders) and their roles (primary/secondary actors). Consequently, this security assessment service delivers a maritime cyber-asset inventory engaging a set of characteristics, such as the type of asset, vendor, version, etc. Therefore, the asset inventory includes all computing (desktops, notebooks, servers) and networking related devices (switches, routers, etc.) printers, appliances (network attached storage, network capable cameras, etc.), applications and IT systems in general owned, managed, or otherwise used by the maritime logistics operators. Such devices are vessel traffic monitoring systems, intermodal maritime-based logistics, SCADA components, such as Human Machine Interface (HMI), Master Terminal Unit (MTU), Programming Logic Controllers (PLCs), sensor systems, controllers for stevedoring equipment (i.e., gantry cranes, trailers and forklifts).

Additionally, the MITIGATE service provides a visualization of the entire infrastructure, which expands the cyber-assets knowledge and improves the data sharing of the spectrum.

Vulnerabilities Management and Open Intelligence Service

This service targets at providing information to the maritime stakeholders regarding the identified vulnerabilities associated with the cyber assets declared in the previous service. The service acts as a central repository for all known and unknown/undisclosed vulnerabilities. It makes use of open data sources, such as the CVE Details portal which presents the disclosed vulnerabilities, replicating all the confirmed and known vulnerabilities and associates them with the affected assets via synchronization mechanisms and knowledge-based rules. Unknown/undisclosed vulnerabilities can be, additionally, declared and treated by the maritime transport stakeholders. In order to quantify vulnerabilities, a set of metrics is considered:

- The access vector showing how vulnerability can be exploited;
- The attack complexity illustrating how easy or difficult is to exploit the discovered vulnerability;
- The authentication describing the number of times that an attacker must authenticate to a target to exploit it;
- The confidentiality outlining the impact on the confidentiality of data processed by the asset;
- The availability describing the impact on the availability of the target asset;
- The integrity describes the impact on the integrity of the exploited asset.

Threats/Controls Management and Open Intelligence Service

The current service aims to arm maritime transport stakeholders with the appropriate tools and solutions to provide them threat awareness regarding their involving assets and to indicate them the implemented security controls and allow them to deeper understand their use; how they can be either deployed or applied in order to mitigate the risks and confront the defined threats and weaknesses. In this context, the maritime system acts as a knowledge base of identified threats engaging corresponding mitigation controls that can be used to counter such security issues. This service adopts the CAPEC classification of MITRE, which synchronizes the MITRE attack identifiers and associates the identified vulnerabilities with one or more weakness identifiers. Custom threats can be declared by maritime transport stakeholders. Furthermore, the service supports the creation and customization of security controls, which are categorized into two types: “Maritime Transport Threats” and “Maritime Transport Vulnerabilities”.

Threat Scenarios Specification Service

The goal of the current service is to employ maritime stakeholders with alternative threat scenarios to help them realize the consequences deriving from the identified threats and vulnerabilities on their cyber-assets. Threat scenario is assumed a use case in which a threat can compromise an asset by exploiting vulnerabilities and weaknesses as well as taking advantage of the lack of adequate security controls. The service provides the capability to declare statically the mapping of threats and vulnerabilities with assets to increase the cybersecurity awareness of maritime transport stakeholders using semantic frameworks and reasoning mechanisms.

Supply Chain Risk Analysis Service

The particular service provides guidance to the maritime transport stakeholders to assess and organize their cybersecurity issues. In this vein, the system encompasses and executes an evaluation process that implements the main steps of the risk assessment process in order to identify and measure all relevant cyber threats and vulnerabilities, estimate the possible impacts and identify and prioritize the corresponding risks. Moreover, the service provides the cyber assets’ risk exposure concerning the following three main types of risks: (i) individual risk, which represents how dangerous a threat appears on a specific cyber asset, (ii) the cumulative risk, which estimates the risk exposure of the successful exploitation of multiple vulnerabilities, targeting a specific cyber asset starting from different entry points and (iii) the propagated risk, which shows how deep

into the network an attacker may penetrate in case he successfully exploits vulnerabilities found in asset entry points dealing with threats.

Risk Assessment is initiated on the declared cyber assets. The Supply Chain Risk Analysis service supports two types of risk assessment: “Real” and “Simulation”. The key difference is that simulation allows operators to further customize their cyber assets by altering the security information on them; disregard certain vulnerabilities and threats, amend the threat probability indicators and add more or replace security controls while the “Real” risk assessment type does not permit such alterations. Furthermore, the simulation mode offers a virtual playground where asset cartography has been cloned and thus it permits to run dynamically different mitigation strategies without affecting the status of the real asset inventory.

Attack Paths Simulation Service

The service implements an attack-path discovery approach that relies on unique characteristics, such as the attacker’s location, the attacker’s capability, assets interdependencies and which the entry and target points are in order to return all attack paths that exist in the underlying assets. The service supports the calculation and rendering of all the relevant attack graphs representing the different paths a cyber-attacker may follow to reach and harm a targeted asset. The operator can see all the potentially affected assets and their individual relationships. This attack path generation and visualization are carried out by the execution of logic rule-based reasoning mechanisms, that are capable of developing all alternative chains of sequential vulnerabilities on the underlying assets following an attack-path discovery method.

Risk Management Service

The vulnerabilities trees, produced during the Attack Path Simulation Service, expose the risks embedded in the individual cyber assets. Thereupon, the maritime stakeholders are guided by recommendations on the selection of the most appropriate security controls, indicating optimization practices, to minimize the expected damage. In this vein, the service assures an acceptable risk level for collaborative business partners. Furthermore, the proposed system provides the necessary defensive capabilities and supports rational decision-making to determine which security controls must be implemented and which partners need to implement them to encounter the identified security issues and cyber-risks.

6.2.1.4 Target Group

A range of maritime stakeholders with interest in the security and risk management processes, including ports’ providers, entities interacting with the ports’ ICT systems (i.e. maritime companies, customs, providers), security companies/experts, auditors, maritime integrators, maritime R&D organizations, standardization and agencies bodies (e.g. IMO, EMSA, ENISA) and more will be contacted and motivated to participate in the Demonstrator MT- D1 “Threat Modeling and Risk Analysis for Maritime Transport Services”. These stakeholders will be mobilized through the business networks of the partners and through the partners’ participation in relevant standardization and agencies. In particular, visibility activities include:

- sending personal and public invitations (by e-mail);
- promoting workshop events to maritime communities;
- inviting maritime stakeholders based on contact information that has been collected so far by networking in conferences and workshop events;
- engaging other stakeholders to communicate with their contact points, motivate potential end-users.

It should be note that the “Maritime Transport” demonstration case aims to address the need for a robust, highly efficient and user-friendly risk management tool. To this end, a radically new collaborative and more integrated

approach will be introduced, which emphasizes risk assessment, simulation and mitigation not only of conventional risks, but also of multi-sector risks that are associated with highly interconnected and complex processes and their cascading effects. The proposed CyberSec4Europe Maritime Transport RA approach has been designed and developed to be modular, extensible, scalable, interoperable and secure, while being capable of providing invaluable insights into the cyber risk of any organization. Some of the benefits of using the proposed solution are the following:

- *Reduction of security breaches costs*: In the digital era, the organizations are facing security and privacy breaches. A breach can cause either direct costs such as fines imposed by regulators or compensation payments to customers or even indirect costs, for example through the loss of intellectual property or revenue leakage. The CyberSec4Europe Maritime Transport RA system provides important decision support for improving the organizations risk situation;
- *Compliance with legal and regulatory security regimes, frameworks and standards*: The compliance of the organizations with a set of legal, regulatory and standardization security framework is a prerequisite of cooperation with other organizations which set similar security requirements to their suppliers. The usage of the CyberSec4Europe Maritime Transport RA system improves their organizations' compliance with security standards (e.g. ISO27001, ISO27002);
- *Reputation protection and image improvement*: A responsible and progressive stand in information security and information protection including the protection of privacy and proprietary information of the enterprises themselves protect their reputation and brand. This CyberSec4Europe Maritime Transport RA system will enable organizations to boost their corporate reputation gaining the customers' confidence, strengthen the ICT security and data privacy level of their e-services; increase their business processes sustainability and thus improve their competitiveness.

Additional service/product offering: A good enough security management is a precondition to maintain existing products and services and to generate new products and services. Therefore, information security is fundamental to business continuity for the organizations.

6.2.2 Demonstrator MT- D2: Maritime System Software Hardening

6.2.2.1 Relation to Use Cases

During the first phase of the demonstrator, the use case MT-UC2 "*Maritime system software hardening Processes*" will be show-cased:

- Identification of unsafe software components;
- Analysis of identified components;
- Application of software hardening;
- Acceleration through hardware support.

6.2.2.2 Relation to WP3 Assets

The current demonstrator is built based on multiple assets from Work Package 3, which we list in what follows.

TypeArmor

TypeArmor utilizes binary-level analysis techniques to significantly reduce the number of possible targets for indirect call sites. More specifically, TypeArmor reconstructs a conservative approximation of target function prototypes by means of use-def analysis at possible callees. We then couple this with liveness analysis at each

indirect call site to derive a many-to-many relationship between call sites and target callees with much higher precision compared to prior binary-level solutions. TypeArmor is efficient—with a runtime overhead of less than 3%.

VTPin

VTPin protects against VTable hijacking, via use-after-free vulnerabilities, in large C++ binaries that cannot be re-compiled or re-written. The main idea behind VTPin is to *pin* all the freed VTable pointers on a safe VTable under VTPin's control. Specifically, for every object deallocation, VTPin deallocates all space allocated, but preserves and updates the VTable pointer with the address of the safe VTable. Hence, any dereferenced dangling pointer can only invoke a method provided by VTPin's *safe* object. Subsequently, all virtual-method calls due to dangling pointers are not simply neutralized, but they can be logged, tracked, and patched.

6.2.2.3 Description and Workflow

The demonstrator MT-D2 will be illustrated in two distinct cases: (a) enhancing the risk analysis framework realized in MT-D2, and (b) hardening unsafe components used in MT-D3. More precisely, MT-D2 will act as a further enabler for MT-D1 and MT-D3. Below, we discuss how MT-D2 will act in the context of both MT-D1 and MT-D3.

Enhancing Risk Analysis

MT-D1 offers a complete framework for risk analysis designed for the maritime section. The demonstrator operates through a web application that is capable of illustrating interesting, from a security perspective scenario, and further modelling them. MT-D2, in this context, will further assess the existence of unsafe components, illustrate the risks that stem from them and highlight mitigation actions.

Hardening Unsafe Components in Maritime Communication

MT-D3 offers secure communication in the maritime domain by means of certain cryptographic protocols and primitives. In this context, MT-D2 will apply hardening to unsafe components that perform the cryptographic operations (e.g., the OpenSSL library) for ensuring that cryptography is not bypassed through software exploitation. For both cases, here is the work-flow of the processes happening as part of MT-D2.

Identification of unsafe software components.

Unsafe components are software modules that are written in C/C++ the do not include runtime support for memory handling. These components are all vulnerable to memory errors, which can be leveraged by software exploitation for compromising the vulnerable module (and sometimes, the entire system). Given a software base, this process identifies all components that are considered unsafe. This process is also enabled to the web application realized in MT-D1 and is applied to all software used for communication in MT-D3.

Analysis of identified components.

Once components are identified, they are further analyzed for: (a) exact identification of their properties (e.g., the programming language used, existing defenses enabled), (b) exact identification of available resources (availability of source code of the main binary and other shared libraries), (c) threat analysis (knowledge of relevant vulnerability classes, knowledge of existing vulnerabilities). This analysis will produce a more detailed profile of the application to be hardened. This analysis is also enabled to the web application realized in MT-D1 and is applied to all software used for communication in MT-D3.

Application of software hardening.
Once the application profile is constructed then hardening can be applied based on the profile and the available options. The web application of MT-D1 will have guidelines for this step, while hardening will be applied all identified and analyzed unsafe software used for communication in MT-D3.

Acceleration through hardware support.
In cases where certain hardware is available, hardening can utilize it for speeding up the final hardened program. This is an optional step, which may be applied to hardened software used for communication in MT-D3.

6.2.2.4 Target Group

Securing systems used in the maritime sector could have an immediate impact on software vendors that are active in this sector, as well as implicit impact on other related entities, such as Ship-owner companies and Cruise Operators. These entities can be potential target groups for this demonstrator, since a secure IT infrastructure in the maritime sector can benefit their operation in the long run.

6.2.3 Demonstrator MT- D3: Secure Maritime Communications and Trust Infrastructure for Secure Maritime Communication

6.2.3.1 Relation to Use Cases

During the first phase of the demonstrator, the sub-use cases contained in MT-UC3 and MT-UC4 will be show-cased:

- MT-UC3: Secure maritime communications:
  - MT-UC3.1: VTS Transmits to Vessels;
  - MT-UC3.2: Vessels Broadcast to Vessels;
  - MT-UC3.3: Vessel Transmits Vessel Voy-age Information to VTS;
  - MT-UC3.4: Maritime Single Window Reporting;
- MT-UC4: Trust infrastructure for secure maritime communication
  - MT-UC4.1: Establishing the PKI;
  - MT-UC4.2: Operating the PKI.

6.2.3.2 Relation to WP3 Assets

The demonstrator will implement the asset "PKI service". In addition, the WP3 asset "BowTiePlus" will be used to model and analyze threats that are relevant for the demonstrator.

6.2.3.3 Description and Workflow

In phase 1, only the PKI service will be demonstrated (i.e., only the use cases in MT-UC4). In phase 2, we will demonstrate how to use the PKI service to secure maritime communications (i.e., both all the use cases in MT-UC3 and MT-UC4). In addition, the PKI service demonstrated in MT-D3 will as act as an enabler for MT-D2, since the PKI service itself will undergo a hardening procedure. Figure 91 and Figure 92 outline phase 1 and phase 2 of the demonstrations, respectively

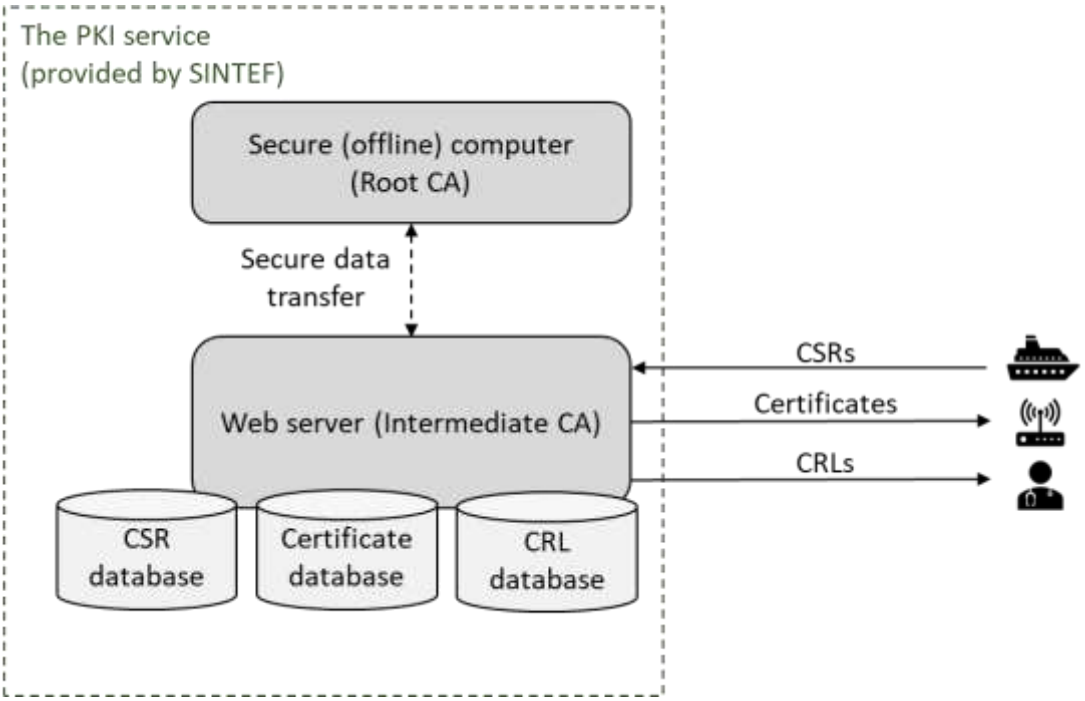

Figure 91: Maritime Transport - Overview of the demonstrator's first round.

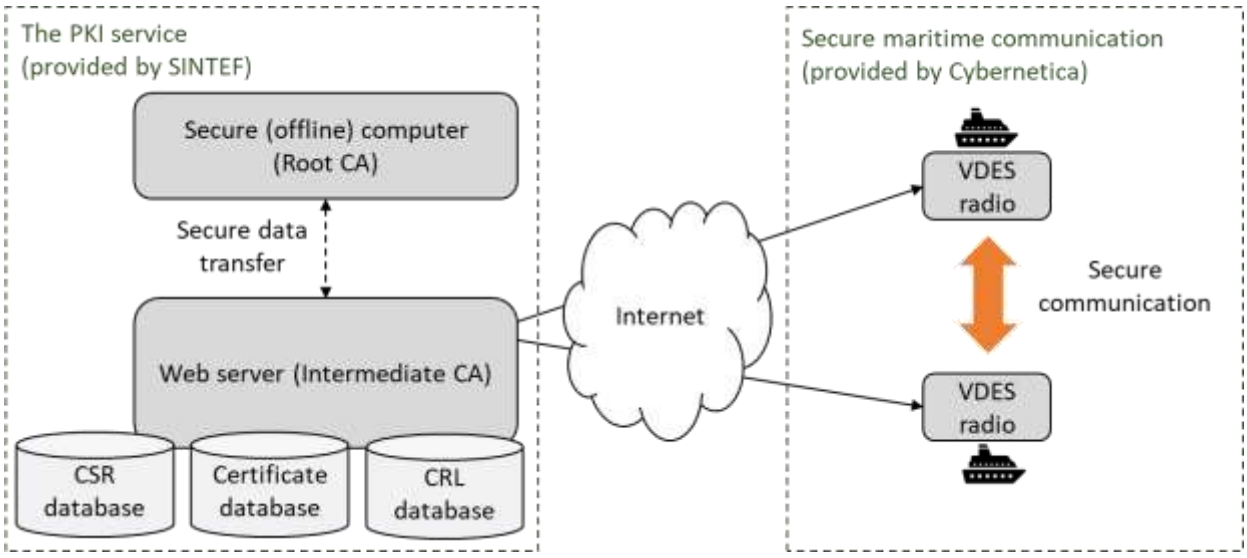

Figure 92: Maritime Transport - An overview over the physical realisation of the demonstrator's second round.

6.2.3.4 Target Group

The most important target groups are:

- The International Maritime Organisation (IMO), which is the organization standardizing the use of the technologies developed in these use cases. They are considering standardizing the use of PKI in the maritime domain and with our demonstration we aim to showcase to them such a technology could be implemented and used in practice. We will reach them by submitting an input paper to their upcoming Facilitation Committee 44th session (FAL 44), which originally was planned for April 2020 but that has now been postponed until fall 2020. We also plan to submit a request for doing a demonstration during this event;

- The Norwegian Maritime Authority, which is the administrative and supervisory authority in matters related to the safety of life, health, material values and the environment on vessels flying the Norwegian flag and foreign ships in Norwegian waters[38]. This organisation is a potential candidate for establishing and operating the PKI service. We are already in contact with them and we are currently discussing the technical and procedural details for setting up a demo version of the PKI in their premises. They will benefit because it will provide them with experience of the feasibility of them operating such a service;
- Kongsberg Seatex, which will deliver the VDES technology that will be used for ship-to-ship and ship-to-shore communication; They are currently participating in a national funded project called CySiMS[39], in which they will demonstrate the use of our PKI, using their VDES radio prototype as the communication link between ships and the shore. They will benefit because of the possibility to showcase an interesting use case where their own technology will be a true enabler;
- Kongsberg Defence, which is considering offering secure onboard storage capabilities for the PKI solution. As with Kongsberg Seatex, they are also participating in the CySiMS project and they will also benefit because the PKI can be used to showcase the use of their own technology.

[38] Norwegian Maritime Authority. https://www.sdir.no/en/
[39] Cybersecurity in Merchant Shipping. http://cysims.no/

7 Medical Data Exchange

As indicated in the main goals stated in the document ofrequirements document [1], the Medical Data Exchange demonstrator is intended to increase the trustworthiness between stakeholders when sharing medical data through a marketplace platform thus generating new business opportunities. This will be achieved by using a real environment provided by the Dawex[40]Data Exchange Platform (DEP), which will offer to the users the following services:

- An anonymization service and a functional encryption service for increasing the user privacy and security when sharing data;
- A cross-border strong authentication mechanism, in addition to a decentralized identity management for allowing a more secure access to the medical data platform;
- A visualization tool which comprises data assessment and data sampling tools (e.g. histogram, tree map, heatmap, data typing, sample) for giving a graphical overview of the data, to improve the user experience when the user accesses the data catalogue.

A high-level overview of this scenario including the services and tools to be used is displayed in Figure 93. A more detailed description is provided in the following sections.

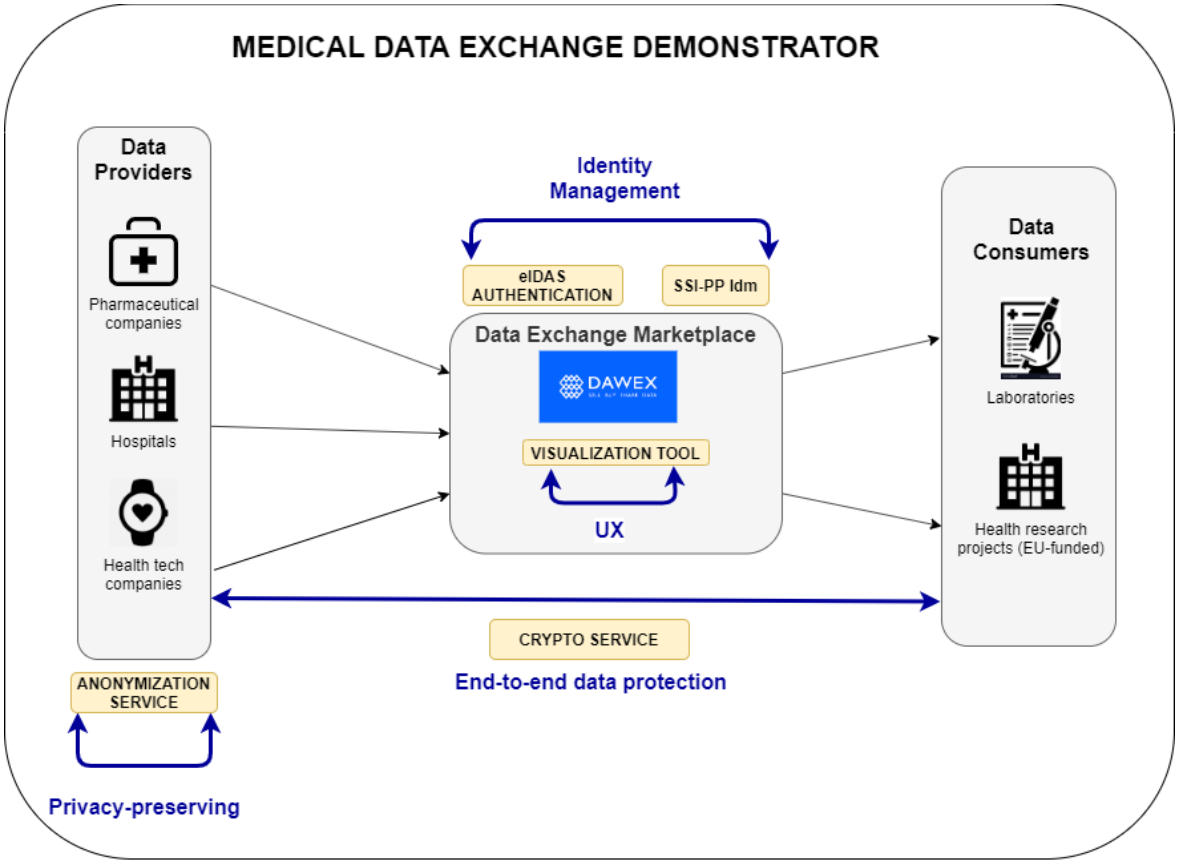

Figure 93: Medical Data Exchange - Services general view

7.1 Use Cases Specification

Three – MD-UC1 Sharing Sensitive Health Data through an API, MD-UC2 Sharing Sensitive Health Data through Files, and MD-UC3 Enhancing the Security of On-Boarding and Accessing the Dawex Platform –

[40] https://www.dawex.com/en/data-exchange-platform/

uses cases were described on a high-level view in the requirements document [1]. In the following sections a more detailed information and specifications are provided.

7.1.1 Use case MD-UC1: Sharing Sensitive Health Data through an API

Use case MD-UC1 comprises the following four main phases:

- The data providers gather personal and health data. Aggregation of these data coming from different sources, and some analytics could be performed. The data are protected by using privacy preserving techniques;
- The data consumers select the data from the marketplace catalogue, based on the related metadata provided by the data providers;
- The data consumers contact the data providers for agreeing on terms and conditions regarding the exchange of the data. Contract services are provided by the data exchange platform;
- Once the data consumers receive the protected data, through the APIs offered by the data provider, they are able to perform the appropriate analytics depending on the privacy preserving techniques already used by the data provider.

It is worth mentioning that the data subjects' privacy is preserved at all times by using privacy preserving techniques.
The protection of the data using the Privacy-enhancing technologies (PETs) will be performed during the second phase of the development of the demonstrator.

Figure 94 shows the use case diagram for the MD-UC1.

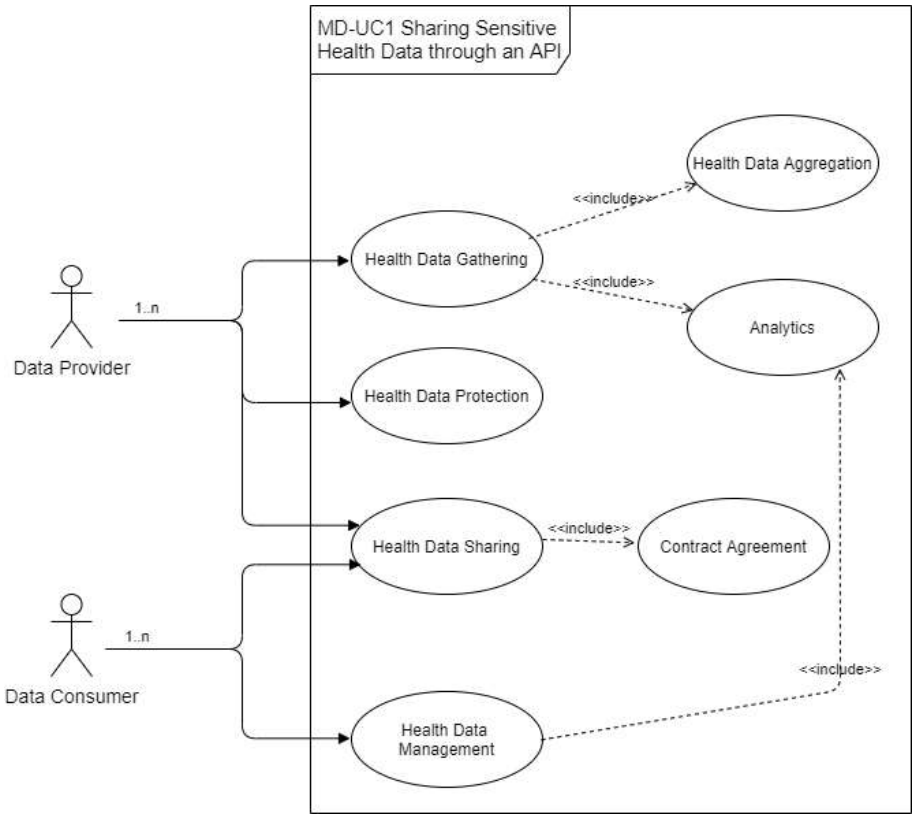

Figure 94: Medical Data Exchange - UML diagram for MD-UC1 sharing sensitive health data through an API

7.1.1.1 Stakeholders

The data exchange management particularly in the health domain which deals with personal and sensitive data, implies that several stakeholders are involved. In use case MD-UC1 the stakeholders are the following:

- **Policymakers** are responsible of developing laws and regulations related to personal data protection (GDPR) and also monitoring regulatory fulfilment when persona data are shared. Namely both country and EU health authorities, and legal and regulatory bodies, have the goal to provide the legal framework to protect data subject rights;
- **Data subjects** are the owner of the personal and sensitive health data. Their consent is needed for sharing health data with third parties (e.g. persons or patients wearing devices/wearables which are data sources);
- **Data providers** will be considered as legal persons (e.g., health tech companies, hospitals, pharmaceutical companies) which upload personal and health data from data subjects from several data sources. The data providers can aggregate this kind of data, performing data analytics with them, playing also the role of data aggregator;
- **Data aggregators** are represented by health tech companies, municipalities, health data hubs and health consortiums, and are able to perform aggregation and analytics on the health data;
- **Data consumers** stakeholders are public and private research organizations, health authorities, hospitals and pharmaceutical companies, which are using the protected data;
- **Data exchange marketplaces providers** are the marketplace owners. They are in charge of connecting the data providers with the data consumers for sharing sensitive health data, assuring at any moment the data subject's privacy across the marketplace. Services for compliance with current regulations and for assuring the data subject's rights are also provided. Additionally, the data consumers are able to upload and share processed data to marketplace.

7.1.1.2 Actors

In use case MD-UC1 those actors who provide or consume data or support the data sharing process are identified.

- **Data source** is the data subject who is the owner of the personal and health data to be shared, and her/his data privacy must be preserved;
- **Data providers** comprise the following actors:
    - **Health tech companies** which are providing data subject's health data, aggregating these health data coming from devices and wearables belonging to patients or citizens;
    - **Pharmaceutical companies** provide medical data. They can also act as consumers;
    - **Hospitals** provide sensitive health data from patients;
- **Data consumers** comprise the following actors:
    - **Research organizations and laboratories** which are consuming health data for research purposes;
    - **Pharmaceutical companies** can also act as consumers;
- **Health data exchange marketplace** is provided by the DEP (health data exchange marketplace and DEP are interchangeable terms);

- **Privacy preserving tools system** (anonymization service and cryptographic service) needed for securing and preserving user privacy;
- **Wearable provider which** provide devices for collecting health data from subjects;
- **Infrastructure providers** which are allowing the data providers and data consumers connect each other and monetize the data exchange process to all involved stakeholders.

All the identified actors except the data subject and the wearable provider participate directly in this use case.

7.1.1.3 Preconditions

As indicated in Section 7.1.1.2, not all the actors are directly participate in this use case MD-UC1, as the activity of the data subject and the wearable provider, is out of the scope of this use case. Otherwise, for the rest of the actors participating in this use case some prerequisites must be satisfied in advance.

- The data provider must have previously **acquired data subject consent** in order to manage their personal and sensitive data, namely for aggregating and sharing these data;
- Regarding the data protection of the sources of data (wearables), when they act as data providers, is out of scope of this demonstrator;
- The data provider should supervise that the data subject's privacy is preserved on the data provider system: Also, the data owner rights must be assured;
- The data provider and the data consumer must previously be on-board on the platform;
- When data are provided from a wearable, the API from the data providers must be connected to the platform in order to allow the access to its data;
- Dawex (the data exchange platform owner) must assure secure connection through the APIs;
- The data consumer will use the Dawex data assessment tools to assess the quality of data, when they browse the data catalogue;
- The communication tools available on the Dawex platform will allow the data consumer to directly contact the data provider on the platform. Also, the Dawex platform will provide means for getting a legal agreement between the parties on the terms and conditions of the data exchange and sign the contract.

The Crypto-FE CyberSec4Europe component needs to be enabled prior to the execution of this use case.

7.1.1.4 Basic Flow

The basic flow of this use case is depicted in Figure 95, and a description of the performed steps is the following:

- Use case begins: the personal and sensitive health data from a specific data source, such as a wearable are gathered by a data provider;
- Event 1: The data provider is able to aggregate health data coming from different sources and perform certain data analytics with them;
- Event 2: The retrieved data are protected preserving the user privacy by using PETs;
- Event 3: With the aim of monetizing the stored health data, the data provider makes them available to interested buyers by providing related metadata on the data exchange marketplace catalogue;

- Event 4: The data consumer (e.g., a public or private research organization) browses the catalogue looking for an appropriate dataset in which it is interested, the provided metadata gives information about how to manage the data (depending on the kind of PETs applied during the data protection process);
- Event 5: For easing the browsing process, data assessment tools (developed by Dawex) will be provided, improving the user experience;
- Event 6: The data consumer will contact to the data provider through the DEP to agree the terms and conditions regarding the management of the further requested data. This step is made through specific contract services that the Dawex DEP supplies;
- Event 7: The data consumer requests the selected health data to the data provider through the API;
- Event 8: The data provided by employing data protection services such as an encryption schema, (functional encryption, or homomorphic encryption) is able to preserve the data subject's privacy and secure the data;
- Event 9: The data consumer obtains the protected data from the data provider, through the appropriate API;
- Use case ends: the data consumer will perform analytics over these retrieved data and could be able to decrypt the encrypted health data in the case of it was allowed to do it.

It is worthy of mention that the user data privacy is preserved at any moment, while allowing the data consumer to perform some analysis with the protected health data.

Relevant preconditions and the steps 1, 2 and 7 are out of the scope of this use case (blue arrows in Figure 95), but details are provided for a consistent description and a better understanding of the whole process in this use case.

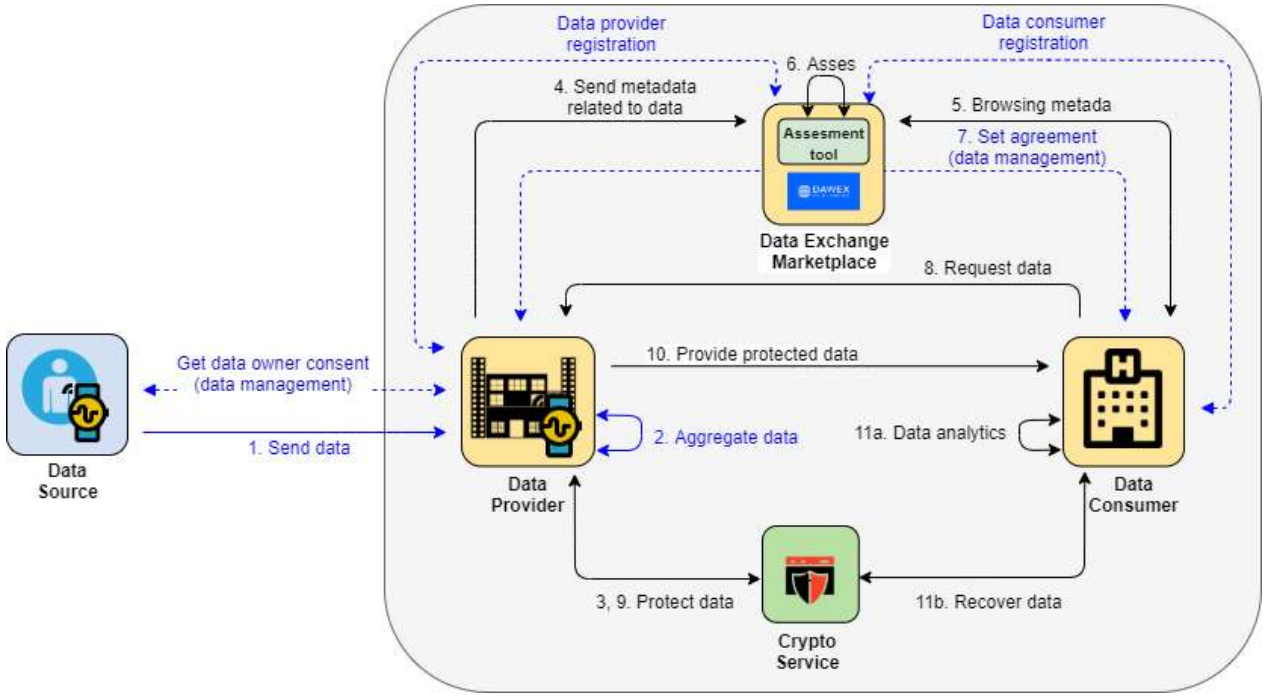

Figure 95: Medical Data Exchange - MD-UC1 Basic flow diagram

7.1.1.5 Alternate Flows

The data provider could perform the protection data process by using the privacy preserving service in the first stages of the process (step 3) after the data aggregation, or after the data consumer requests the agreed data (step 9). The privacy preserving service is offered by the data exchange platform and is available at any moment of the process, is a service provider decision when to use the PETs.

The data consumer, at the end of the use case, has two alternatives when managing the protected data. Depending on the kind of PETs applied for protecting the health data the data consumer is able to perform some analytics over these retrieved data and could be able to decrypt the encrypted health data by using the same PET used by the service provider. Otherwise the data consumer would only be able to perform analysis with the encrypted data (e.g., by using homomorphic encryption).

7.1.1.6 Postconditions

Following the end of the use case MD-UC1 the infrastructure provider monetises the data exchange to all the stakeholders involved, according to the reached agreement between the different stakeholders.

7.1.1.7 Included Use Cases

This use case MD-UC1 includes three additional use cases:

- Data aggregation on the health data coming from different sources;
- Perform analytics on the protected health data;
- Contract agreement between the different stakeholders involved in the sharing process, which comprises the legal contract, the signature of the agreement and the monetization of the process.

All of these included use cases are out of the scope of the demonstrator but are necessary for the completion of the operational sharing process.

7.1.2 Use case MD-UC2: Sharing Sensitive Health Data through Files

This use case is focused on sharing health data through files stored in the data exchange marketplace, unlike use case MD-UC1 focused on sharing data through an API. Use case MD-UC2 also comprises four main phases:

- The data providers receive personal and health data from a data source. The data subject's privacy is protected by using anonymization and PETs. The data provider uploads the file on the data exchange platform, including a set of related metadata;
- The data consumers select the data file from the marketplace catalogue, based on the related metadata provided by the data providers.
- The data consumers contact to the data providers for agreeing on terms and conditions regarding the exchange of the data. Contract services are provided by the data exchange platform;
- Once the data consumers receive the protected data from the platform. they are able to perform the appropriate analytics depending on the PET already used by the data provider.

As indicated in the previous use case, the data subjects' privacy is preserved at any moment due to the PETs (anonymization and privacy preserving services applied on the health data).

During the first phase of the development of the demonstrator, data will be protected using the anonymization service.

Figure 96 shows the UML diagram for use case MD-UC2.

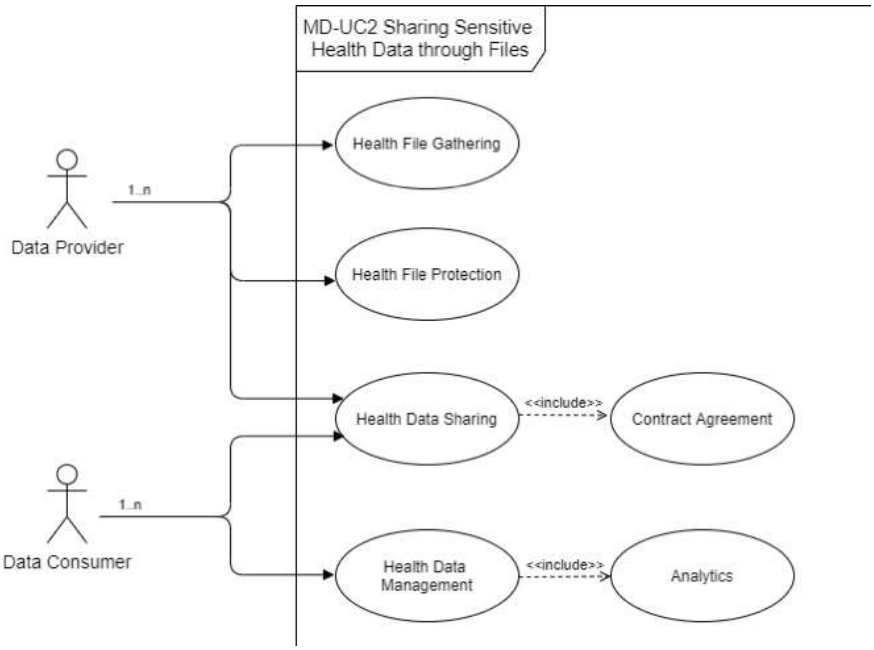

Figure 96: Medical Data Exchange - MD-UC2 UML diagram

As several process and features are common to both use cases, only those different will be described in the following subsections.

7.1.2.1 Stakeholders

This use case involves the same stakeholders involved in use case MD-UC1 (see Section 7.1.1.1).

7.1.2.2 Actors

This use case involves the same actors involved in use case MD-UC1 (see Section 7.1.1.2) except the health tech companies and the wearable providers. In use case MD-UC1 the data source are wearables from users, whereas in use case MD-UC2 the data are exclusively coming from files.

7.1.2.3 Preconditions

The preconditions applying to use case MD-UC2 are the following:

- The data provider must have previously **acquired data subject consent** in order to manage their personal and sensitive data, namely for aggregating and sharing these data;
- The data provider must supervise that the data subject's privacy is preserved on the data provider system. The data owner rights must be assured, as well;
- The data provider and the data consumer must previously be registered on the platform;
- Dawex uses asymmetric encryption protocols to encrypt data at rest. A dedicated microservice manages the encryption / decryption of each file. The seller's files can be stored in any cloud provider system and are always encrypted after upload on the platform and before being stored. Data files are decrypted on demand upon transaction validation and are only available to the buyer for the duration of the buyer's download;

- Dawex (the data exchange platform owner) must assure secure connection through the APIs;
- The data consumer will use the Dawex data assessment tools to assess the quality of data, when they browse the data catalogue;
- The communication tools available on the Dawex platform will allow the data consumer to directly contact the data provider on the platform. Also, the Dawex platform will provide means for getting a legal agreement between the parties on the terms and conditions of the data exchange and sign the contract.

The DANS and the Crypto-FE CyberSec4Europe components need to be enabled prior to the execution of this use case.

7.1.2.4 Basic Flow

The basic flow of this use case is depicted in Figure 97, and a description of the performed steps is the following:

- Use case begins: the personal and sensitive health data, in form of files, from a specific data source, are retrieved by a data provider;
- Event 1: The data provider uses the data protection services over the received files;
- Event 2: The data provider uploads to the data exchange platform the protected file to be shared. Also, a set of related metadata is provided;
- Event 3: The data consumer browses the catalogue looking for an appropriate data file in which it is interested, the provided metadata gives information about how to manage the data (depending on the kind of PETs applied during the data protection process);
- Event 4: For easing the browsing process, data assessment tools (developed by Dawex) will be provided, improving the user experience;
- Event 5: The data consumer will contact the data provider through the DEP to agree to the terms and conditions regarding the management of the further requested data. This step is made through specific contract services that the Dawex DEP supplies;
- Event 6: The data consumer requests the selected health data to the data exchange marketplace;
- Event 7: The data exchange marketplace provides the protected file to the data consumer;
- Use case ends: the data consumer is able to decrypt the health data from the just received file and, will be able to perform analytics over such data.

As indicated in Section 7.1.1.4 the data subject's privacy is still preserved thanks to the previous data protection service, while the data consumer is able to perform some analysis.

Relevant preconditions and the steps 1 and 6 are out of the scope of this use case (blue arrows in Figure 97), but details are provided for a consistent description and a better understanding of the whole process in this use case.

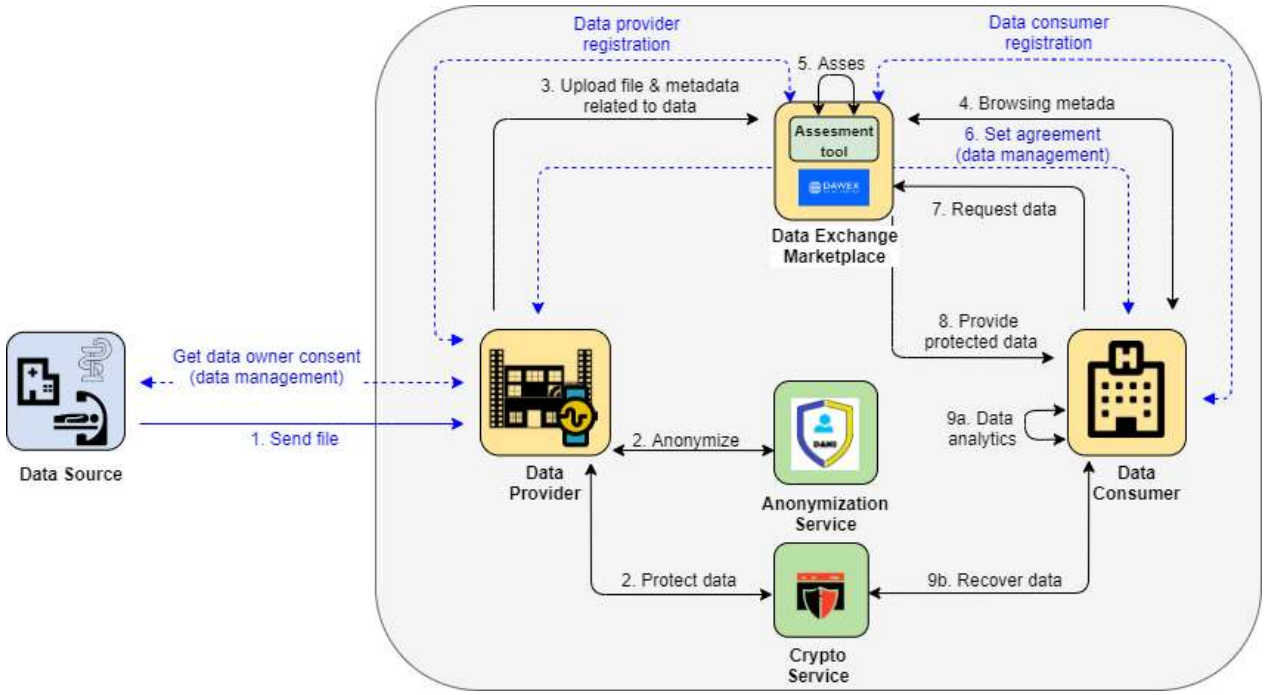

Figure 97: Medical Data Exchange - MD-UC2 Basic flow diagram

7.1.2.5 Alternate Flows

The data provider could perform the protection data process by using both, the privacy preserving service and the anonymization service or a single protection service, in the first stages of the process (step 2).

The data consumer, at the end of this use case, is able to decrypt the encrypted health data by using the same privacy preserving service used by the service provider. Otherwise the data consumer only would be able to perform analysis with the encrypted data (e.g., by using homomorphic encryption).

7.1.2.6 Postconditions

Use case MD-UC2 has the same post condition as use case MD-UC1 (see Section 7.1.1.6).

7.1.2.7 Included Use Cases

Use case MD-UC1 includes two additional use cases:

- Perform analytics on the protected health data;
- Contract agreement between the different stakeholders involved in the sharing process, which comprises the legal contract, the signature of the agreement and the monetization of the process.

All of these included use cases are out of the scope of the demonstrator but are necessary for the completion of the operational sharing process.

7.1.3 Use case MD-UC3: Enhancing the Security of On-Boarding and Accessing the Dawex Platform

Use case MD-UC3 is focused on the access of the different stakeholder can access the data exchange platform. The aim is to increase the security of the onboarding process and to facilitate the access to the platform in a secure way. In order to provide a secure mechanism for online registration, the use of eID issued by EU member

states authorized organizations is envisaged. In this way the eIDAS network integration with the Dawex data exchange platform will be performed. An eIDAS connector call SPeIDI will be used for connecting the data exchange platform with the country eIDAS node facilitating the user cross-border authentication allowing stakeholders from different EU countries to get access to the platform. The trustworthiness and assurance will be increased not only the online registration process, but the access process as well. At this moment the eIDAS network is able to authenticate a natural person. Although the eIDAS network is also prepared for authenticating a legal person, this functionality is not supported by all country eIDAS node. For this reason, only the authentication of natural person will be performed during the development of this use case. Additionally, a decentralized access control mechanism is planned leveraging the Self-Sovereign Privacy-Preserving Identity manager (SS-PP IdM) asset, which will be developed during the life of the project.

The integration of the eIDAS network will start during the first phase of use case MD-UC3. During the second phase the finalization of this integration will be performed. Additionally, the adoption of the decentralized mechanism is planned for the second phase of use case MD-UC3.

The use of two factor authentication (e.g., use of eID with eIDAS) and the decentralized access control mechanism make more robust the authentication process, when users get access to the DEP and the files stored in cloud environments.

Figure 98 shows the use case diagram for the MD-UC3.

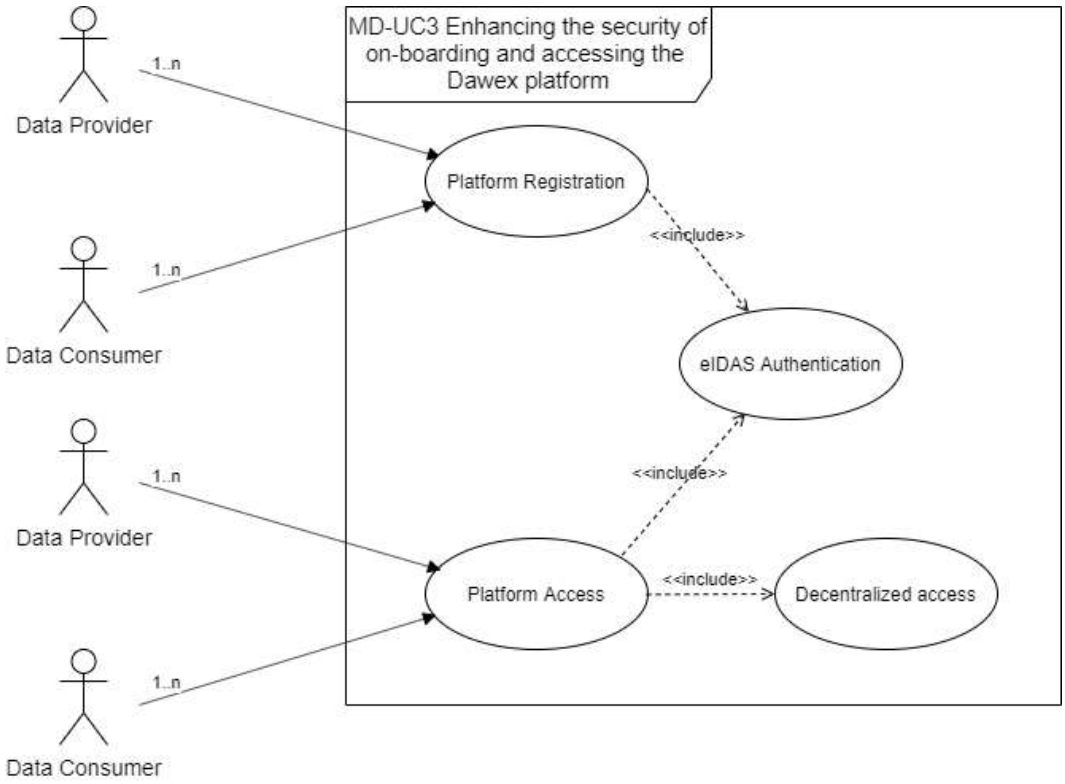

Figure 98: Medical Data Exchange - MD-UC3 UML diagram

7.1.3.1 Stakeholders

Use case MD-UC3 includes the same stakeholders as use case MD-UC1 (see Section 7.1.1.1). Additionally, stakeholders involved with the authentication process must be included:

- **Identity provider** creates, stores and issues credentials on principals, and also authenticates user identity;

- **Identity management platform providers** are in charge of managing the infrastructure needed for an identity management system.

7.1.3.2 Actors

In this use case, those actors which are involved in the processes of accessing the data platform, or support these processes are identified. The actors involved are the following:

- Users comprise the following actors:
  - **Health tech companies, hospitals and pharmaceutical companies** that are accessing the data exchange platform as data providers;
  - **Research organizations, laboratories and pharmaceutical companies** that are accessing the data exchange platform as data consumers;
- **Health data exchange marketplace** which is provided by the data exchange platform;
- **Infrastructure providers** which are facilitating the data providers and data consumers reach the data exchange platform and the authentication process;
- **Identity provider** from the data provider/consumer country, in charge of the user authentication.

7.1.3.3 Preconditions

Use case UC-MD3 involves the following preconditions:

- The data provider and the data consumer must hold an eID issued by an authorized organization from an EU member state under an eID recognized scheme;
- The data provider and the data consumer must be already registered in the platform;
- As the Dawex DEP is managed in France, the DEP must be integrated with the French eIDAS node through the eIDAS connector;
- The French eIDAS node must be connected to the eIDAS network pre-production environment;
- The SPeIDI asset for cross-border eIDAS authentication, and the SS-PP IdM need to be available prior the execution of this use case.

7.1.3.4 Basic Flow

The basic flow of this use case is depicted in Figure 99, and a description of the performed steps is the following:

- Use case begins: the already registered user tries to get access to the DEP;
- Event 1: The platform redirects the user to the eIDAS network through the eIDAS connector in order to be authenticated;
- Event 2: The identity provider (IdP) from the user origin country asks the user for credentials. The user provides credentials;
- Event 3: The IdP authenticates the user;
- Event 4: The IdP provides the user credentials to the eIDAS connector, which sends the user info to the platform. The user is redirected to the platform.
- Event 5: The platform validates the credentials;

- Use case ends: the platform grants user access to the platform.

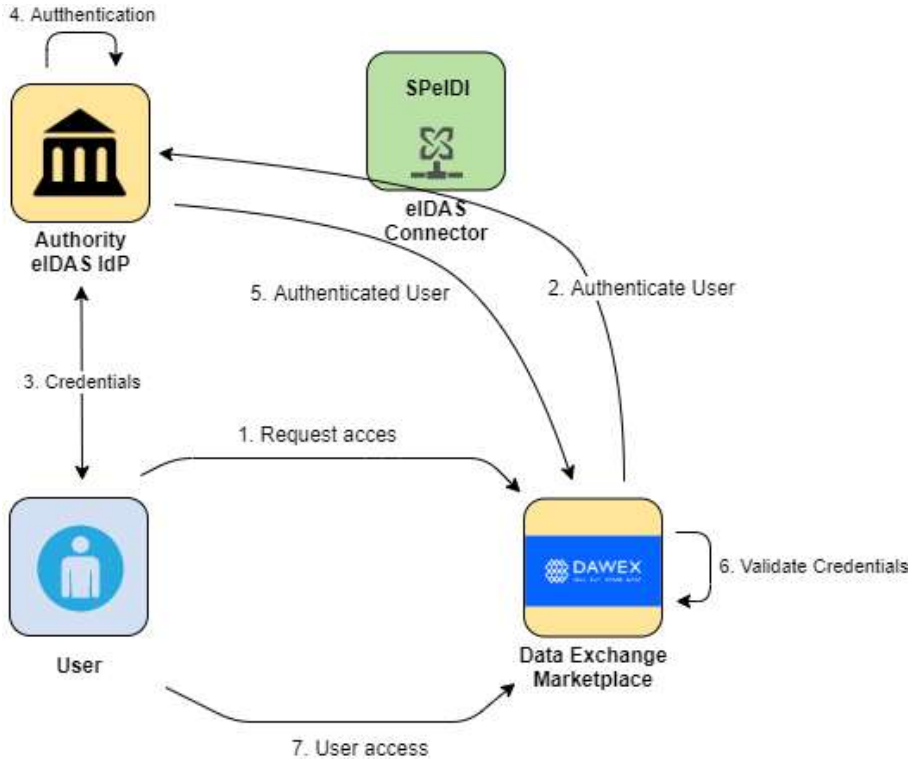

Figure 99: Medical Data Exchange - MD-UC3 Basic flow diagram

7.1.3.5 Alternate Flows

Two alternatives could be followed for accessing the data exchange platform. The indicated in the basic flow involves a federated identity management based on eIDAS network, and the use of eID issued by the EU member states. The second alternative implies a decentralized mechanism were the self-sovereign identity and the disruptive blockchain technology are used. A more detailed description of this later alternative is provided in Section 7.1.3.7.

7.1.3.6 Postconditions

The user is registered on the platform in the case of the on-boarding process, or access to the platform is granted if access is requested.

7.1.3.7 Included Use Cases

Use case MD-UC3 includes two additional use cases:

- MD-UC3.1: User Registration with eIDAS;
- MD-UC3.2: Deriving Identity Provided by eIDAS to SSI BC.

MD-UC3.1: User Registration with eIDAS

Figure 100 shows the registration process based on eIDAS authentication.

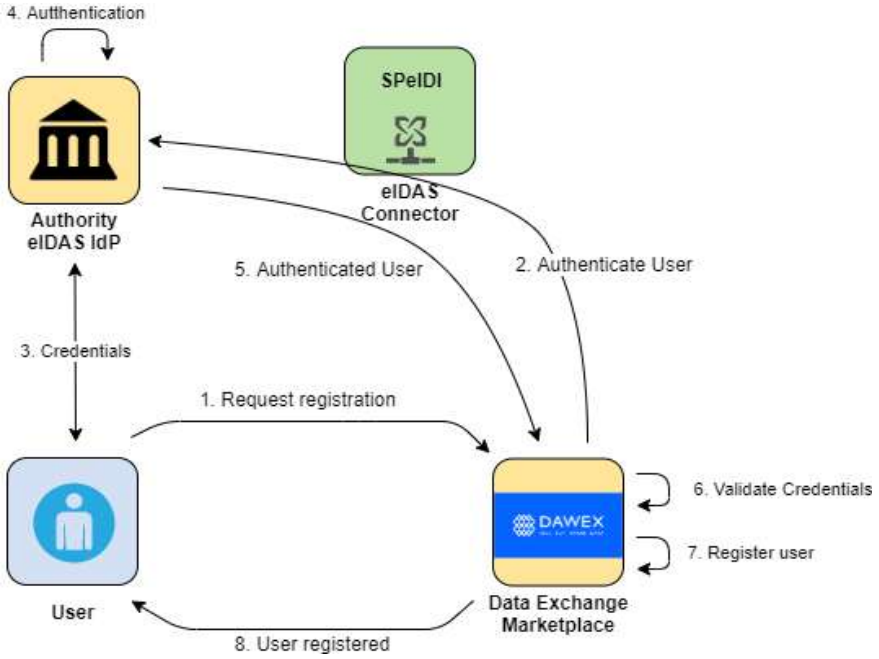

Figure 100: Medical Data Exchange - MD-UC3.1 basic flow diagram

MD-UC3.2 Decentralized Access

Figure 101 shows the process of generating a verifiable credential (VC) based on eIDAS authentication (see basic flow) and the validation of this VC by the platform using the blockchain technology.

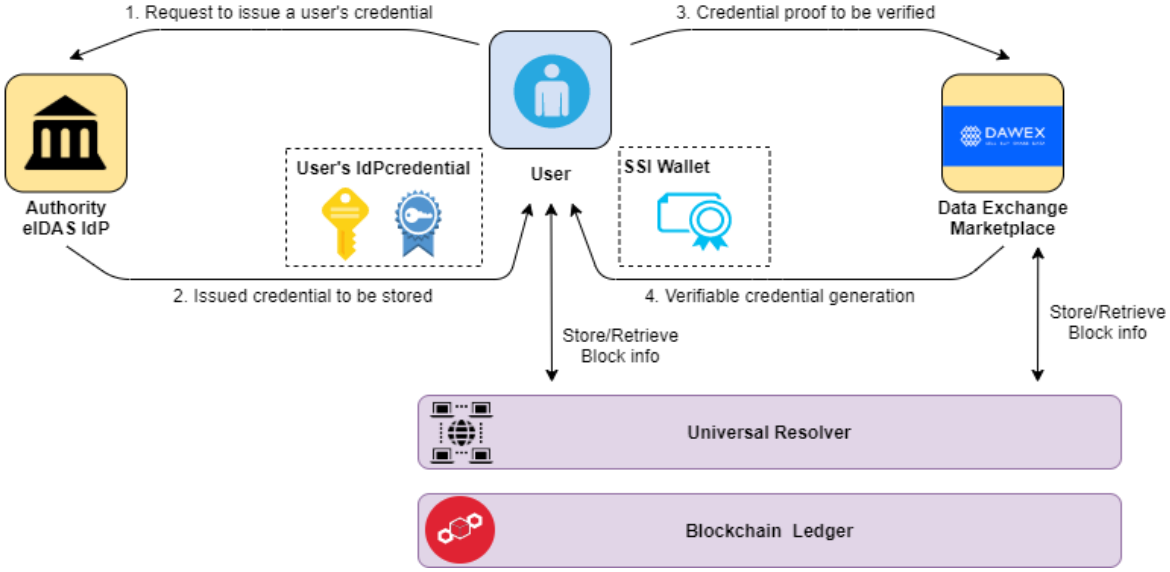

Figure 101: Medical Data Exchange - MD-UC3.2 basic flow diagram

7.2 Demonstrator Set-up

The Medical Data Exchange Demonstrator is based on the Data Exchange Platform (DEP) provided by Dawex[41], which is designed to support companies for sharing data in an easy a secure way and facilitating the

[41] https://www.dawex.com/en/data-exchange-platform/

data monetization. In the context of CyberSec4Europe project, the Dawex platform is focused on the exchange of medical data. As indicated in deliverable D5.1 [1], the main objectives are:

- Enhancing the multi-lateral trust among stakeholders generating and consuming data in the medical business sector;
- Improving data marketplace platform trustworthiness;
- Generating new business opportunities.

An overview of the generic use case process was provided in Figure 93, and a more detailed description is provided in deliverable D5.1 [1].

With the aim to achieve the indicated goals, this demonstrator is focused on proving how the personal and sensitive data, from citizens and patients, can be secured and their privacy preserved by using the assets developed in the context of the project. To this end, the participation of different stakeholders (e.g. hospitals, pharmaceutical companies, research organizations or laboratories), leveraging the functionalities of these assets is essential.

The use of privacy preserving services and anonymization assets for securing and preserving user privacy, in addition to the integration of strong cross-border authentication mechanisms, and also the adoption of innovative decentralized access, will make the use of these data exchange platforms trusted and secure.

7.2.1 Relation to Use Cases

The envisaged plan for the implementation of described use cases in Section 7.1 has been detailed in [2]. Basically, the plan for the **phase I** is:

- In the context of use case MD-UC2 the anonymization service (DANS) will be implemented. The Dawex DEP will offer this asset to the users as a service. Therefore, an end-to-end privacy preservation tool is provided to users, while the analytics process is not affected.
- As part of the work in use case MD-UC3, the first steps for designing and implement the SPeIDI asset to French eIDAS connectivity, will be done.
- The development of the Dawex visualization tool and integration into the DEP, will be performed for the use cases MD-UC1 and MD-UC2.

During the **phase II the following** is planned:

- The integration of SPeIDI asset with the Dawex DEP will be performed for the MD-UC3, which means that a secure and stronger cross-border authentication service for accessing data is included.
- The integration of the visualization tool into the Dawex DEP for MD-UC1 and MD-UC2.
- For the MD-UC1 and MD-UC2, the integration of the privacy preserving service will be offered to the users for sharing data in a secure and privacy way.

In the context of MD-UC3 will be performed the adoption of the SSI-PP IdM asset, which will allow users to easily access the Dawex platform from different environments. Their integration will be evaluated depending on the maturity of this asset, which will be developed during the project. A study providing the basis for their adoption will be provided.

The next mapping table shows the when and what will be performed for each use case.

		MD-UC1		MD-UC2		MD-UC3	
		Phase I	Phase II	Phase I	Phase II	Phase I	Phase II
DANS	Implementation						
	Integration						
Crypto-FE	Implementation						
	Integration						
SPeIDI	Implementation						
	Integration						
Visualization Tool	Implementation						
	Integration						
SS-PP IdM	Implementation						
	Adoption						

Table 3: Medical Data Exchange - Use cases and assets mapping. Implementation and integration plan

7.2.2 Relation to WP3 Assets

In order to cover the requirements identified in deliverable D5.1 [1] this demonstration will use the following assets produced by task T3.2 (more detailed information on these asset can be found on deliverable D3.2 [4]) in the context of WP3:

- **SPeIDI** is the eIDAS connector, integrating the DEP with the eIDAS network used for cross-border strong authentication purposes;
- **SS-PP IdM** provides "a privacy-respectful solution, enabling users with full control and management of their personal identity data without needing a third-party centralized authority taking over the identity management operations" [4].
- **DANS** is the anonymization service which will preserve the user data privacy;
- **Crypto-FE** is a "functional encryption FE library containing attribute-based encryption (ABE) schemes for the privacy-preserving in health information management" [3].

The availability of these assets is different, depending on their maturity level and the implementation status. SPeIDI, Crypto-FE and SS-PP IdM, are in the implementation phase to be adapted for this demonstrator or to be implemented in full. They will be not available during the phase I. The adaptation of the SPeIDI asset to the eIDAS network and the Crypto service (adapted from FENTEC[42] EU project) will be ready for integration during the phase II. The SSI-PP IdM asset is in the process of development and is expected to be available at the end of the project. Due to these constraints use cases MD-UC1 and MD-UC2 are planned to be partially implemented during the first iteration and use case MD-UC3, and the remaining functionalities of use cases MD-UC1 and MD-UC2, will be implemented during the second iteration (see **Error! Reference source not**

[42] http://fentec.eu/

found.).

Apart from these planned assets there are other assets provided by the WP3 that are in the radar of this demonstrator and have been identified as assets to be considered for future works in the field of the health domain.

In line with the envisage work on how the health data exchange marketplace is facing the GDPR regulation, two assets have been identified, the "GDPR compliant user experience" providing guidelines on how to perform a DPIA, and the "GDPR-Based User Stories in the Access Control Perspective" a "solution to minimize errors and issues in the GDPR enforcement" [4]. The feasibility study will be performed during the phase II. The objective is to produce GDPR guidelines, which could be applied to different domains.

7.2.3 Description and Workflow

This demonstrator is using the DEP provided by Dawex supporting the data marketplace. An overview of the DEP architecture is shown in Figure 102. The platform provides a cloud agnostic infrastructure and comprises different main components as follows:

- **User Interface** for interacting with the data providers and the data consumers in a user-friendly manner;
- **Management module** for securing management of the data life cycle;
- **Services** providing features for data sharing supporting the data exchange platform performance assuring user's privacy and taking care of legal matters;
- **Data base** for storing data;
- **Orchestrator module** for platform access control and communication management.

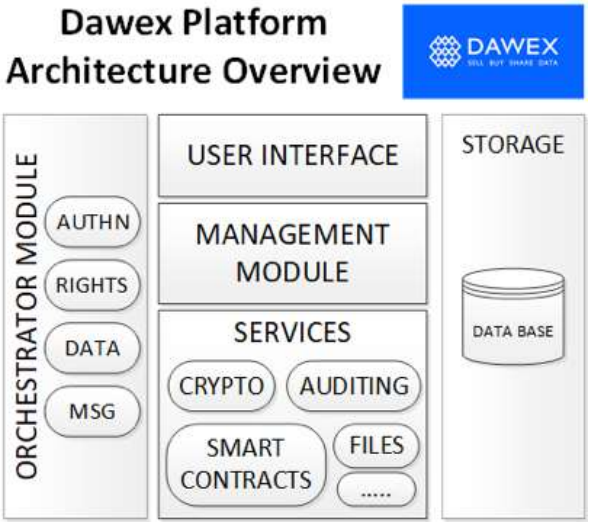

Figure 102: Medical Data Exchange – Dawex DEP architecture high-level view

The current medical data exchange platform (Dawex platform) comprises several security aspects for accessing and sharing data and for storing and managing the data [1]. The objective of this task task T5.6 is providing an additional security layer to the Dawex platform.
Several services are envisaging to be used by the Dawex platform as follows:

- Anonymization service: DANS. Atos asset;
- Strong Authentication service: SPeIDI, from LEPS[43] CEF project;
- Self-sovereign privacy-preserving IdM in blockchain service: SS-PP IdM. UMU enabler;
- Crypto service: from FENTEC project provided by Atos.

These state-of-the-art components are based in open source code and will be integrated easily by using well known and secure standard protocols.
The process for acquiring these features is split in two phases:

- **First phase**: offering an anonymization service in order to provide and end-to-end privacy -preserving tool to users, while the analytics process is not affected.
- **Second phase**: including a secure and stronger cross-border authentication service for accessing data, and a self-sovereign identity management to allow to allow users easy access to the Dawex platform from different environments. Additional privacy preserving services will be offered to the users for sharing data in a secure way.

An initial approach for a high-level architecture is depicted in Figure 103 showing how the Dawex platform is wrapped.

Figure 103: Medical Data Exchange – Task T5.6 demonstrator high-level view architecture

Figure 104 displays a high-level view on how the different assets interact each other.

[43] http://www.leps-project.eu/

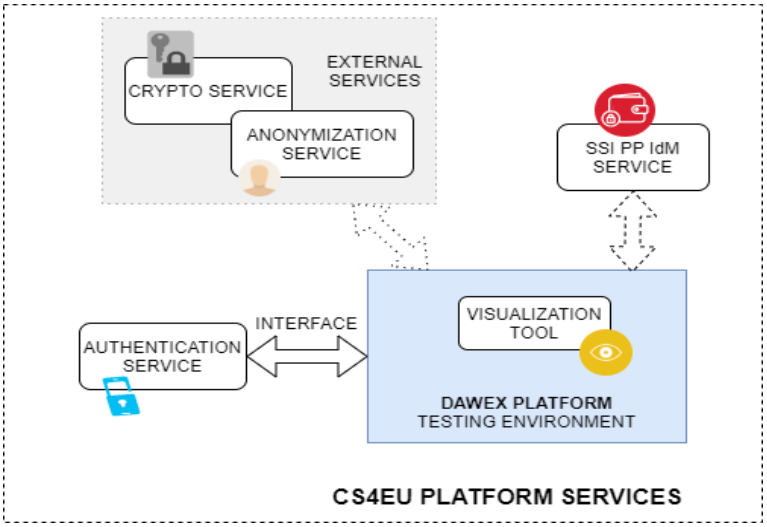

Figure 104: Medical Data Exchange - High-level view of services interaction with the Dawex DEP

The following pictures shows how the different assets identified to be used in this demonstrator interact with the DEP and the involved stakeholders. Figure 105 depicts the interaction between the privacy preserving, the DEP, and the stakeholders in use case MD-UC1.

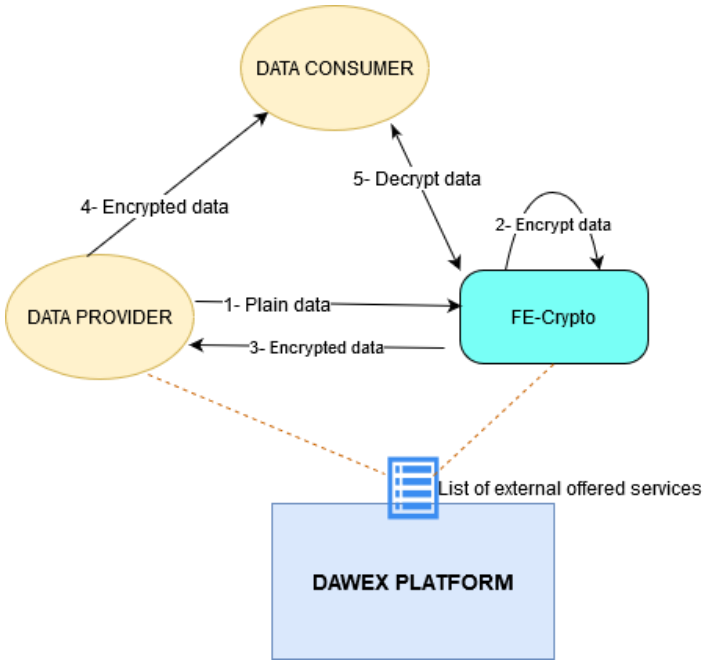

Figure 105: Medical Data Exchange - Crypto service, DEP and stakeholder's interaction in use case MD-UC1

Figure 106 depicts a high-level view of the interaction between the anonymization service, the DEP and stakeholders in use case MD-UC2.

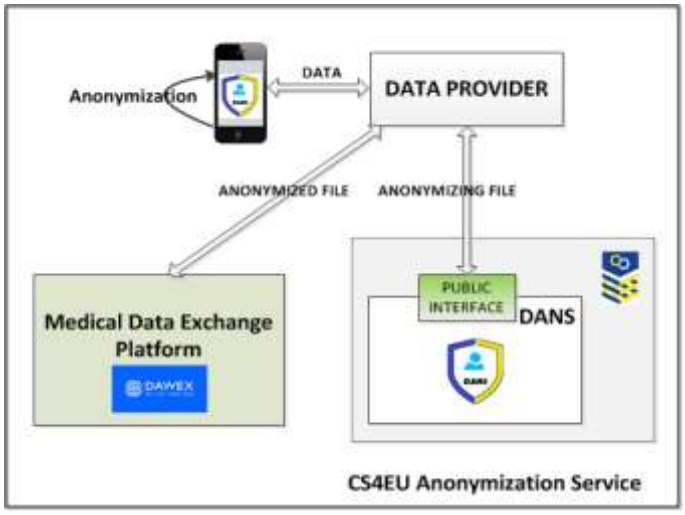

Figure 106: Medical Data Exchange - Anonymization service, DEP and stakeholder's interaction in use case MD-UC2.

Figure 107 shows a high-level view of the interaction between the anonymization service and DEP in use case MD-UC2.

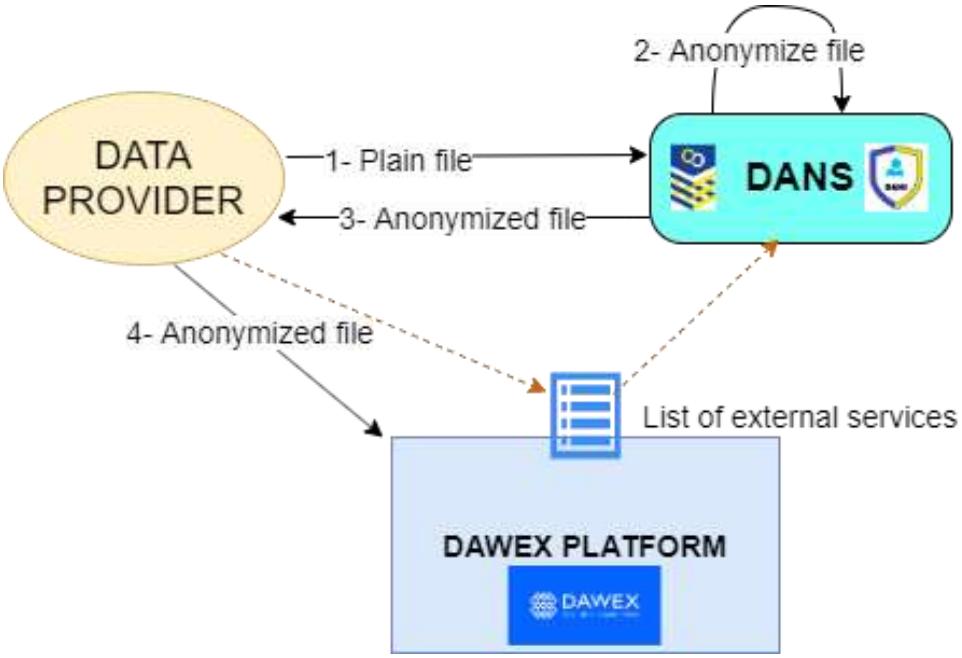

Figure 107: Medical Data Exchange - Anonymization service and DEP detailed interaction in use case MD-UC2.

Note that the data protection services (Crypto-FE and DANS) is envisaged to be provided by the data exchange platform, by a third party or by the data provider itself. Different deployment alternatives are also planned:

- As a jar file to be integrated in the data provider system;
- As a standalone REST service to be deployed on the data provider environment or by a third party.

Figure 108 presents a high-level view interaction between the eIDAS connector service and DEP in use case MD-UC3.

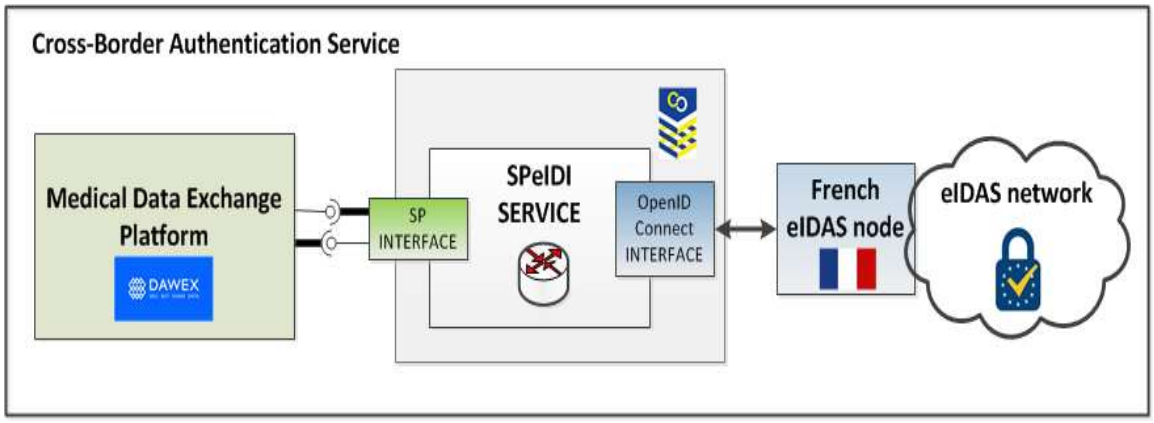

Figure 108: Medical Data Exchange - SPeIDI and DEP interaction in use case MD-UC3.

Figure 109 presents a more detailed interaction between the eIDAS connector and DEP in use case MD-UC3.

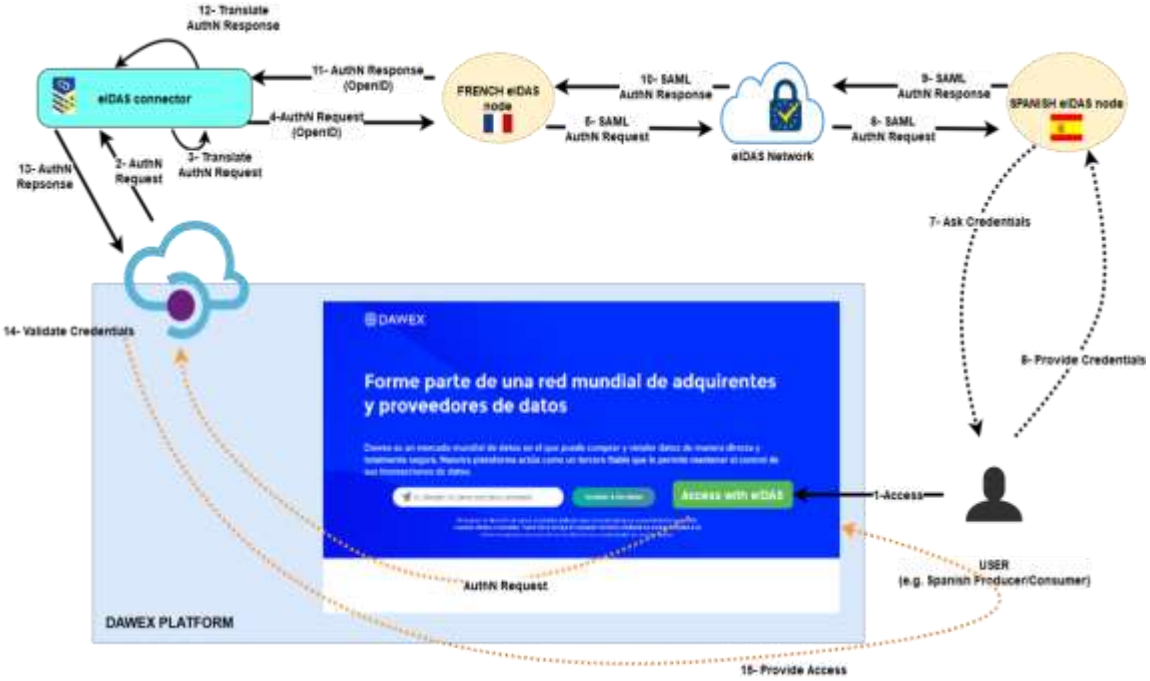

Figure 109: Medical Data Exchange - SPeIDI and DEP detailed interaction in use case MD-UC3.

7.2.4 Target Group

The main target group are data exchange platforms not limited to the health domain. As indicated in Section 7.2.3, the provided services could be deployed in different ways facilitating the uptake of these secure and privacy preserving mechanisms. The integration in smart devices could be an important progress for extending the use of these tools to a wider audience.

8 Smart Cities

In this section, we describe the specifications of use cases of CyberSec4Europe “Smart Cities” demonstration cases. In the first section the use cases specifications are provided starting from the set of use cases identified in D5.1. The detailed specifications of the use cases takes into account also functionalities supported by the tools scouted in WP3 activities. In the second section a general description and related workflow of the three demonstration cases involved in "Smart Cities" context and then indicating which use cases will be performed in the first phase of demonstration.

8.1 Use Cases Specification

8.1.1 Use Case SMC-UC1: Register Data Consumer and Manage Services

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

8.1.1.1 Stakeholders

We consider the following categories of stakeholders:

- Local Public Administration: it includes all public entities involved (administrative, public employee, civil servants and other staff...) in smart cities processes and public service provision;
- Service Suppliers: public and/or private organizations which provide any type of smart cities services generally processing data (personal or not);
- Platform Provider: entities working with the providers of city data and services, and managing the content, defining policies and regulations of the platform.

8.1.1.2 Actors

We consider the following actors as possible participants in this use case:

- Employees;
- Citizens;
- Service Providers;
- City Data Publisher;
- Data Protection Officer.

All of them are considered users of the system, being able of registering into the system, allowing them to consume data and manage services with which they can share their own data. For an exhaustive description of these actors, please refer to [1].

8.1.1.3 Preconditions

No preconditions at this stage are required.

8.1.1.4 Basic Flow

1. Use case begins;
2. User registers into the platform, providing valid registration details;
3. Platform processes and confirms User registration;
4. User requests permission to consume city data;
5. User accepts usage terms and conditions of the platform;
6. User defines how hers/his personal data can be used by the Platform Owner and value-added services;
7. User is successfully registered into the platform and can manage and alter hers/his registration information at any later time;
8. Use case ends.

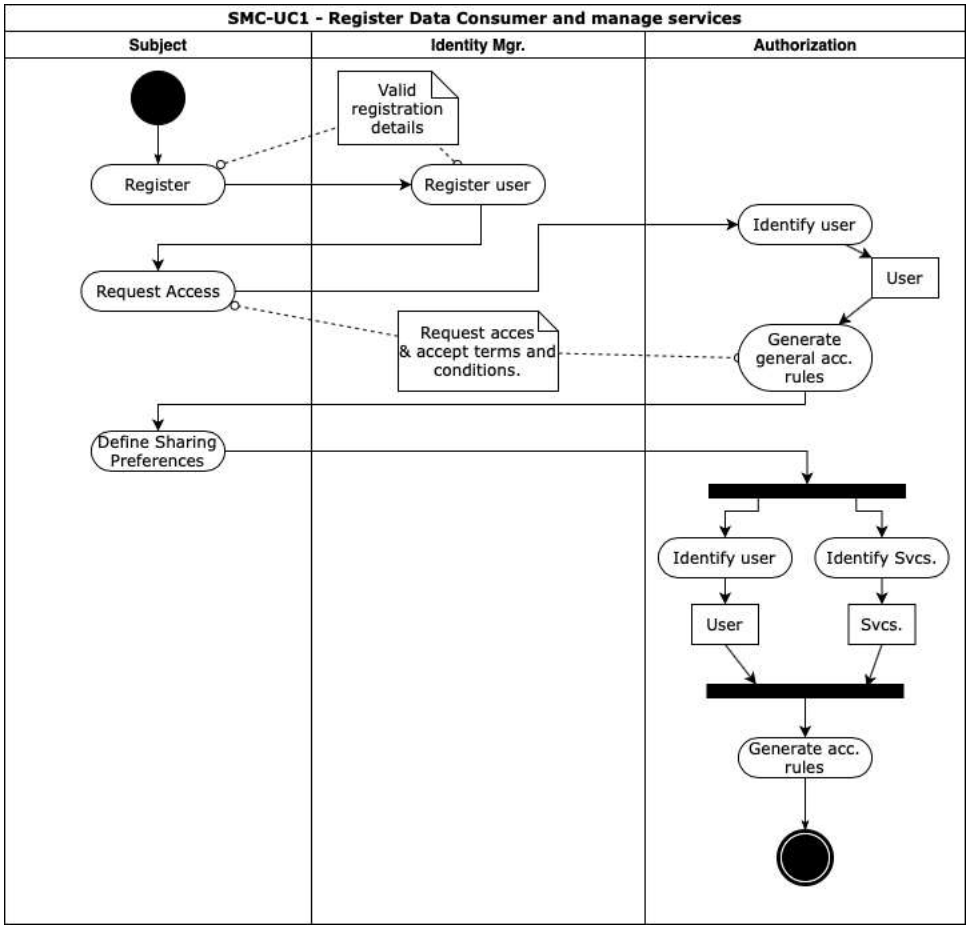

Figure 110: Smart Cities - SMC-UC1 use case diagram

The process for user registration into the system and service management, as depicted in Figure 110, starts with the registration activity, in which the user registers into the system by providing valid registration details that are validated by the identification manager. Following that, the user will request permission to consume city data after accepting the usage terms and conditions of the platform. The authorization system will then verify the identity of the requester as a user of the system, and generate the general access rules that will enable that specific user to retrieve data from the system. Finally, the user will set hers/his preferences regarding private data sharing to third party and institutional services. To that end, the authorization service (once again)

will verify the identity of the user, and generate the appropriate access rules to her/his private information, as requested by the user.

8.1.1.5 Postconditions

A new user has registered into the platform and defined hers/his preferences on personal data sharing. She/he can later login into the platform and manage hers/his preferences and registration information at any later time.

8.1.1.6 Included Use Cases

Use Case SMC-UC1.1: Register Consumer

Description

User registers into the platform in order to discover and consume data.

Basic flow

1. The platform prompts the user for a username and password or register new account;
2. The user selects registration options;
3. The platform prompts user for data consumer registration information (e.g. username, password) and privacy policies;
4. The user enters in their information;
5. Platform verifies information and creates account;
    - If non-valid information, platform shows error message and returns to step 1.
6. Platform acknowledges registration has been successful;
7. End of registration.

Postconditions

The user has been registered.

Use Case SMC-UC1.2: User Manages Services

Description

User gives permissions to different institutional and third party services to access hers/his data.

Preconditions

User must be already registered into the platform.

Basic flow

1. Platform provides user with an interface for services management;
2. User chooses to edit or delete services;
3. If edit, user revise service information (access-control, commercial models, parameters) and deployment;
4. If delete, user selects services to be removed / disabled;
5. User confirms action;
6. Platform quickly process user’s request;
7. Platform confirms execution of request;
    - If valid request, platform acknowledges request has been processed successfully;

- If non-valid request, platform returns to step 1.

8. End of services management.

Postconditions
Services have been managed.

Use Case SMC-UC1.3: User Tracks Services Usage

Description
User tracks how different services have been using hers/his data.

Preconditions
User must be already registered into the platform and given access to some services.

Basic flow

1. Platform provides user with an interface for services management;
2. User chooses to visualize usage information of a service;
3. Platform quickly process user's request for data usage information;
4. Platform provides user with statistical information about services usage and data users anonymised information;
5. End of data services tracking.

Postconditions
Services have been managed.

8.1.2 Use Case SMC-UC2: Discover and Consume City Data

Users are registered in the platform and have received approval to consume city data via GUI or APIs in a lawful manner. Users have accepted the terms and conditions of platform usage and define how their personal data can be used by the Platform Owner, including their usage for data profiling tools for service enhancing and personalization. Users, in any time, can manage and alter their registration information at any time they want to.

8.1.2.1 Stakeholders

We consider the following categories of stakeholders:

- Local Public Administration: It includes all public entities involved (administrative, public employee, civil servants and other staff) in smart cities processes and public service provision;
- Service Suppliers: Public and/or private organizations which provide any type of smart cities services generally processing data (personal or not);
- Platform Provider: Entities working with the providers of city data and services, and managing the content, defining policies and regulations of the platform.

8.1.2.2 Actors

We consider the following actors as possible participants in this use case:

- Employees;
- Citizens;

- Service Providers;
- City Data Publisher;
- Data Protection Officer.

All of them are considered users of the system being able of registering into the system, allowing them to discover and consume city data. For an exhaustive description of these actors, please refer to [1].

8.1.2.3 Preconditions

Users querying the system shall be already registered into it, and some information shall also be already introduced in the system in order to get results.

8.1.2.4 Basic Flow

Data discovery and consumption in the platform, usually follows two steps: data discovery, by which the user retrieves the catalogue of data available to her/him according to the access rules in place, and a second step of data consumption, in which the user retrieves the information of her/his interest. As a general rule, the first step will be repeated whenever the user wants to get updated on the available information of the system, and the second will be performed (repeatedly) to get the actual current values of the specific piece of information that the user needs.

1) **Data discovery** begins with the user requesting access to the authorization system, providing his identification credential. This request generates a Capability Token that will later grant her/him access the discovery service, which will return the data catalogue to which user is allowed access.

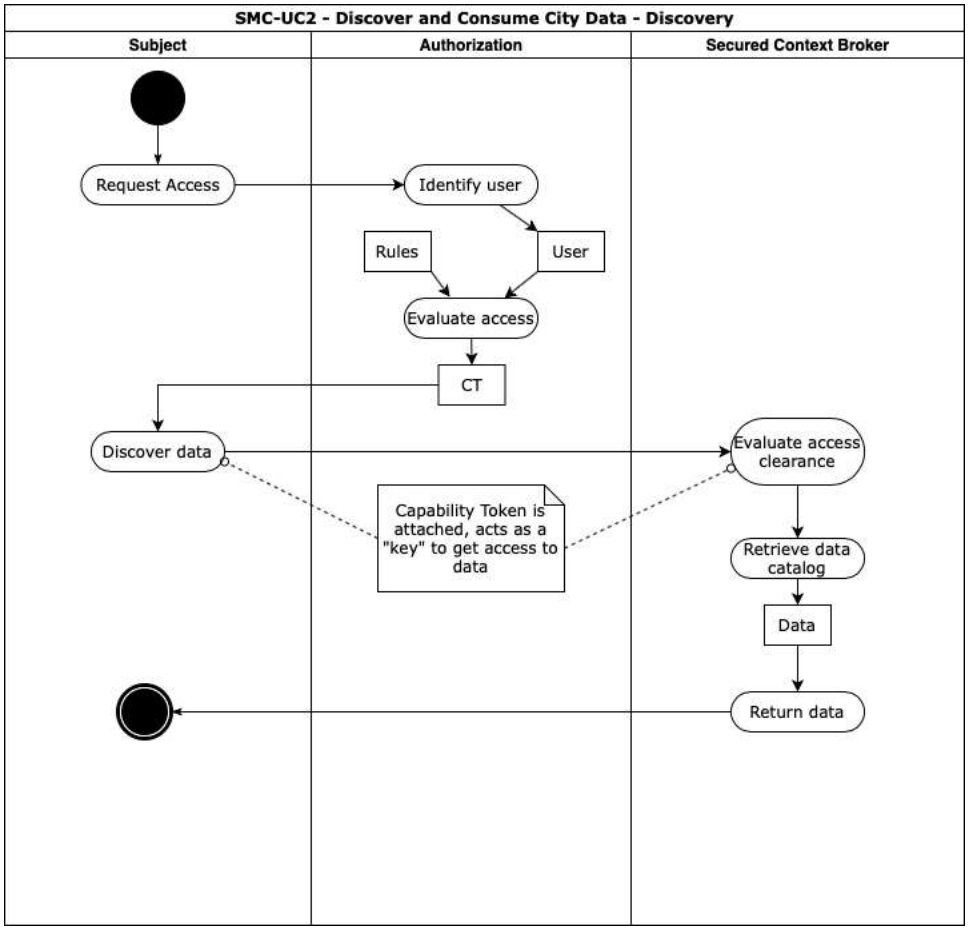

Figure 111: Smart Cities - SMC-UC2 data discovery use case diagram

2) **Data consumption** follows a similar pattern to the previous flow, starting with the user requesting access to the authorization system. The Capability Token (CT) obtained, this time, grants the user access to retrieving data.

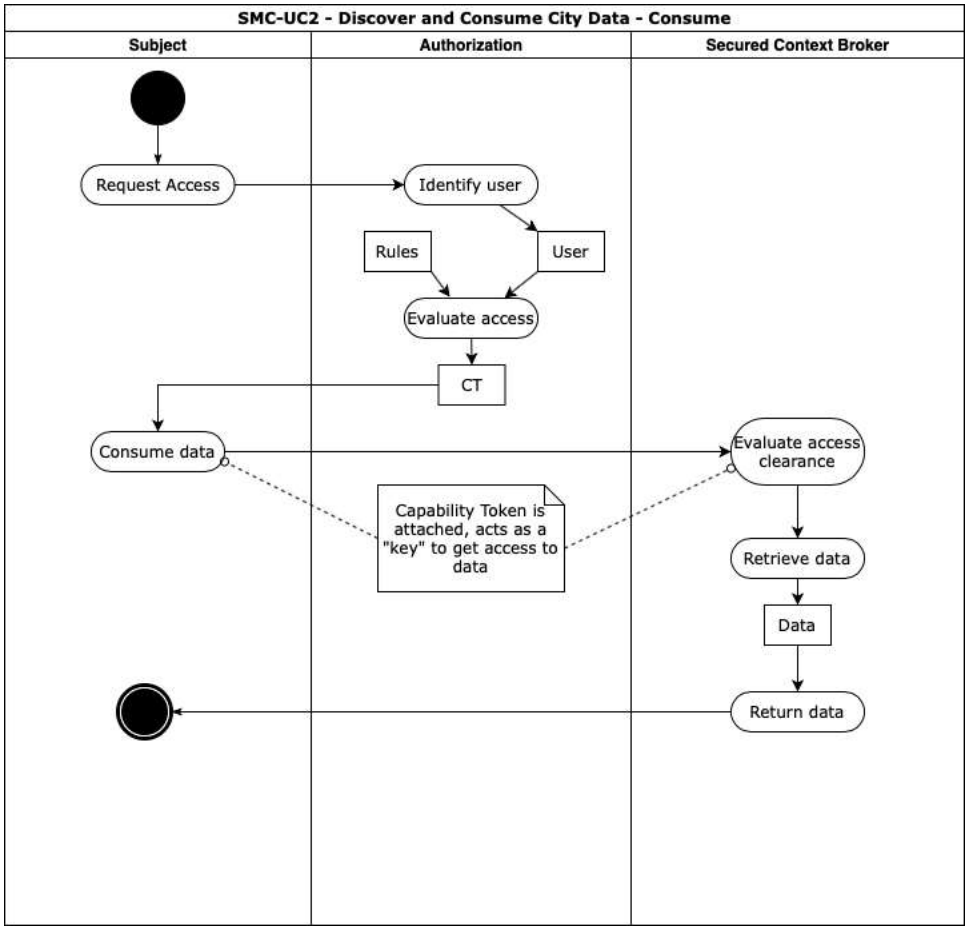

Figure 112: Smart Cities - SMC-UC2 discover and consume city data use case flow diagram

8.1.2.5 Postconditions

The system's state doesn't change as a result of this use case.

8.1.2.6 Included Use Cases

Use Case SMC-UC2.1: Discover City Data via data query end-points

Description

User discovers available city data in the platform, and end-points to access it

Preconditions

User must be already registered into the platform and given access to services.

Basic flow

1. Users access specialised data query end-points (e.g. SPARQL);
2. Users provides information for pre-defined parameters for search;
3. Users request data search;
4. Platform quickly process users request for data:
    - All queries are verified against access rights restrictions;
    - If restriction applies users are redirected to log in interfaces;

- Users provide credentials and log on the system.

5. Users are provided with query results on the end-point if access is allowed;
    - If access is not allowed, platform issues an error message to the user.

Postconditions
This use case has no postconditions.

Use Case SMC-UC2.2: Discover City Data via GUI

Description
User discovers available city data in the platform, and end-points to access it, via GUI

Preconditions
User must be already registered into the platform and given access to services

Basic flow
1. Users search city data via GUI;
2. Users inputs search parameters (e.g. key words, categories, formats, publishers);
3. Users request data search;
4. Platform quickly process users request for data:
    - All queries are verified against access rights restrictions;
    - If restriction applies users are redirected to log in interfaces;
    - Users provide credentials and log on the system.
5. Users are provided with query results on an interface;
    - If access is not allowed platform issues an error message to the user.

Postconditions
This use case has no postconditions.

Use Case SMC-UC2.3: Customise City Data

Description
Users retrieve City Data in a customised form.

Preconditions
User must be already registered into the platform and given access to services.

Basic flow
1. Users request data to be formatted in a particular format supported by the platform;
2. Platform quickly process users request for data formatting;
3. Mechanism for data conversion is called and process data;
4. Users are provided with data formatted as requested.

Postconditions
This use case has no postconditions.

Use Case SMC-UC2.4: Consume City Data via GUI

Description

Users retrieve City Data in a customised form, via GUI.

Preconditions

User must be already registered into the platform and given access to services.

Basic flow

1. Users / Machines select data to be downloaded;
2. Users / Machines are redirected to authentication mechanism in case of registration is needed for the particular dataset:
    - If authentication is successful, users are provided with requested data streams.
3. Users are provided with requested data via APIs.

Postconditions

This use case has no postconditions.

Use Case SMC-UC2.5: Consume City Data via APIs

Description

Users or services retrieve City Data via APIs.

Preconditions

User must be already registered into the platform and given access to services.

Basic flow

1. Users / Machines makes data request on the platform's API;
2. Users / Machines are redirected to authentication mechanism in case of registration is needed for the particular dataset;
    - If authentication is successful, users are provided with requested data streams.
3. Users are provided with requested data via APIs.

Postconditions

This use case has no postconditions

8.1.3 Use Case SMC-UC3: Personal Data Sharing

A municipality manages a large number of information regarding citizens and the territory and sometimes by sharing part of its data with third party actors (companies, other public entities etc.). Data sharing process, and in particular citizen personal data sharing has to be supported by privacy enhancement tools. It is important to introduce a tool for consent management for a lawful data sharing processes, supporting data subject to grant and withdraw consent to sharing data from a service (Data Source) to be processed in another service (third party). Consent authorizes Data Sources to provision data to Data Consumer and authorizes Data Requester to process that data. Consent has to refer to a Data Usage Policy that can be linked to consent formalization. Consent needs to be given in a clear manner so that the data controller can demonstrate that a valid consent has been given. Consent record should demonstrate:

- Who consented;
- When they consented;

- What was consented;
- How was consented;
- Whether a consent withdrawn occurred;
- (in case of minor) consent on his/her behalf.

Citizen as data subject by means of a dashboard/wallet is enabled to manage and control "personal data" during the interactions in data sharing process. By means of that dashboard Data subject has a single point to verify which data are used, and how and for which purpose, receive notifications about data processing and perform objections or consent withdrawal as well as perform right to be forgotten and data portability rights.

In the general scenario of data sharing and processing we can have involved both Data Sources and Data Using Services. Data Source provides data about individuals to the services that use this data (Data Using Service) for example in the provision of personalized smart services. Data Source and Data Using Service may be the same organization, therefore in the following use case scenario we consider two types of consenting:

1. consenting to processing within a service for a specific purpose
2. consenting to sharing data from a service (Source) to be processed in another service (Sink) for a specific purpose.

8.1.3.1 Stakeholders

With the introduction of new General Data Protection Regulation (GDPR) every company, organization or other type of vendors supporting Smart Cities in service provisions and making use of personal data related to people in the EU, need to be compliant with the new privacy rules. The data controller determines the purposes for which and the means by which personal data is processed by determining and controlling also the third parties involved in personal data sharing and processing.

8.1.3.2 Actors

We consider the following actors:

- Employees;
- Citizens as data subjects;
- Service Providers as Data Controller in consuming or providing personal data;
- City Data Publisher;
- Data Protection Officer.

For an exhaustive description of these actors, please refer to [1].

8.1.3.3 Preconditions

Each informational component or service of the system acting as personal data source or data requester or both has to be assessed by collecting information about which type of personal data is collected or shared, for which purpose, with whom and definition of legal basis and reference of a specific privacy statement. This assessment has to be performed by the key persons of Data controller in collaboration with the Data Protection Officer. Another precondition is to identity any interaction with existing legacy systems, for example the identity manager, during the consent collection and management and related personal data sharing and processing, or where to collect individual consents (consent register).

8.1.3.4 Basic Flow

The end-to-end process of consent management for personal data sharing and processing encompasses the following steps:

1. Use case begins;
2. **Service description and registration**: data controller of the service provider registers the services in the platform describing the legal basis of personal data processing. Each service that will process personal data must be described and registered in a service registry provided by the consent manager. The description in particular provides, as well as basic information, the description of the data that will be processed for each purpose, indicating the type of purposes and processing according to shared and standard vocabularies and providing reference a privacy policy statement. According to the type of integration with existing legacy systems, technical details (e.g. service endpoints, storage APIs, etc.) must be included in the service description. A new description of the service and any next related update at the service registry requires its versioning with related time stamp and digest. The data controller can save the versioned description of the service in the service registry:
   i. in "as a service" mode, accessing to a remote service registry;
   ii. or locally through the integration, by means of ad hoc SDK, with already existing local systems.

   The registration of the service (and therefore the upload of its description) is performed directly by means of APIs exposed by the service registry or mediated by a graphical service editor.

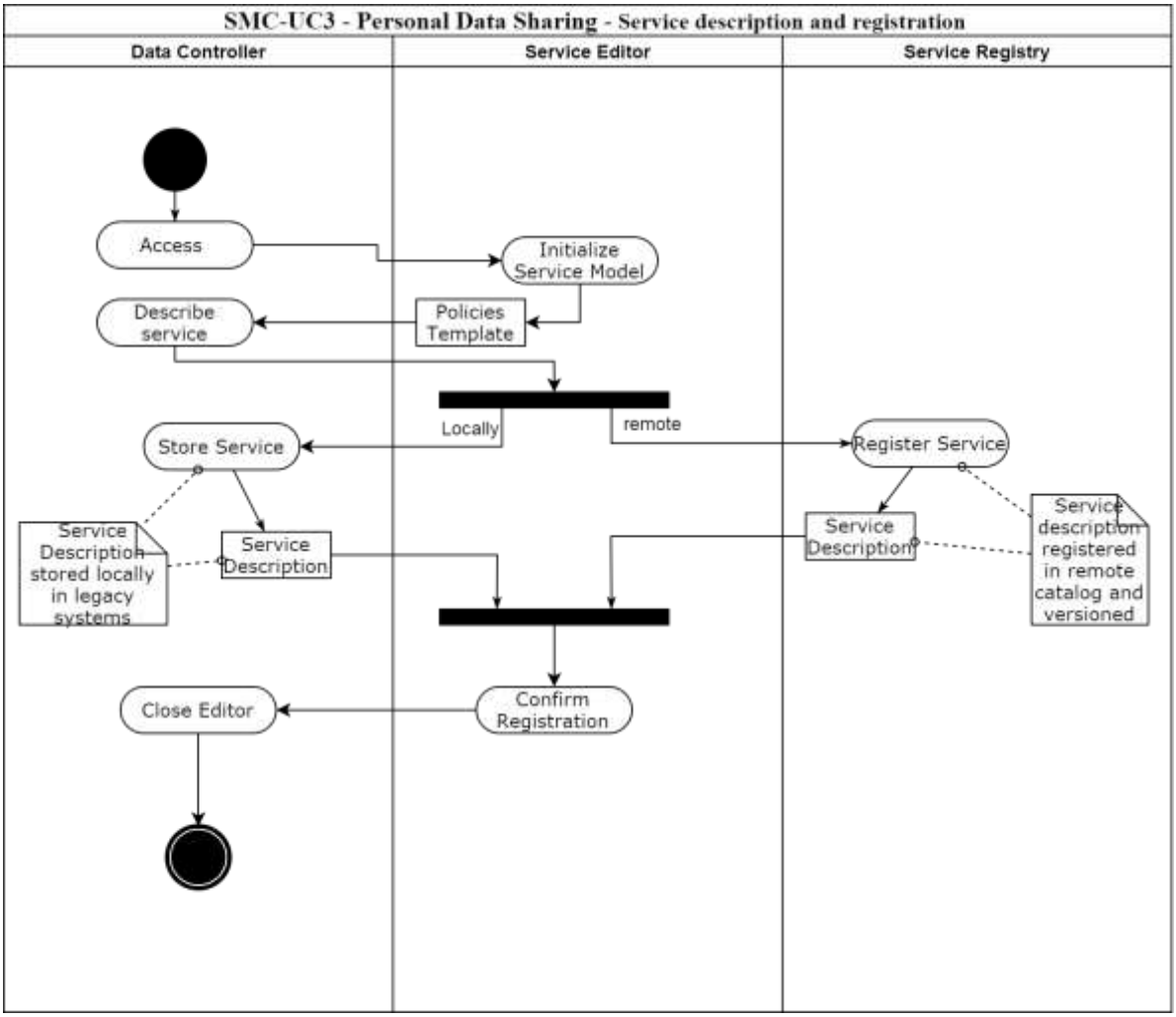

Figure 113: Smart Cities - SMC-UC3 Service description and registration use case flow diagram

3. **Service linking**: in order to interact with a specific Data Subject and request a lawfully data processing, each registered service must be able to identify the data subject at consent management system. This "Service Linking" phase creates a one-to-many reference between the identification of the data subject at consent management tools and his/her identification at each service. The Service Linking phase is based on a process of identification, and possibly authentication of the data subject both at consent management tools and at the service. The identification and authentication process can include several cases:

   iii. Consent manager and each service use different Identity Managers (IdM);

   iv. Consent manager uses a specific IdM and all services use a unique IdM, as they belong to the same organization (e.g., organization single sign-on SSO);

   v. Both consent manager and services use a unique (internal or external) IdM.

   Service Linking process can be initiated either by the data subject through a client front-end (dashboard, wallet or user profile page) by selecting/activating a specific service, or by each service during the data subject's interaction with the service itself, for example by accessing in a registration page. In both cases, a token (service link record - SLR) is created for each association containing the pair of references of the data subject, and related status, SSR (e.g., active, suspended, etc.). The aforementioned token and its status will be saved both by the consent manager and by the service.

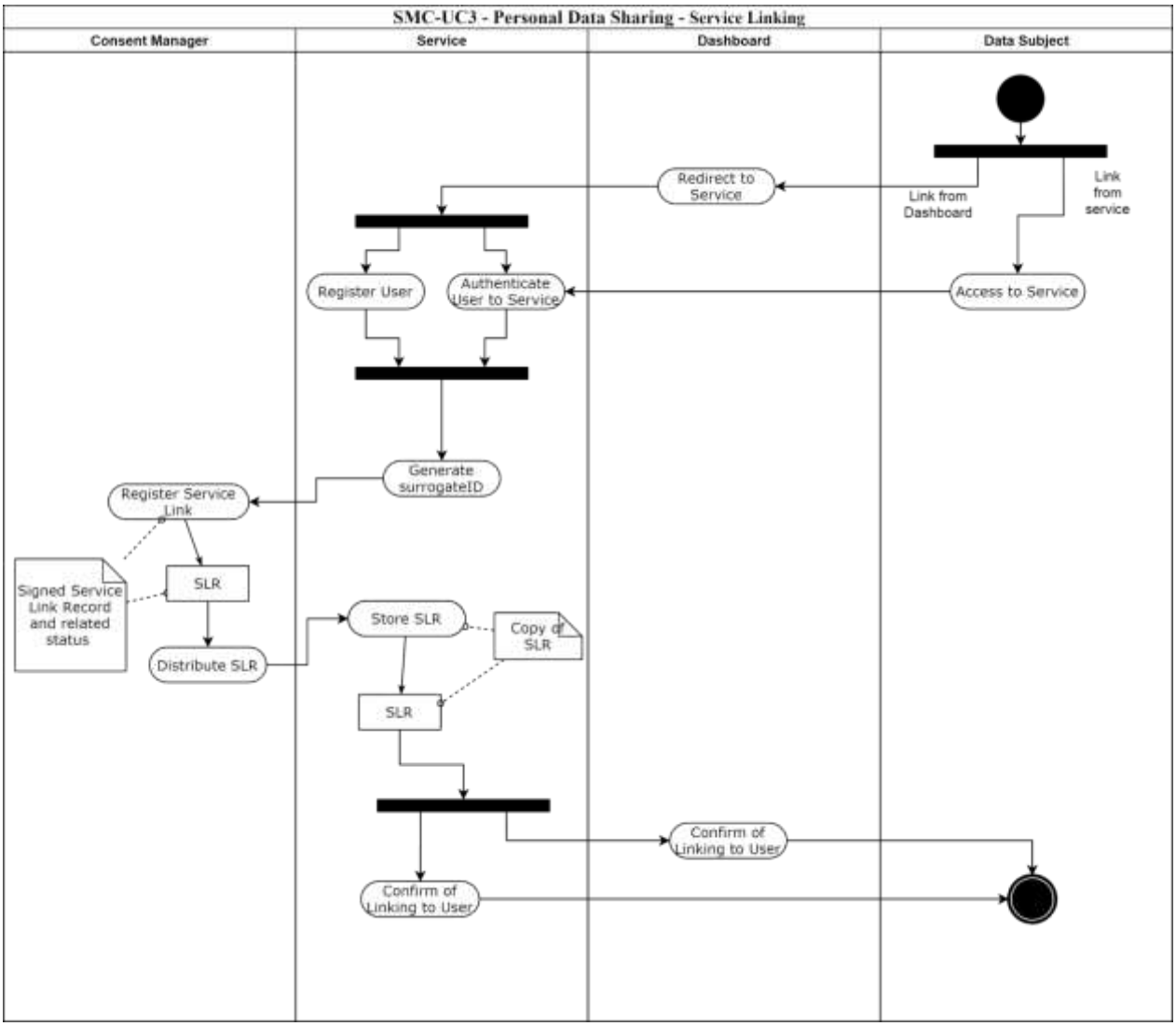

Figure 114: Smart Cities - SMC-UC3 Service linking use case flow diagram

4. **Consent Management:** the consent management process always starts from the phase in which the user accesses the service which, either because the user accesses the first time or the conditions have changed, requires the consent for the processing of the data for the specific purposes as also reported in the privacy disclaimer. Two type of consenting are envisaged:

   vi. *Within a service*: consent is required for the processing of data within the service itself for different purposes for which personal data have been obtained or if it is intended to share them with other companies/services for the declared purposes.

   vii. *Sharing among services*. Scenario in which in an ecosystem of inter/intra connected services consent is required for the sharing of personal data among data sources and data using services.

   The explicit acceptance phase of the consent requires that the service retrieve the descriptions of the legal basis described during registration (or any next updates of service description), generate the consent form to be shown to the user, retrieve the consent options selected by the user and send the request to consent manager to save, notify and certificate the consent. The service will receive a signed consent receipt (CR) and related consent status (CSR) with time stamp and digest. In case ii) (sharing among services) the consent receipt is forwarded both to data source and data requester. Besides the requesting service receives an authorization token to be used for data requests.

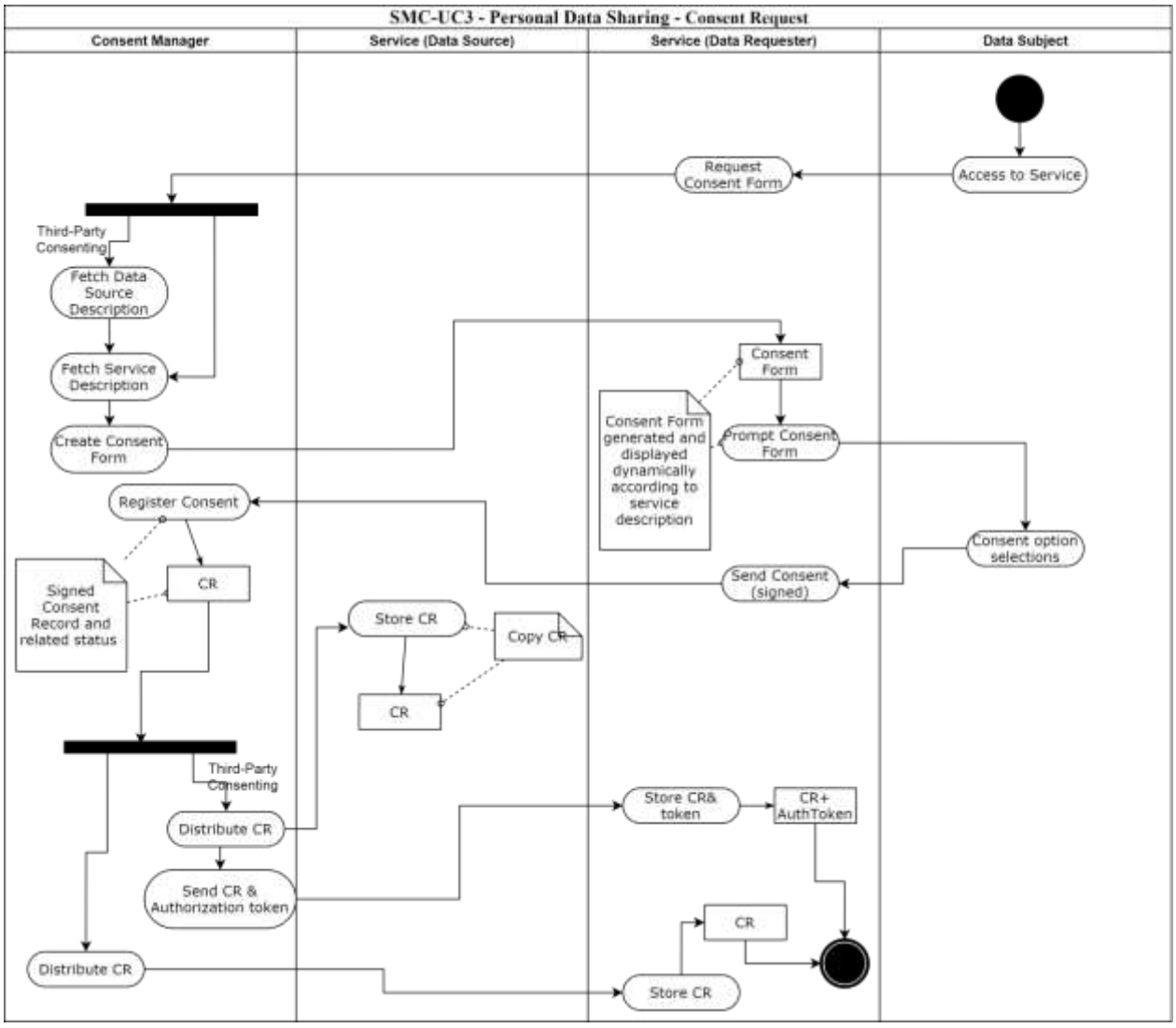

Figure 115: Smart Cities - SMC-UC3 Consent request use case flow diagram

5. **Personal data request:** once received authorization token during the previous consenting transaction, the requesting service can perform multiple requests to data provider (Data Source) as long as the authorisation and related consent are active. In the request payload the requesting service provides the authorization token and the reference to the active consent. The request is signed by the requesting service. When the data provider receives the data request it verifies the request, token and consent record status. The data provider verify that the request is for a dataset settled in the active consent and related to the constraints contained in the consents (purposes, processing, third party sharing, etc.). According to the validation data provider either denies or grants access to requested resources.

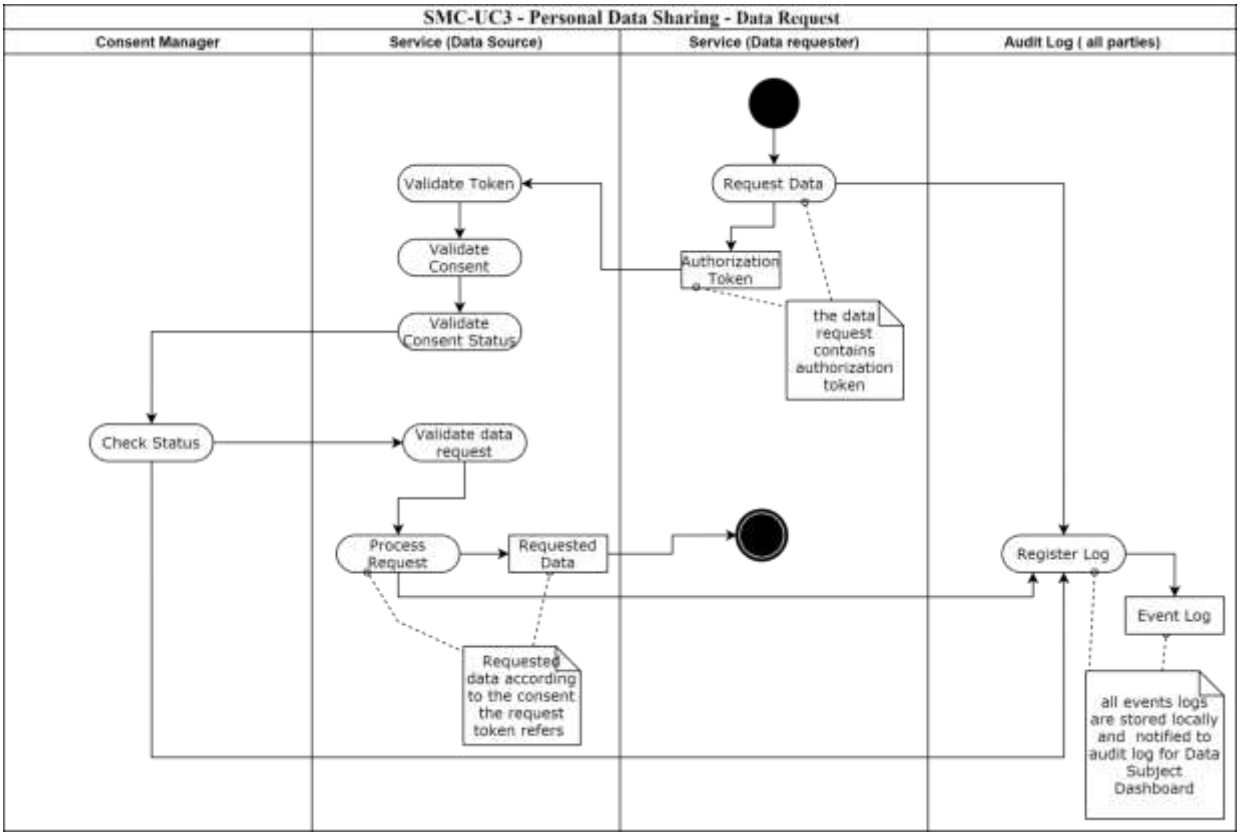

Figure 116: Smart Cities - SMC-UC3 Data request use case flow diagram

6. **User Data Usage Control:** once a consent is given the data subject can display and verify all the punctual information on a single type of personal data, or on a timeline basis, or grouped by categories on who, when and for what purpose their personal data are being processed. For each given consent that data subject can modify the constraints (data sets, purposes, processing, third party sharing) suspend the consents or definitely withdraw them. The data subject can receive notifications from each data controller or send objections about the usage of personal data. Any change of consent performed by the data subject by means of dashboard is elaborated by consent manager and the new consent receipt is forwarded to all parties involved (data requester and data provider);

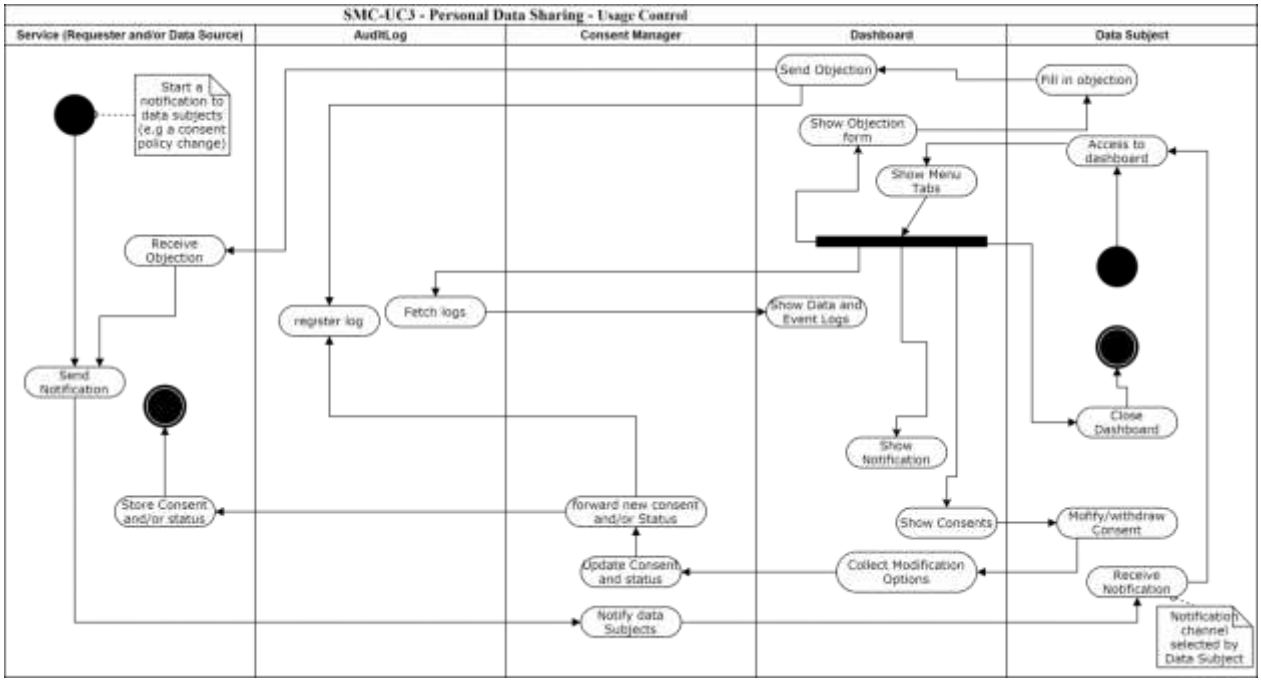

Figure 117: Smart Cities - SMC-UC3 Usage control use case flow diagram

7. Use case ends.

8.1.3.5 Postconditions

Data requester service either receives the personal data it requested or receives a denial message. The results of data request are based on the definition of the legal basis of personal data sharing and processing, the consent collection and its distribution to data provider and data requester and its lifecycle management by the data subject. Besides, the data subject receives all the information about the usage of personal data according to the given consents and related modifications.

8.1.4 Use Case SMC-UC4: Sensor Data Sharing and Processing

Cities must leverage the multiple sources of information regarding sensor data, i.e. IoT data. In this scenario, different stakeholders can produce data, so the ownership of data is spread across these actors. The data processing performed by various entities must be compliant to the GDPR so the following concerns must be taken care of:

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

The Municipality's goal is to maintain data security and governance while allowing multiple stakeholders to participate, private (companies) and public (law enforcement, etc.) entities to participate.

8.1.4.1 Stakeholders

We consider the following categories of stakeholders:

- Local Public Administration: It includes all public entities involved (administrative, public employee, civil servants and other staff...) in smart cities processes and public service provision;
- Service Suppliers: Public and/or private organizations which provide any type of smart cities services generally processing data (personal or not);
- Platform Provider: Entities working with the providers of city data and services, and managing the content, defining policies and regulations of the platform.

8.1.4.2 Actors

We consider the following actors:

- Citizens;
- City and Service Providers as Data Providers or Data Consumers;
- Other Data Providers (e.g., IoT owners);
- Data Protection Officer.

For an exhaustive description of these actors, please refer to [1].

8.1.4.3 Preconditions

Each sensor is installed and registered to platform describing the type of data is collecting.

8.1.4.4 Basic Flow

The figure below, describes the flow of this use case.

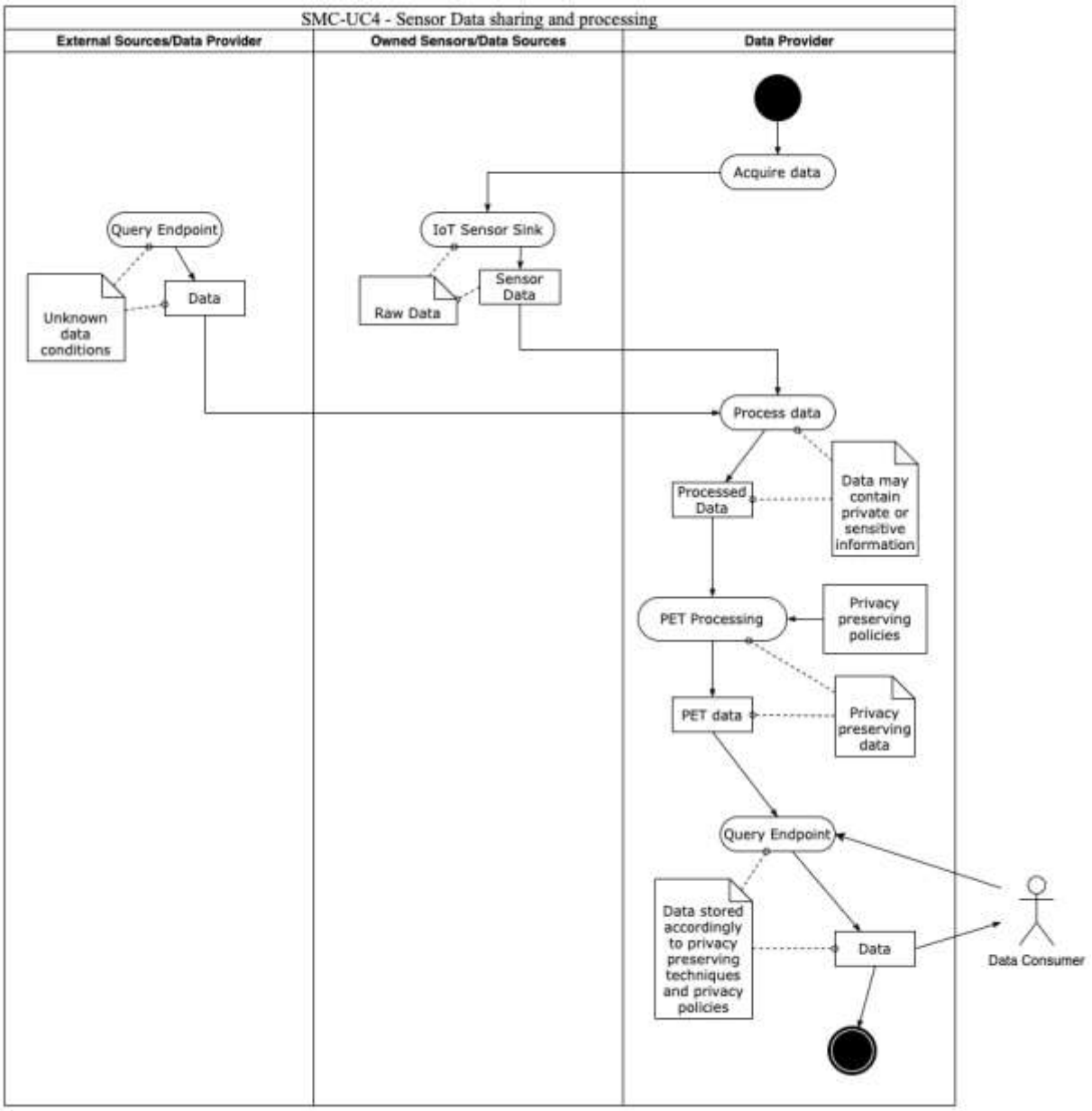

Figure 118: Smart Cities - SMC-UC4 Sensor data sharing and processing use case flow diagram

1. Use case begins;
2. **Data acquisition**: The Data Providers acquires data from the sensors it owns (RAW data) or from third-party (other data providers or external data sources). This data is expected to be processed according to the provider's business model or usage. Since both RAW data and third-party data may contain sensitive or private information, the processed data is expected to contain private/sensitive information;
3. **Applying privacy preserving tools**: Processed data is treated using privacy enhancing technologies (PET) and tools for removing sensitive information according to the privacy preserving policies. This step is essential for preventing leakage of private information as this data will be made available to third parties.
4. **Sharing data**: A query endpoint allows Data Consumers or third-party entities to access data shared by the Data Provider.

8.1.4.5 Alternate Flows

As an alternate flow, the Data Provider may also apply privacy enhancing technologies (PET) and tools prior to the data processing step for ensuring that no privacy issue are compromised during data processing, as presented in the figure below.

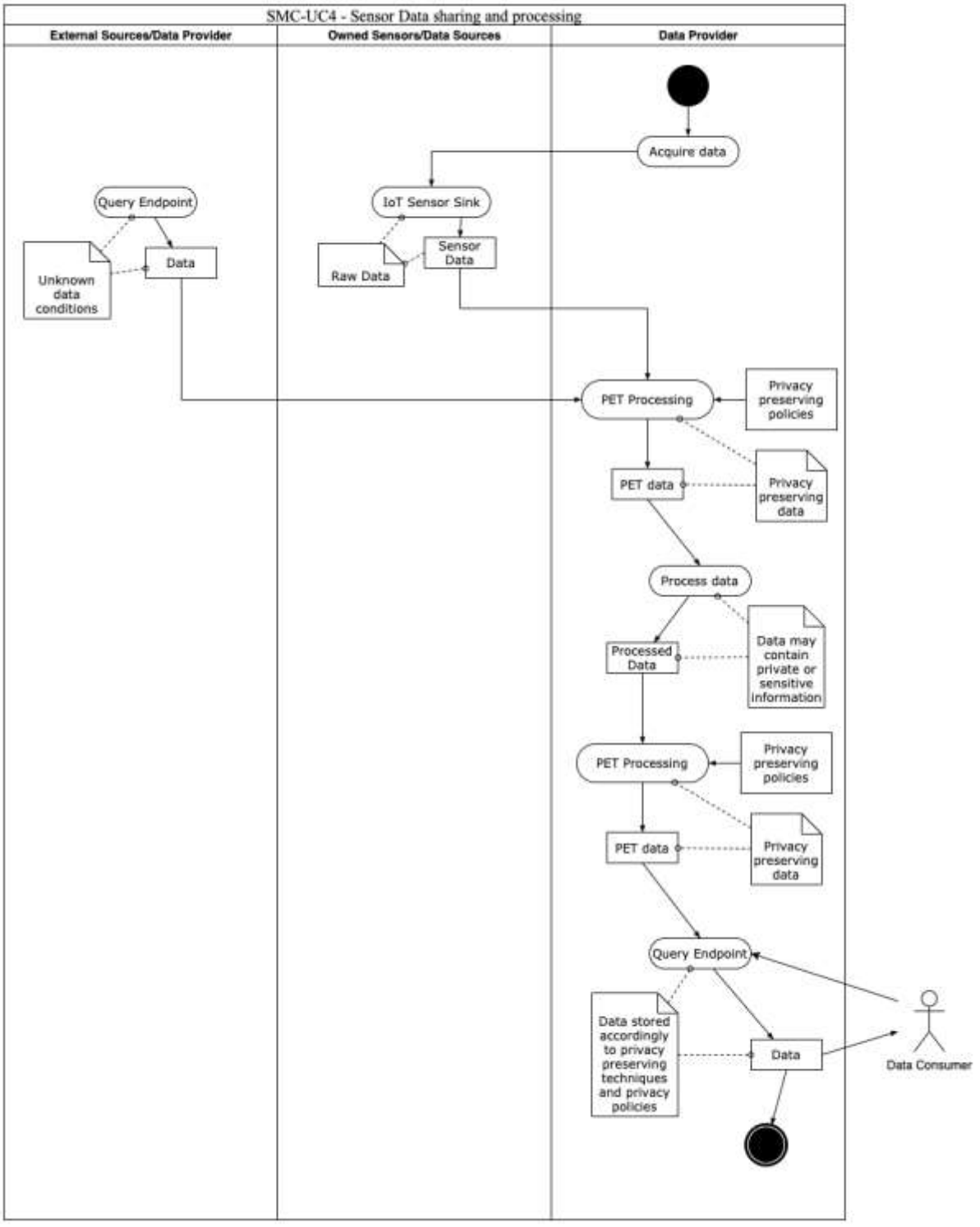

Figure 119: Smart Cities - SMC-UC4 use case alternate flow diagram

8.1.4.6 Postconditions

Data and elaborated information are available to Data Consumer.

8.1.5 Use Case SMC-UC5: Assess Social Engineering Exposure by Simulating Phishing Attacks on Service Provider's Target Groups

In this Use Case the CISO (or managers), performs a social driven vulnerability assessment (SDVA) (e.g. phishing simulation) within pseudo-anonymized target groups (employees, department, specific team, etc…). The UC 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. The. pen-tester basically performs the stages, described below:

- **Information gathering**: in this stage, the pen tester performs search about Digital Shadow of the Service Providers. Such research can be performed on several sources, such as Pastebin, WikyLeaks, WhoIS, DNS etc, simply by providing query strings. The results are then filtered according to sensitive/no-sensitive type of information;
- **Design and implementation of the attack**: this stage is focused on the design of the attack-hook and the landing page of the fake website. Basically, the pen tester, defines the attack vector to implement;
- **Launch and monitorin**g: once defined the hook, the attack must be armed with targets, scheduled and launched. This stage collects attack-information about hit targets, and also get fingerprints of the attacked devices;
- **Information Aggregation and Reporting**: this stage aggregates results of the attack and, according to pseudo-anonymization policies, provides statistical representation of the attack, focusing on successful attacks. Moreover, for each successful fingerprint detected, the discovered Common Vulnerabilities and Exposures (CVE) are compared with external data sources to get evidence, in human readable reports, about criticality of the target's technologies.

This UC finish once the attack is terminated and final reports has been provided to the CISO, whose can analyse the phishing campaign results, address the most critical assets and keep going, its control/awareness/assessment cycle.

8.1.5.1 Stakeholders

Several stakeholders are involved with several interest:
CISO:

- To set up the Social Driven Vulnerability Assessment and delegate pen-tester to perform the assessment;
- To get evidence of the most critical aspects of the attack;
- To understand the technological vulnerabilities of hit devices in order to be aware of the risks;
- To easily understand which targets-group are the most susceptible to phishing attacks, in order that is possible to focus on specific awareness methods;
- To not know personal data of targets neither to be able to identify people.

Pen Tester:

- To gather information about the service providers, in order to define the digital shadow of the organization, useful information to be used to define the attack vectors;
- To define hook of the phishing attack and easily create a fake-landing web page to conclude the attack;
- To execute the attack, define time schedule and monitor the attack in order to find the most critical aspects;
- To collect all the outcomes and reports both human and technological vulnerabilities to C-Levels.

8.1.5.2 Actors

We considered the following actors:

- Chief Information Security Officer, Chief Information Officer, Chief Executive Officer, Risk Manager: They represent the main contact of the organization. This actor is the only one who needs to talk with the pen tester. Moreover, such actor set up the SDVA;
- Penetration Tester: such actor performs the social driven vulnerability assessment. It is responsible to execute all the main stages reported in Figure 120, except the SDVA set up step;
- Employees: they are the targets of the attacks, they don't have an active role in the system since they receive the phishing email in their own mail boxes.

8.1.5.3 Preconditions

Before the execution of the SDVA, the organization (DPO – CISO – or who else) must define a Privacy Impact Assessment according to the Attack Plan. Such Assessment will be followed by the Pen Tester, so that he/she can execute the attack and comply with privacy regulations and boundaries. Finally, according to the Pen-tester, the CISO must provide information about SMTP server, and provide targets list.

8.1.5.4 Basic Flow

The figure below, describes the complete round of the Social Driven Vulnerability Assessment.

1. Use case begins;
2. CISO access to the SDVA Management GUI, initialize the assessment and set pen-tester account;
3. Pen tester access to the SDVA Management GUI and start the Information Gathering Process;
4. The Information gathering stage:
   4.1. Create a search;
   4.2. Select the search type and provide the query string (url, key word, etc.);
   4.3. Start the search - Data Collection;
   4.4. Data Set Analysis - Filtering the results according to Privacy Regulations (deleting, for instance, possible sensitive information about targets).
5. Pen tester access to the "hook preparation" stage:
   5.1. Create the hook of the attack;
   5.2. Web Site Configuration - Pen tester create the landing page of the fake web site;
   5.3. Email Configuration - Pen tester create the email content of the hook.
6. Pen tester access to the "execution of the attack" stage:
   6.1. Set up of the attack;

6.2. Attack Scheduling - Define time scheduling of the attack;

6.3. Launch the attack;

6.4. Attack Monitoring - Monitor the attack;

6.5. Close the Attack.

7. Pen tester access to the “Information Aggregation and Reporting” stage:

7.1. Access to the Aggregation and Reporting Module;

7.2. Perform by-default aggregation rules;

7.3. Can define new aggregation rules and have custom reports:

7.3.1. Create and select the aggregation rules;

7.3.2. Perform aggregator service.

7.4. Access to the statistical representation of the outcomes, whose aim is to analysis the percentage of people that have fall into the attack;

7.5. Discover technological vulnerabilities according to discovered CPE (fingerprint);

7.6. Pen tester make the report for C-Level.

8. The use case ends.

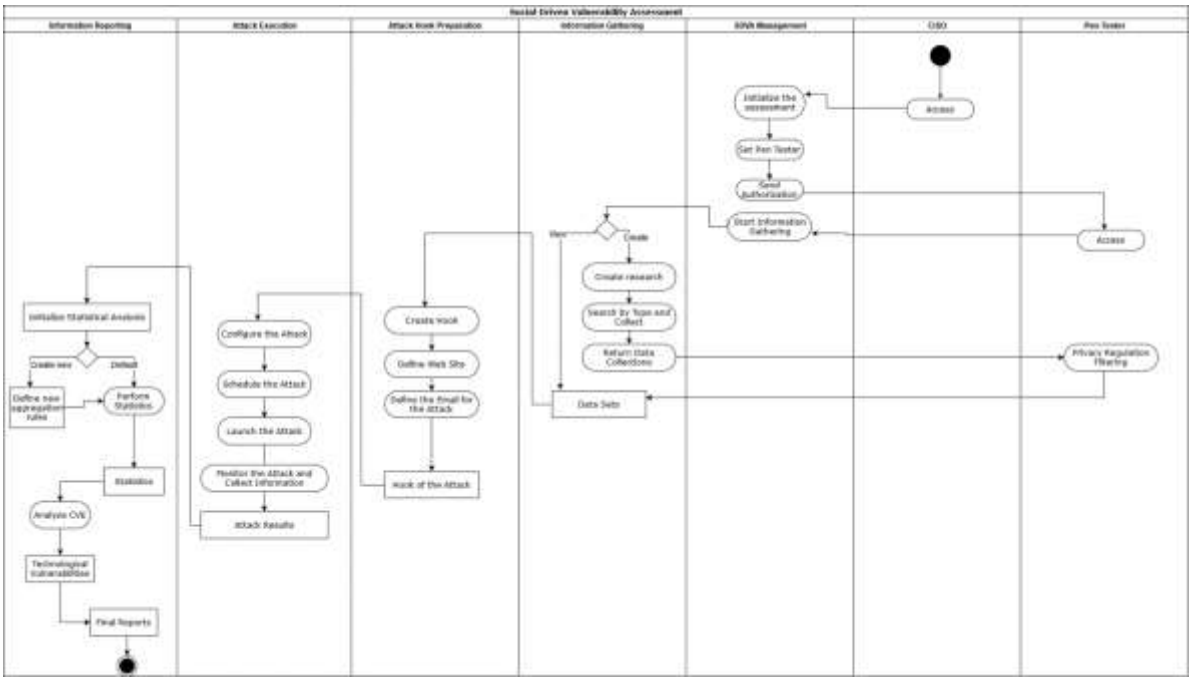

Figure 120: Smart Cities - SMC-UC5 Social driven vulnerability assessment use case flow diagram

8.1.5.5 Postconditions

CISO will have complete reports of the SDVA. With this UC, the Service Provider can understand the percentage of social engineering attacks exposure and enhance awareness about the most critical target-groups to better focus countermeasures/awareness procedures.

8.1.6 Use Case SMC-UC6: Cyber Risk Assessment

This UC allow 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. In details, through this UC, is possible to perform a cyber risk assessment, whose main stages are described below:

- **Company Profiling:** such stage, is focused on the identification of the main assets of the service provider. Such assets are basically the resources involved in a specific process/team/department etc… whose managers decide to profile during the assessment;
- **Cyber Vulnerability Assessment:** this stage allows CISO to evaluate the cyber maturity model of the service-provider. The assessment process follows holistic approach, which is based on the identification of the most dangerous Threat Agents, the estimation of the likelihood to be attacked and the vulnerability exposure of the assets. Through this stage, the CISO is able to analyse critical aspects and give useful information to the risk model;
- **Impact Analysis:** following both qualitative and quantitative impact analysis, the CFO, can easily identify cascading effects scenarios on assets, evaluate the capital at risk, simulate the losses and prioritize main key assets. Finally, this stage provides the impact scores of each evaluated asset;
- **Risk Modelling:** this stage is basically the aggregation of the likelihood, vulnerability and impact scores produced by previous analysis. In this way the CRO can, be supported by risk matrix models, and distinguish tolerable risk from non-tolerable ones. Finally, makes decision on best cybersecurity mitigations strategy to implement.

8.1.6.1 Stakeholders

Basically, for large/medium enterprises, CISO/CFO/CRO are the main stakeholders of this use case, while for small enterprises, even managers should be able to perform such cyber risk assessment. To better describe the main interests of the stakeholders, below a "user story" description is provided:

- As CRO I want to identify the cyber risk of my organization so that I can be supported to identify best cybersecurity investments to protect the organization;
- As CISO I want to assess the vulnerability of my organization so that I can evaluate its cyber posture and the exposure to cyber-attacks;
- As CISO I want to implement a cybersecurity program aligned with business strategy so that I can protect the business and take evidence of possible cascading effects;
- As CISO/CFO/CRO I want an inventory of the processes at risk and their assets so that I can prioritize my cybersecurity investments;
- As CISO/CFO/CRO I want to identify costs related to the cyber-attacks so that I can estimate the cascading effects of the losses scenario;
- As CISO/CFO/CRO I want to identify both tangible and intangible assets at risk so that I can be in line with ISO31000 and 27001;
- As CFO I want to perform qualitative impact analysis so that I can prioritize my processes/asset at risk;
- As CFO I want to perform a quantitative impact analysis so that I can simulate the economic losses;

- As CISO/CFO/CRO I want to access to a clear risk management dashboard so that I can easily have clear prospective of my risks;
- As CRO I want to define risk tolerance for each scenario so that I can take my own decisions;
- As CISO/CFO/CRO I want human readable reports so that I can easily understand the situation and communicate it to other C-boards.

8.1.6.2 Actors

We considered the following actors:

- CISO/Cybersecurity Manager: this actor is responsible to perform the cyber vulnerability assessment;
- CRO/Risk Manager: this actor is responsible to manage the identified cyber risk. He defines risk tolerance and priority;
- CFO/Financial Manager: this actor is responsible to provide financial information about the organization in order to estimate both tangible and intangible capitals at risk.

8.1.6.3 Preconditions

- For the CISO: It is expected that he/she is aware of the currently procedures, best practices and cyber controls implemented in the organization;
- For the CFO: to perform quantitative impact analysis on economic losses, the component requires some financial data as inputs. It is expected that such information is provided by the CFO.

8.1.6.4 Basic Flow

1. Use case begins;
2. The CISO initializes the risk assessment, providing information about the title of the assessment;
3. CISO (in create-mode), identifies the assets involved in the assessment (Asset Clustering). They can be tangible and intangible;
4. 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;
5. 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;
6. Based on estimated cascading effects and vulnerability exposures, the CFO can perform both qualitative and quantitative analysis. For the qualitative analysis, it's required to prioritize the assets at risk, while, for the quantitative, it is expected that the CFO provides financial data to estimate capital at risk;
7. 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;
8. 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;
9. 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;

10. Use case ends.

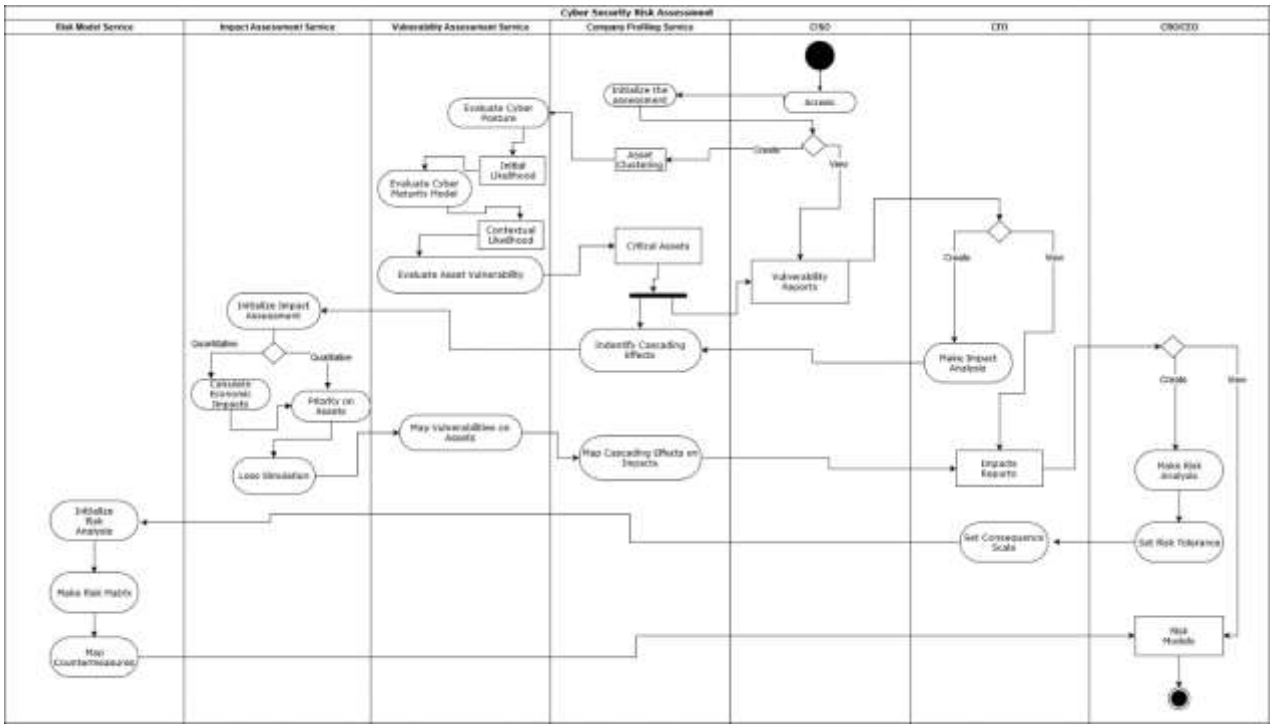

Figure 121: Smart Cities - SCM-UC6 Cybersecurity risk assessment use case flow diagram

8.1.6.5 Postconditions

With this UC C-boards can identify and prioritize Cybersecurity risks. Following the basic flow, the users get evidence of organization's risks, with a special focus on intangible losses, as reputation, brand and key competences.

8.1.7 Use Case SMC-UC7: Cybersecurity Needs and Solution Elicitation and Selection

Following a security and privacy assessment the stakeholders of a Smart City stakeholders as authenticated user have access to functionalities to provide information about their needs, ideas and/or challenges. Each stakeholder is involved in the process and is invited to cooperate with each other to identify and address needs, implement ideas and meet challenges.

8.1.7.1 Stakeholders

Smart City stakeholders can identify cybersecurity threats/risks and collaborate on "co-defining" related potential solutions/best practices, already available or new ones to publish in a city market place. Based on the service or process subject to assessment, the stakeholders can be entities of the municipality and/or external entities (e.g., service providers)

8.1.7.2 Actors

We consider the following actors, as authenticated users:

- Smart City Employees;
- Chief Information Security Officer, Chief Information Officer, Chief Executive Officer;
- Data Protection Officer;
- Risk Manager.

For an exhaustive description of these actors, please refer to [1]. Each type of actor could perform several roles as authenticated user: as *author* to create a need, an idea or a challenge, as *collaborator to* provide further information during the process, as *evaluator* to evaluate idea/solution.

8.1.7.3 Preconditions

Smart City stakeholders involved (in particular representatives from the Local Municipality) have previously assessed and identified security and privacy risks, needs and problems related to the services and/or processes subject of the assessment.

8.1.7.4 Basic Flow

The use case encompasses the following steps:

1. Use case begins;
2. Problems Definition. Stakeholders involved (in particular Municipality) share information in order to have a mutual understanding about needs, problems and services. Mutual knowledge is created;

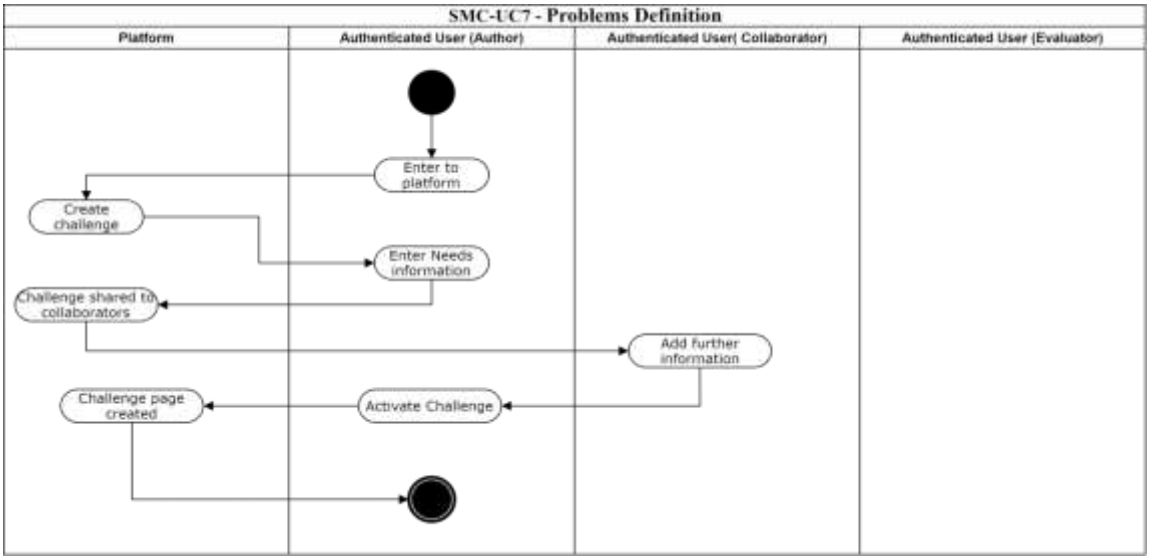

Figure 122: Smart Cities - SCM-UC7 Problem Definition flow diagram

3. Idea generation. Stakeholders co-define the implicit knowledge created in the previous phase and convert it in explicit and shared knowledge. The collaboration between the users is promoted in this phase, in order to co-create innovative ideas to solve the problems discovered in the previous steps;

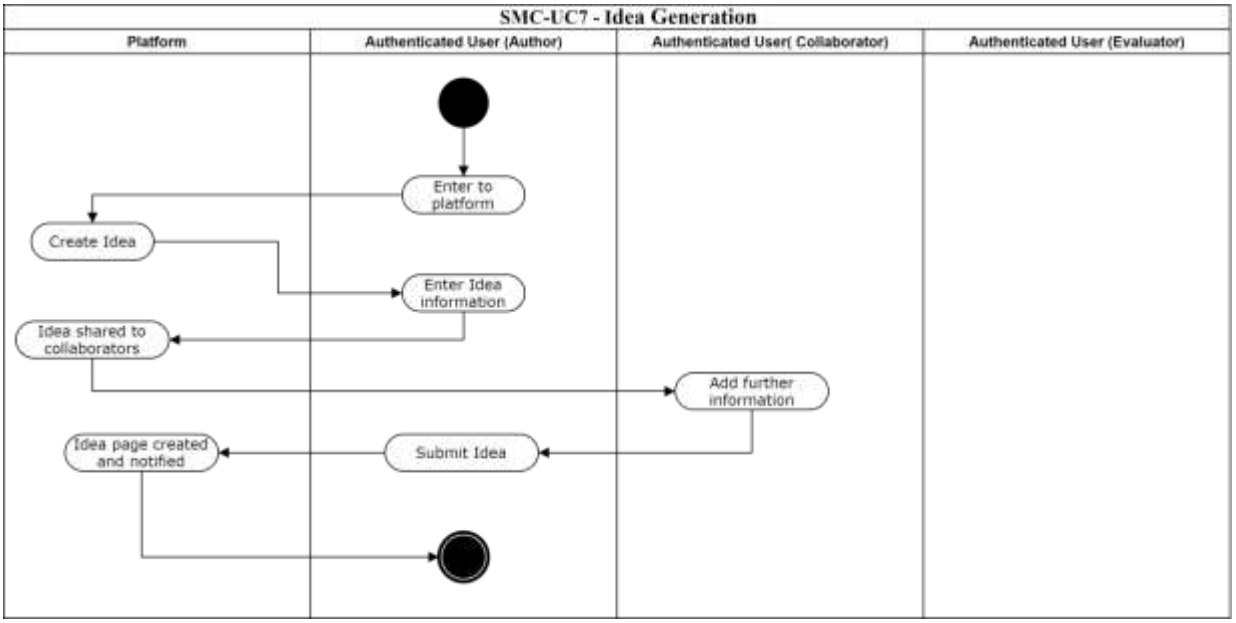

Figure 123: Smart Cities - SCM-UC7 Idea Generation flow diagram

4. Ideas Selection. The Municipality, together with an expert team (appropriately appointed) evaluates all the proposed ideas based on a set of barrier and quantitative criteria and select a subset of ideas to be refined;
5. Idea Refinement. Each idea/solution is further analysed, detailed and, in case, partitioned in sub solutions;

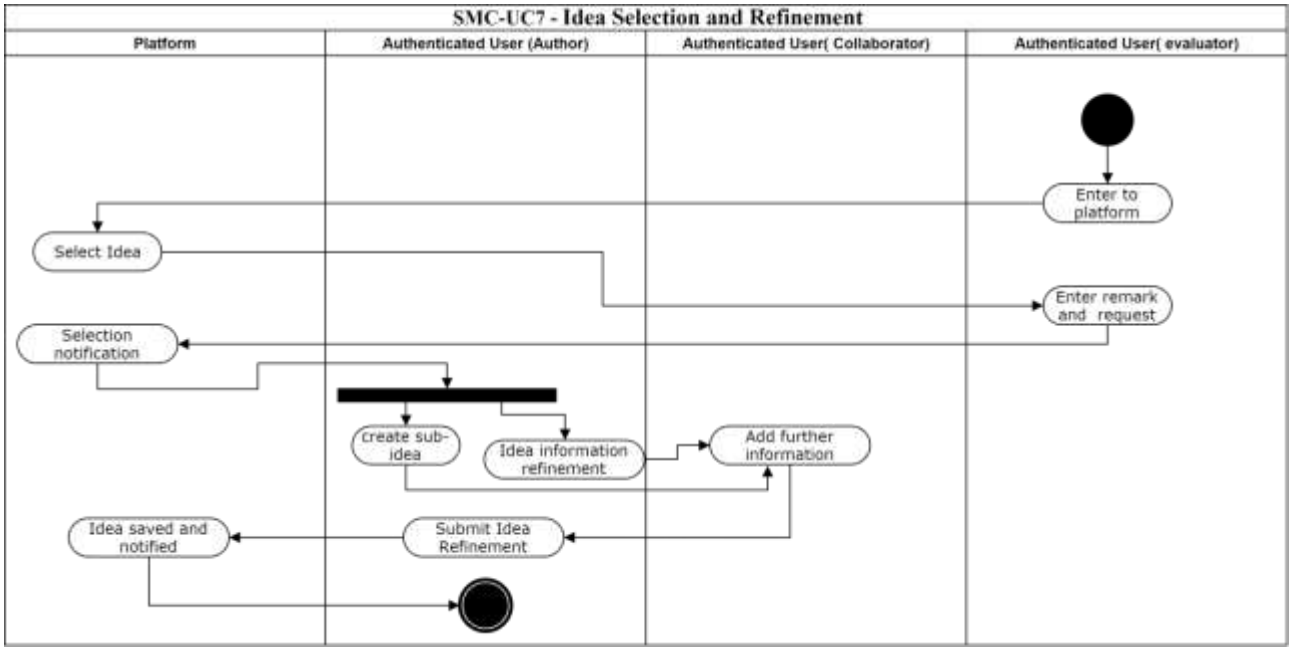

Figure 124: Smart Cities - SCM-UC7 Idea Selection and Refinement flow diagram

6. Solution selection. Starting from the refined ideas a solution is selected. The stakeholders start a process of collaborative design and development. The author and the collaborators of an idea cooperate

with each other to implement the refined idea. To do this, the involved actors are also supported by a marketplace of cybersecurity services and best practices to be used for the solution implementation;

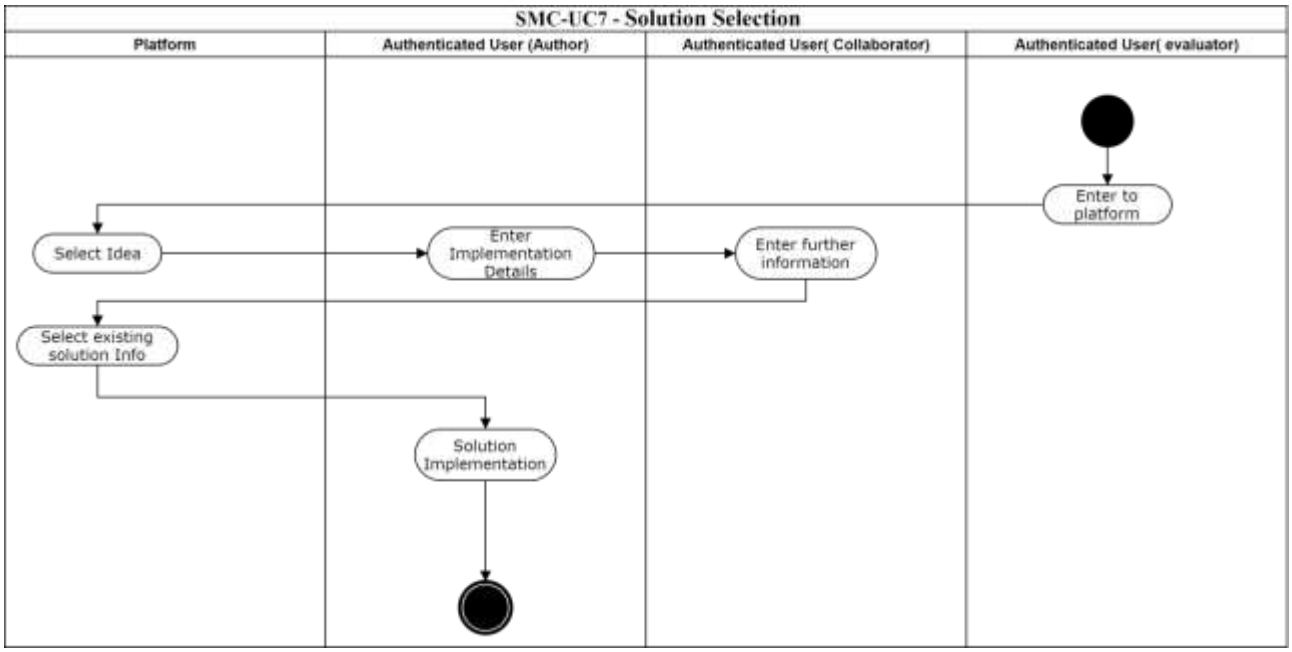

Figure 125: Smart Cities - SCM-UC7 Solution Selection flow diagram

7. Use case ends.

8.1.7.5 Postconditions

The implemented solution can in turn be published in the marketplace for later discovery and adoption.

8.1.7.6 Included Use Cases

Use Case SMC-UC7.1: Register New Need

Description

Actor registers a new need into the platform

Preconditions

Actor already indicated his/her city.

Basic flow

1. Actor asks to create a new need;
2. The system provides the creation form including all the required input areas, as title and description;
3. Actor fulfils the form and concludes the action;
4. The system creates the new need and updates the related list of needs available.

Postconditions

Actor already indicated his/her city.

Use Case SMC-UC7.2: Create New Idea

Description
Actor creates a new idea.

Preconditions
Actor already indicated his/her city.

Basic flow

1. Actor asks to create a new idea;
2. The system provides the creation form including all the required input areas, as title and description;
3. Actor fulfils the form and concludes the action;
4. The system creates the new idea and updates the list of ideas available.

Postconditions
The new idea has been created.

Use Case SMC-UC7.3: View Needs, Challenges, Ideas

Description
Actor visualizes the list of available needs, challenges, ideas.

Preconditions
Actor selected his/her city.

Basic flow

1. Actor requires to view the list needs, challenges, ideas;
2. The system retrieves the contents related to the city and provides a page representing the results.

Postconditions
Actor is allowed to interact with the results list.

Use Case SMC-UC7.4: Manage Challenge

Description
Actor manages the challenge.

Preconditions
Actor accessed the challenge page.

Basic flow

1. Actor manages the challenge description providing additional details, defining the selection criteria and updating the deadlines;
2. The system accepts the changes and updates the challenge details page.

Postconditions
The challenge has been updated.

Use Case SMC-UC7.5: Evaluate Ideas

Description
Actor provides the evaluation for each idea.

Preconditions
Actor accessed the challenge page.

Basic flow

1. Actor accesses the evaluation page;
2. The system provides evaluation form for each gathered idea
3. Actor provides evaluations and motivations according to the selection criteria;
4. The system accepts the changes and updates the challenge details page;
5. Actor complete the action closing the evaluation phase;
6. The system provides the evaluation page where the promoted ideas are highlighted.

Postconditions
The challenge has been updated.

Use Case SMC-UC7.6: Manage Idea Life Cycle

Description
Actor receives a notification about the improvement of an idea and updates the phase in the life cycle.

Preconditions
Actor accessed the idea page.

Basic flow

1. Actor checks if the idea description and the tasks completed addressed all the requirements and specifications expressed;
2. Actor checks if the selected NBS is coherent with the solution to be co-defined;
3. Actor complete the action promoting the idea to the next phase in the life cycle;
4. The system executes the request updating the idea description page.

Postconditions
The idea has been updated.

Use Case SMC-UC7.7: Contribute Idea

Description
Collaborator checks the task assigned and provides the requested contributes.

Preconditions
Collaborator accessed to idea details page.

Basic flow

1. Collaborator accesses the task management session;

2. The system provides the list of the tasks related to the idea
3. Collaborator checks the details of the tasks assigned to him/her;
4. Collaborator provides the contribution requested and set the task as accomplished;
5. The system saves the contribution and updates the task status.

Post Condition
Tasks list has been updated.

8.2 Demonstrators Set-up

8.2.1 City of Murcia

The Smart-City of Murcia consists of a FIWARE platform that gathers data provided by hundreds of sensors and other data sources, such as parking providers or public transportation companies. The available information in the system ranges from agronomical sensor information from probes deployed on parks and gardens, parking availability information, traffic information, noise sensors, weather stations and public transport information to name but a few.

Some of the potential applications of the existing technology and data, range from traffic congestion alleviation, improving on the efficiency and sustainability of resource usage (with special interest on hydric resources) and general safety and well-being of citizens. Additionally, the dynamization of local commerce and the improvement of the interaction between city officials and citizens have also been postulated as objectives of the project.

With this demonstrator, we are extending the security and privacy aspects of the existing platform (see red outlined box in Figure 126, by implementing the Self-Sovereign Privacy-Preserving Identity Management System (SS-PPIdM), that will allow to accommodate the registration of users to the Smart-City ecosystem, taking into consideration their preferences regarding privacy and how their personal data is to be shared and used for identification by the different services registered as part of the Smart-City project.

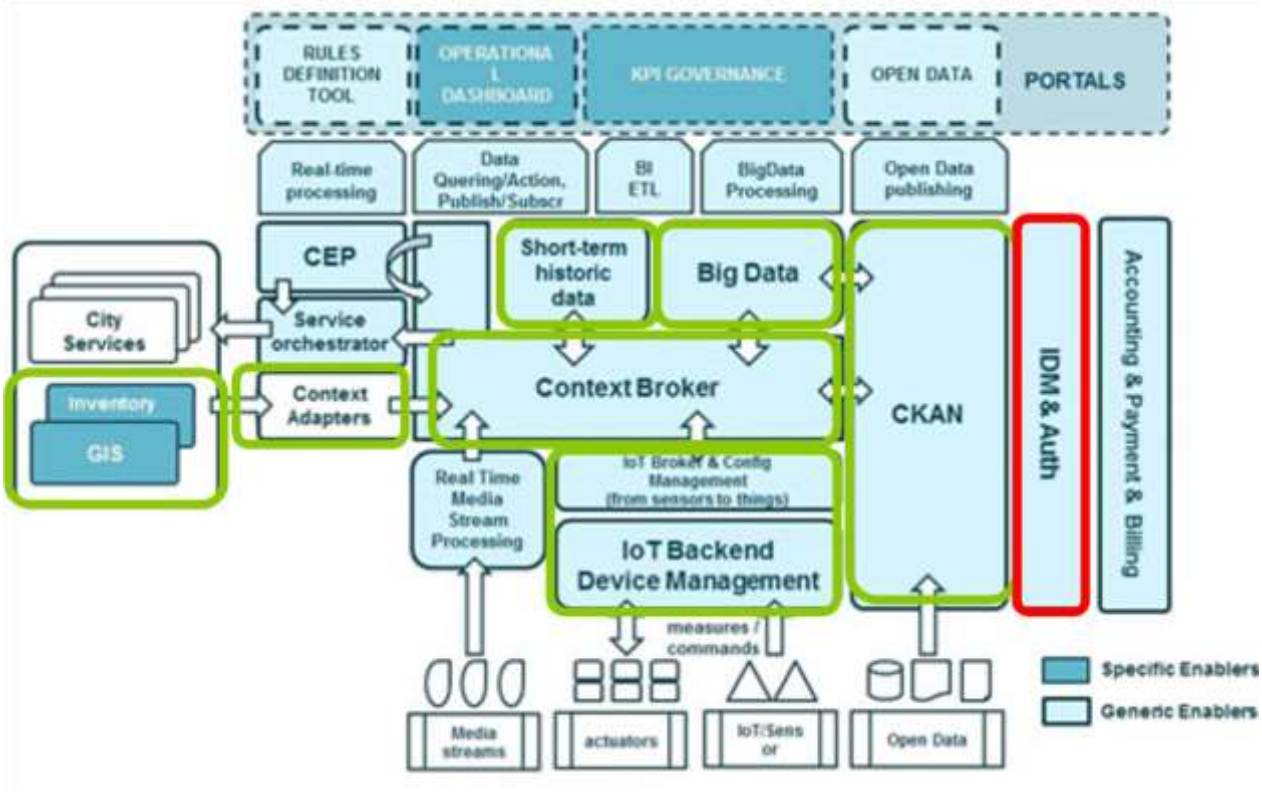

Figure 126: Smart Cities - Fiware architecture implemented in Murcia

Security tools based on XACML for the enforcement of policy-based access control to the Smart-City platform data, working hand in hand with the SS-PPIdM, will be deployed as well in order to allow registered users (citizens, SMEs and other services) to search, discover and consume Smart-City data in a secure and regulated way. The XACML-based Access-Control Enforcement System deployed, addresses the distributed nature of the platform by providing a Capability-based Access Control system in which constrained devices (e.g. sensors, actuators) are able to make authorization decisions without the need to delegate this task to a different entity, following the DCapBAC model.

Concerning privacy and personal data, GPDR based tools will be deployed and used in order to guarantee that the conceived XACML policies are compliant by-design with the regulation. More precisely, inspired by the Data Protection by-design and by-default requirement, these tools ensure XACML policies development and testing in line with the GDPR's demands.

Finally, additional technologies based on CP-ABE are also being considered for deployment, as a way of securely and privately sharing and distributing sensor-data information among groups of users in a resource-efficient way.

By implementing these technologies, we expect to not only provide a privacy-aware solution that enables secure access to Smart-City data and services, but to do it in the most efficient and flexible way, accounting for the diversity in devices as well as the distributed nature of the system.

8.2.1.1 Relation to Use Cases

In order to address the above security and privacy objectives the demonstrator set-up of Murcia Municipality will take care to implement and deploy some of the use cases described in the previous sections, in particular:

- SMC-UC1 - Register Data Consumer and manage services

This use case represents the starting point of the data-sharing with citizens and third parties, and is one of the key points to latter support GDPR compliance, defining the way in which identification of users is going to take place, as well as authorization of user's personal information to institutional and third-party services;

- SMC-UC2 - Discover and Consume City Data

  Registered users will be able to secure and privately consume and discover city-data in a number of ways, which are further defined in this use case. With it, the Municipality of Murcia gives access to citizens and third-party services to the different data-sets available in the smart city catalogue, ensuring privacy and security by using different data-distribution and access control mechanisms;

- SMC-UC3 - Personal Data Sharing

  Personal data sharing is also applied in this demonstrator set-up. Citizens are capable of managing their preferences regarding private data sharing with third party and institutional services. Not only can they decide who/which can access their data, they can also later manage those permissions and keep track of how their data is being used.

8.2.1.2 Relation to WP3 Assets

The demonstrator will integrate open source tools and components for identity management and privacy preserving. In particular, the following assets will be integrated in the demonstrator during the first phase of the development, to support the above selected use cases and related requirements identified in D5.1 [1] and mapped during WP3 activities (D3.1 - Common Framework Handbook [3]):

- **Self-Sovereign Privacy-Preserving Identity Management:** This asset will investigate, integrate and adapt privacy-preserving solutions like Anonymous Credentials Systems (e.g. Idemix) in blockchains (e.g. Hyperledger), following a Self-sovereign identity management approach. To this aim, it is envisaged to use, as baseline, the outcomes from the Decentralized identity Foundation (DIF). The assets will be aligned with "Verifiable Credentials" and "Decentralized Identifiers" (DIDs) standards from W3C;
- **Privacy Preserving Middleware:** The IoT middleware platform should aim to (semi-)automatically combine different privacy-preserving techniques to support end-to-end privacy. The middleware platform must also help the user to manage and monetize its data, behaving as a data broker with the existing data consumers. This task aims to design and build the middleware framework;
- **GDPR-based Access Control:** also called GENERAL_D - (Gdpr ENforcEment of peRsonAL Data) is an asset for supporting the integrated GDPR-based process development life cycle for the specification, deployment and testing of adequate fine-grained authorization mechanisms able to consider legal requirements. GENERAL_D provides different features for: specifying the privacy requirements, controlling personal data, processing them, and demonstrating the compliance with the GDPR in collecting, using, storing, disclosing and/or disposing of the data.

8.2.1.3 Description and Workflow

The demonstrator of the city of Murcia will be based on the foundation of the current FIWARE platform, that already gathers an assortment of data from different sensors and providers. On top of the existing platform, an SS-PPIdM system will be deployed, allowing for users and services to register onto the system, establishing their preferences regarding the usage of their personal and private data as part of the identification process. This will allow to generate "zero-knowledge proofs" of possession of credentials and also the selective disclosure of attributes chosen by the user to be revealed.

Those "zero-knowledge proofs" with specific user-attributes selected for disclosure, will be used by the next tool to be deployed: the XACML-based Access-Control Enforcement System (see Figure 127), allowing or denying access to the Smart-City platform's data, based on the former proofs and the set of policies.

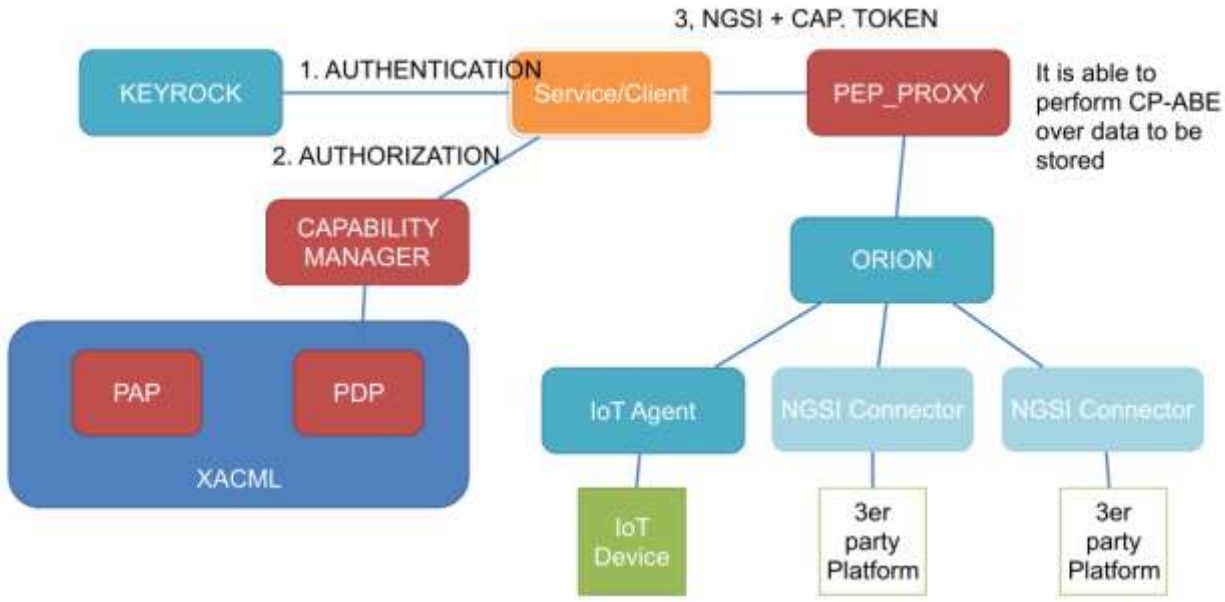

Figure 127: Smart Cities - Secure data-access infrastructure

With those tools in place, users will be able to register to the platform, providing the credentials in their possession that will later allow them access to different sets of information on the Smart-City platform. Users will also be able to manage during the registration, as well as later in time, their preferences regarding specific private information disclosure for identification on different services of the Smart-City, on a service-by-service basis, allowing or denying access to attributes associated to their user profile.

In particular, by using the GDPR-based Access Control asset, and in case of the processing of personal data, for each user it will be generated a set of XACML policies, each compliant with a specific GDPR article so as to be compliant by-design with the regulation. However, before deploying those policies, a testing phase will be conducted through state-of-the-art XACML testing facilities so as to highlight possible inconsistencies of the developed policies with respect to the predefined access control requirements and the GDPR's demands.

Registered users will later be able to discover and consume Smart-City information by accessing the different NGSI-API service points offered by the Smart-City project. In order to be granted access to the information and services requested, by following the DCapBAC model they will need to provide a "capability token" akin to a key that takes them through the security gate to operate with a resource. In order to obtain that token, the user will need to provide the "zero-knowledge proof" to the Capability Manager which in turn, based on the XACML policies set on the system, will issue a verdict regarding the clearance status of the user's request, and a corresponding "capability-token" for it (off course only in the case the user's request is deemed clear).

8.2.1.4 Target Group

The main prospect user groups of the system are businesses (SMEs, service providers), organizations (universities, city officials) and individuals (regular citizens). The interaction with the system will be via web applications in the case of the registration and management of personal data and private information disclosure preferences, as well as web services in the case of discovery and consumption of Smart City data.

8.2.2 City of Porto

Porto currently has a laboratory testbed that combines diverse physical sensors and multiple computing devices with heterogenous resource capabilities. Its purpose is to map a wide range of application scenarios and use cases, including video and audio surveillance, 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, Porto is also focused on device provisioning and privacy preserving middleware, including data storage and computation. We are currently designing an architecture for integrating the different devices with the FIWARE platform for studying additional security and privacy concerns created by these eco-systems.

Focusing on device provisioning, in IoT contexts 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. Currently, most systems base their identity and authentication through the use of Public Key Infrastructure (PKI), depending on a centralized Certification Authority (CA). However, if the CA becomes compromised the entire system is compromised as well. Also, PKI-based solutions are still unable to provide security by default, as systems rely on user-provided security through manual device provisioning configurations. On this regard, many security and privacy issues are caused by human configuration errors. To prevent these errors from occurring we need systems with better user interfaces and better tools to help with the provision of new devices.

Focusing on privacy preserving middleware, preserving privacy of users is a key requirement for every system as imposed by privacy protecting policies such as GDPR. However, most sensorial data increases access to sensitive information that when processed can directly jeopardize the privacy of individuals and violate data protection laws. Data anonymization techniques and multiparty computation are some of the mechanisms currently used for allowing computations on data while preserving individual and citizen privacy.

In this demonstrator, Porto will study how current data anonymization and privacy preserving techniques perform for achieving individual and citizen privacy.

8.2.2.1 Relation to Use Cases

In order to address the described objectives, the demonstrator set-up of Porto will take care to implement and put on operation some of the use cases described in the previous sections, in particular:

1. SMC-UC3 - Personal Data Sharing: The inclusion of this use case will support the 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 portal);
2. SMC-UC4 - Sensor Data sharing and processing: The inclusion of this use case will support data privacy techniques in compliance with the new GDPR and at the same time provide in a tool for stakeholders to have more control on privacy preserving mechanisms and their compliance and performance in regard to the implementation of privacy policies.

8.2.2.2 Relation to WP3 Assets

The demonstrator will integrate open source tools and components for data anonymization and privacy preserving. In particular, the following assets will be integrated in the demonstrator during the first phase of the development, to support the above selected use cases and related requirements identified in D5.1 [1] and mapped during WP3 activities (D3.1 - Common Framework Handbook [3]):

1. Privacy Preserving Middleware - The IoT middleware platform should aim to (semi-)automatically combine different privacy- preserving techniques to support end-to-end privacy. The middleware platform must also help the user to manage and monetize its data, behaving as a data broker with the existing data consumers. This task aims to design and build the middleware framework;
2. Argus, Enforcing Privacy and Security in Public Cloud Storage - Privacy brokerage system aiming to enhance confidentiality and availability by partitioning encrypted data over multiple public Cloud providers;
3. DANS (Data ANonymization Service) - DANS is an anonymization service based on the data anonymization Java tool (ARX) that provides different privacy models (e.g., the k-anonymity model) to enable the application of certain privacy criteria over a specific dataset.

8.2.2.3 Description and Workflow

The following describes how each use case will be implemented in the demonstrator and how each identified asset will be adopted:

1. SMC-UC3 - For this use case, we will start by focusing on smart-home scenarios and develop tools and mechanisms that will allows users to improve their perception on the type of and amount of data that they unknowingly share. Next will focus on analysing the processes of collection and conservation user privacy consents and how these can be applied in different contexts. Finally, by implementing a consent-based approach for users to decide what data they want to share and the conditions in which they want to do it;
2. SMC-UC4 - For this use case, we will start by studying how existing tools and mechanisms implement GDPR compliant systems and how current data anonymization approaches perform in real world scenarios. Next, we will study how anonymization mechanisms, such as DANS, can be used in data sharing systems and how these mechanisms perform when added to existing (legacy) systems. Finally, we will implement a privacy by design solution data sharing solution that independently of the collected data and the computations applied to that data will be able to share data without compromising user and citizen privacy.

8.2.2.4 Target Group

The main prospect user groups of the system are individuals (regular citizens) and service providers. The interaction with the system will mainly with the systems and public services identified in the demonstrator scenario and related workflow.

8.2.3 City of Genova

The Genoese municipality 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 the security aspects, adopted mechanisms should help in assessing the actual security level, preventing data leaks and unauthorized access to internal systems. 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.

Obviously, as a public administration, the Municipality of Genoa includes a large number of services that are offered its citizens, sharing the same requirements and necessities. Therefore, it is reasonable that the

aforementioned activities should be executed by following a scalable approach, i.e. in a way that guarantees the highest number of services to benefit of the security improvements.

The goal of our demonstrator is to improve those systems and processes (of the Municipality) that handle, manage and protect citizen data. To this aim, we assess the current security level of our infrastructure, we improve the technical skills of data officers and managers and we centralize the management of privacy consents and data processing records.

8.2.3.1 Relation to Use Cases

In order to address the security and privacy objectives described before, the demonstrator set-up of Genova Municipality will focus on implementing and putting on operation some of the use cases described in the previous sections, in particular:

- SMC-UC3 - Personal Data Sharing.

  The implementation of the security mechanisms of this use case will provide the municipality with a user centric management of citizen personal data in compliance with the new GDPR. At the same time, it will allow the municipality to offer (to its citizens) a set of tools for tracking the given consents and monitoring the usage of their data (through a so-called self-service transparency portal);

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

  As presented in various technical reports, social engineering is one of the most used strategies that are employed by attackers to gather sensitive/personal and work-related information from users and employees. Executing the activities referring to this UC, Genova Municipality can assess the exposure level to this type of attack and measure the awareness level of its employees. Moreover, the extension (or the integration) of the aforementioned activities with the municipality awareness plan program, would increase the positive impact of the employed tools in the overall security of the municipality itself, since it would help not only in improving the exposure to the attack but also in enhancing the skill of employees to identify phishing emails;

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

  This use case can support Genova Municipality to identify cyber risks related to critical digital services. It also gives a simple way for SMEs to understand their cyber-domain and get informed of most common cybersecurity mitigation solutions;

- SMC-UC7 - Cybesecurity needs and solution elicitation and selection. This use case will be evaluated for the adoption in the second phase of demonstrator setup to support the identification of potential solutions to the needs emerged from assessment activities.

8.2.3.2 Relation to WP3 Assets

The demonstrator will integrate open source tools and components for security risk assessment and privacy preserving. In particular, the following assets will be integrated in the demonstrator during the first phase of the development, to support the above selected use cases and related requirements identified in D5.1 [1] and mapped during WP3 activities (D3.1 - Common Framework Handbook [3]):

1. **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[44] principles to exploit the potential of personal data, facilitates its control and new business opportunities in compliance with the GDPR;

2. **RATING**. The tool aims to support organizations to assess evidence-based cyber-risk profiles. Following ISO31000, RATING is supports Organizations to identify major cybersecurity risks for their business and main assets. Using this asset, Service Providers can conduct an entire cyber risk assessment, based on holistic approaches, involving both Financial and Cybersecurity boards to understand the relationships between cyber-attacks and intangible capital at risk;
3. **TO4SEE**. It aims at measuring the susceptibility of the employees against Social Engineering attacks based on simulating a phishing campaign. Such tool can perform a real phishing attack regulated by several security and privacy by design principles. According to privacy regulations policies, the results of the assessment are aggregated and anonymized, so that it is possible for CISO to get informed of the most critical "target-groups" prone to human-based vulnerabilities.

8.2.3.3 Description and Workflow

SMC-UC3 - CaPe

For this use case, we firstly analysed the processes of collection and conservation of privacy consensus. As previously mentioned, the Municipality offers multiple services to the citizens, sharing the need of compliance with the same requirements – as collecting user consensus before actually providing the service.

The analysis highlighted a non-homogeneous adoption of mechanisms for handling the privacy consensus. In other words, each of the offered services implemented a mechanism that was not necessarily similar to the mechanisms of another service. This fact, besides providing a not homogeneous user experience, causes multiple issues. Firstly, it is not guaranteed that each of the implemented mechanisms provide the same level of security (in terms, for instance, of resistance to attacks or data leakage). Secondly, it is difficult to have an overview of the privacy consents that a citizen accepted.

The Municipality of Genoa decided to adopt the CaPe platform as a central mechanism for managing privacy consensus. This means that CaPe will be integrated in the global IT architecture (Figure 128), becoming a fundamental service to be employed by any service requiring the user to provide a privacy consent. Moreover, the role of CaPe in the whole architecture would consent – both to users and back office operators – to obtain an overview of the given consent forms for every service

[44] https://mydata.org/

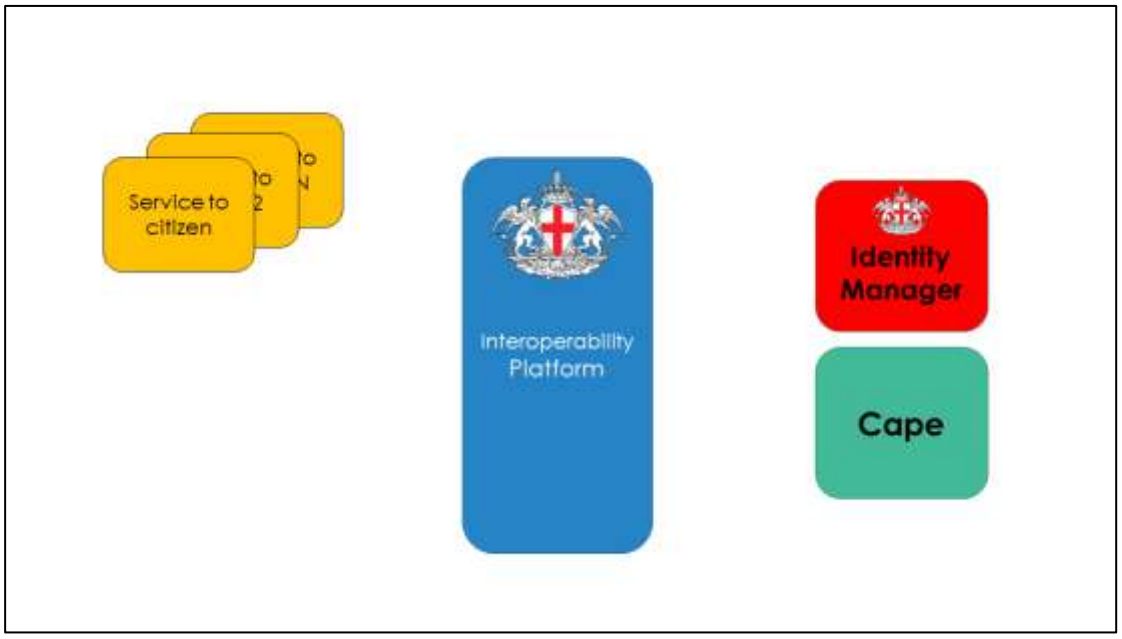

Figure 128: Smart Cities - CaPe in the Municipality architecture

More in detail, CaPe will be connected to the interoperability platform (WSO2), to be reached via API that will be made available to any service. Each service will have to undergo a setup phase, in which the consent form should be loaded in CaPe (Figure 129).

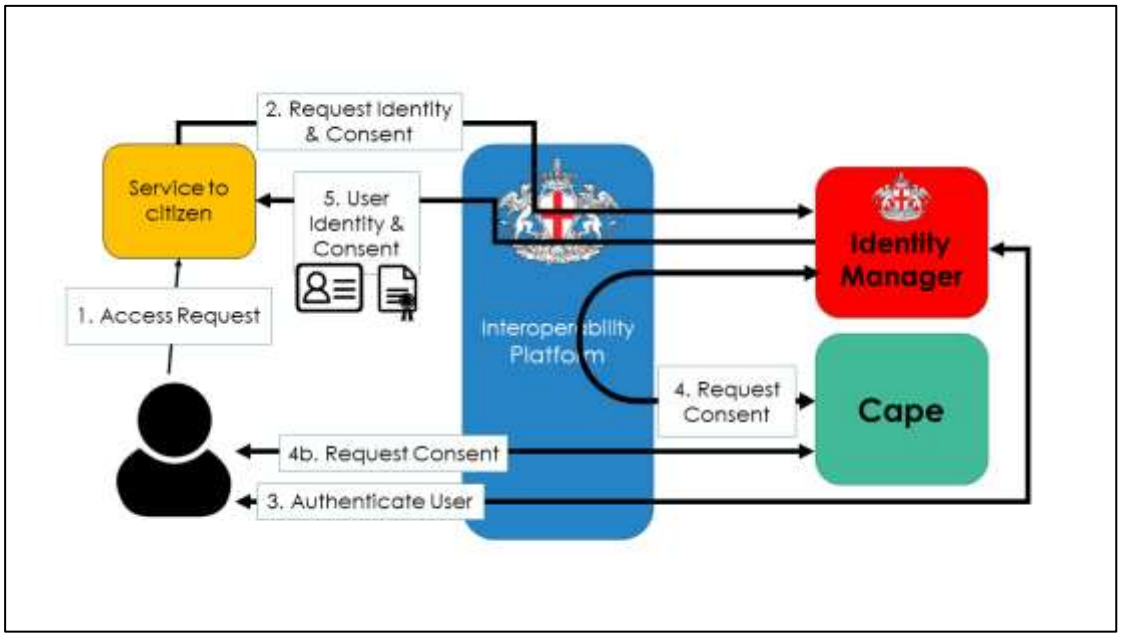

Figure 129: Smart Cities - Usage of CaPe

After that, a typical use case is the one in which 1) the user wants to access the service, 2) the service redirects to the authentication platform (SIRAC), 3) the authentication platform identifies the user and redirects her to CaPe, 4) Cape shows the consent form and collects the answer, 5) the user is redirected to the service, being able to use it.

SMC-UC5 – TO4SEE

The municipality employs several clerks, operators and officers in various services that handle user data. Therefore, besides improving the security level provided by the security mechanisms in place, the education of users in terms of cybersecurity has to be considered.

In order to test and improve the skills of its employees, the Municipality decided to adopt TO4SEE. In particular, such tool would be integrated in the educational program adopted so far. Indeed, the adoption of such a mechanism would allow for increasing the awareness of the employees, preventing data leaks and identity thefts that can cause loss of personal data.

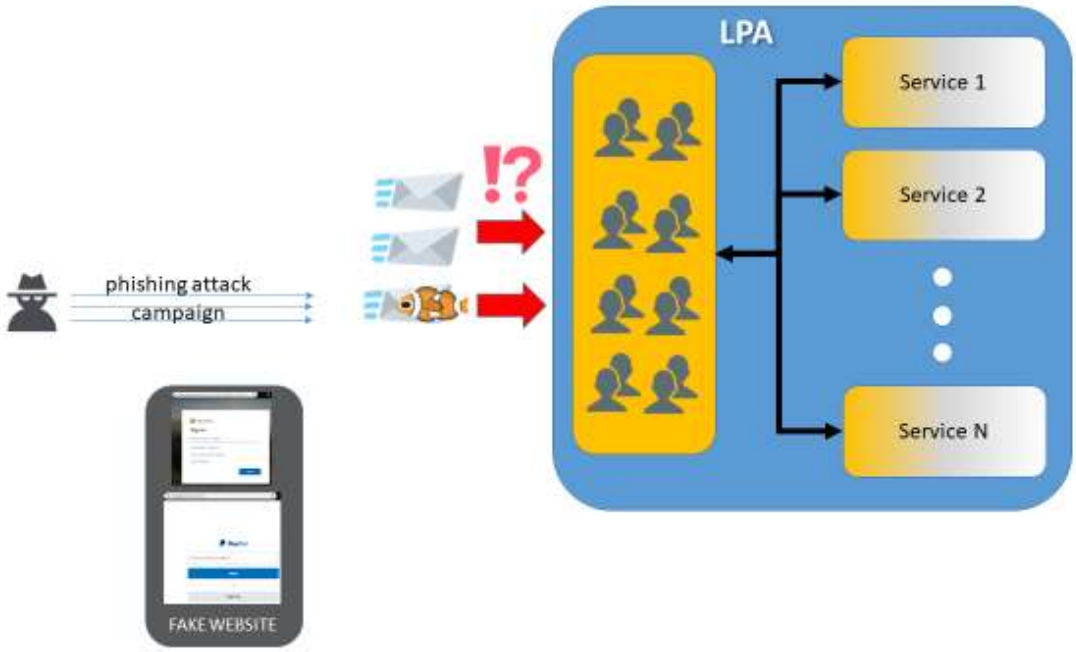

Figure 130: Smart Cities - LPA phishing campaign attack - phase 1

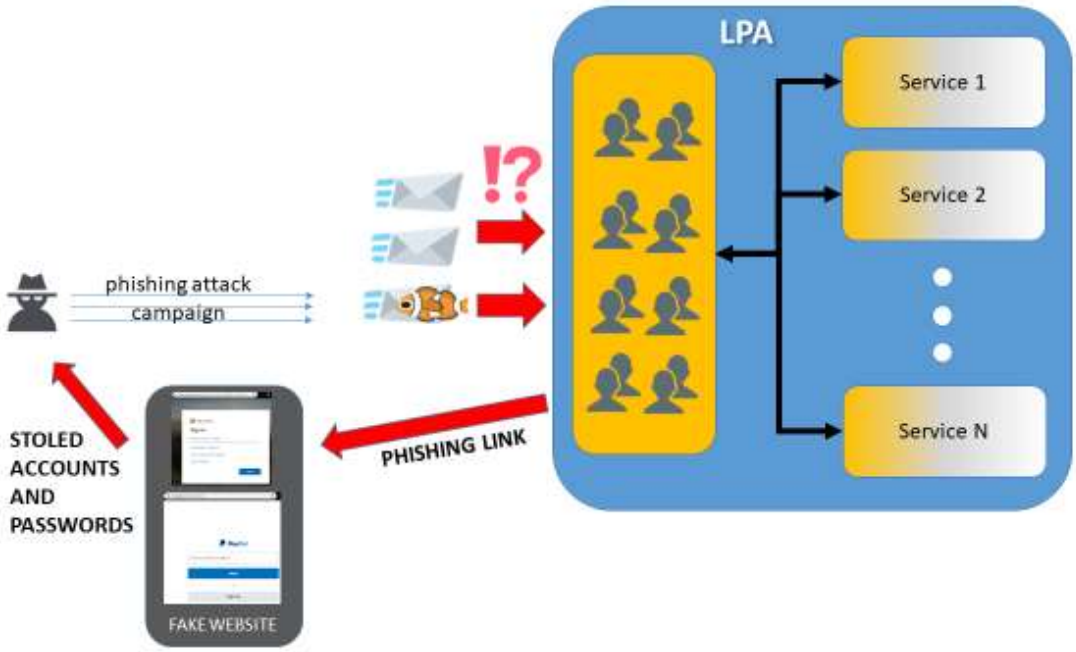

Figure 131: Smart Cities - LPA phishing campaign attack - phase 2

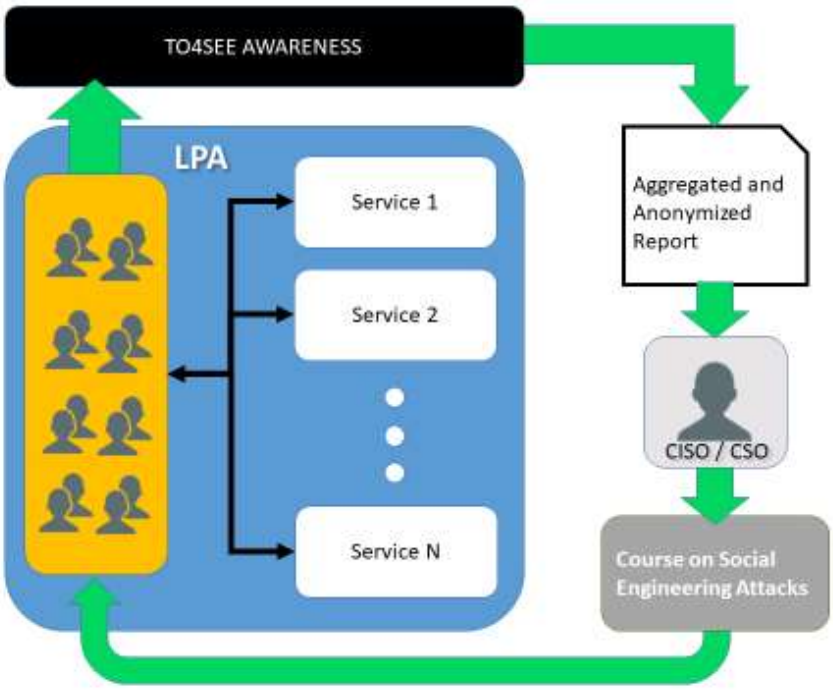

Figure 132: Smart Cities - LPA TO4SEE Awareness and mitigation

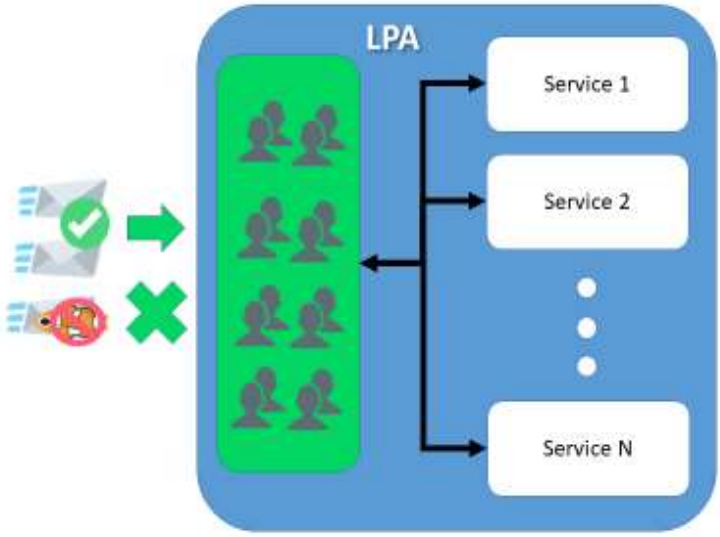

Figure 133: Smart Cities - LPA Phishing Recognition

Among the expected benefits, the employment of TO4SEE will allow to perform a preliminary evaluation of the security risks related to user skills and behaviour w.r.t social engineering attacks (e.g. Phishing). Moreover, for what concerns the educational aspects, TO4SEE will allow to plan and organize more specific courses for improve the user knowledge on security risks related to Social Engineering.

SMC-UC6 - RATING

RATING will be employed for assessing the current cyber posture and security level provided by the mechanisms that are currently in place (Figure 135).

In particular, RATING allows for evaluating (Figure 136) the potential losses following a cyber-attack, in terms of both economic and image impacts. Furthermore, the employment of RATING is expected to highlight a series of usually underestimated issues and challenges, both in the economic aspects of the municipality (EBITDA) and economic impacts following a cyber-attack (Figure 137).

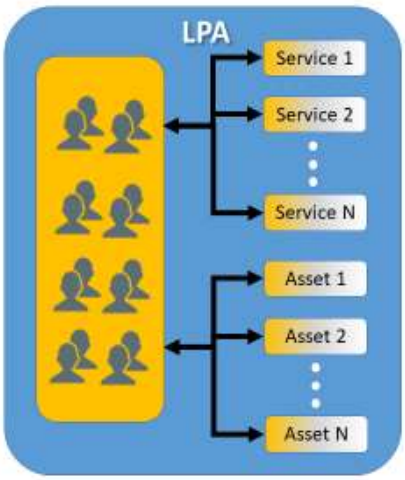

Figure 134: Smart Cities - LPA clerks, services and assets

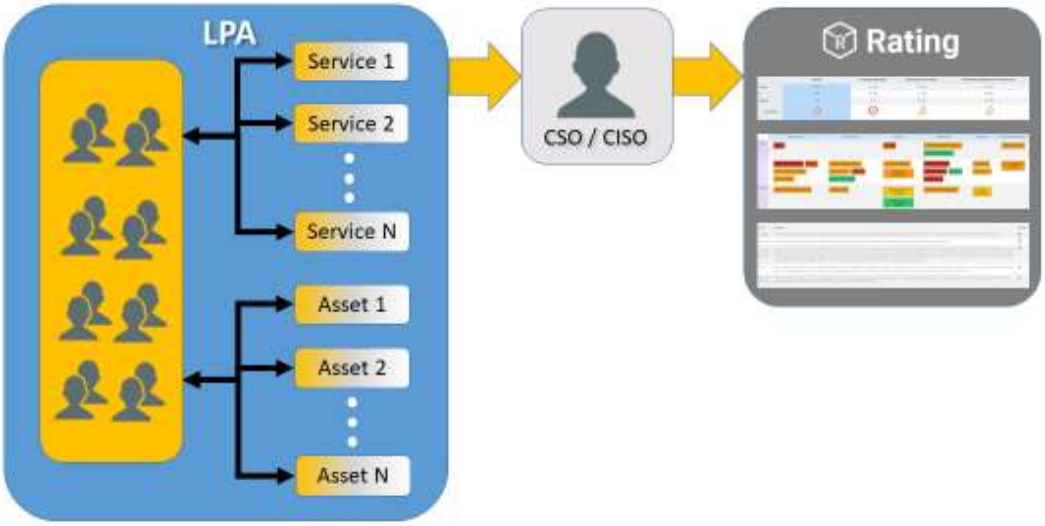

Figure 135: Smart Cities - LPA clerks, services and assets evaluated

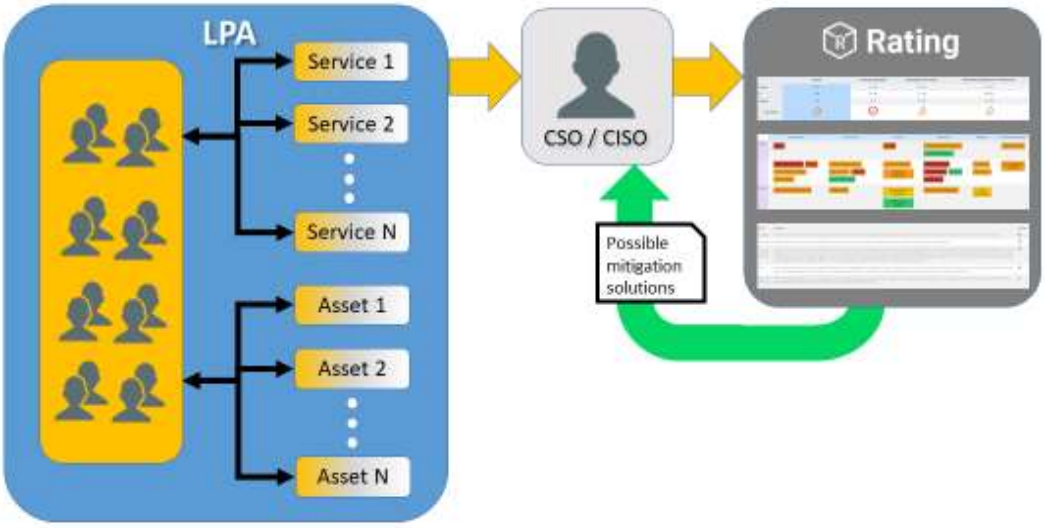

Figure 136: Smart Cities - RATING reports and possible mitigation solutions

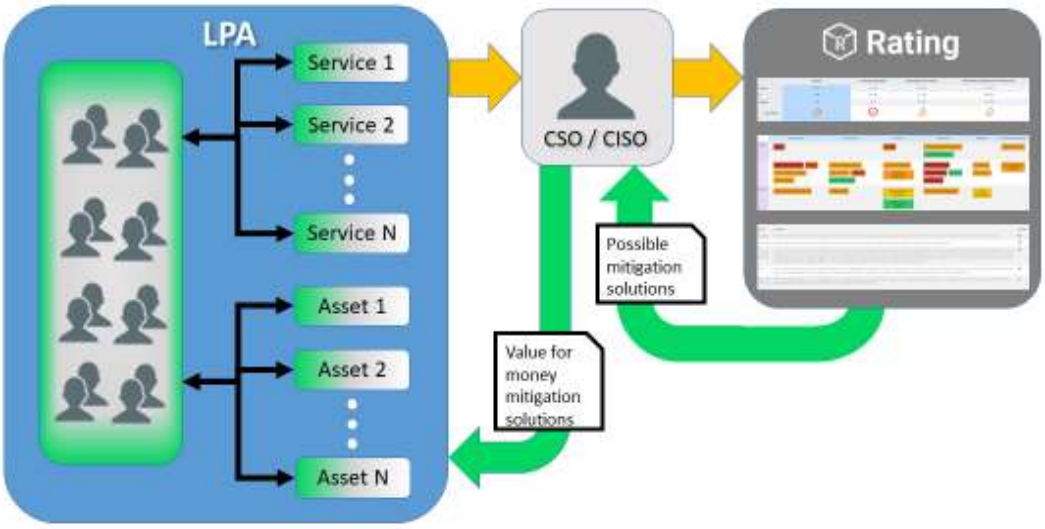

Figure 137: Smart Cities - LPA adopted mitigation solutions

For what concerns the workflow, the Municipality plans to use RATING before and after the adoption of the tools for SMC-UC3 and SMC-UC6, for monitoring and evaluating the improvements (in terms of security) given by other use cases.

8.2.3.4 Target Group

The main prospect user groups of the system are individuals (regular citizens) and Public organization (clerks, operators and officers). The interaction with the system will mainly with the systems and public services identified in the demonstrator scenario and related workflow.

9 Conclusions

We presented deliverable [18] [19]D5.2, titled “Specification and Set-up of Demonstration Cases Phase 1”. We continued the discussion started in D5.1 [1] by further defining the seven demonstrators – also known as “demonstrators”. Namely, this document provided a detailed specification of the demonstrator’s use cases, featuring preconditions, workflows, and postconditions for each, thus giving an engineering overview that complements the high-level concepts laid out in D5.1. Furthermore, it described how the use cases come together to form the demonstrators. Use cases model a part or a specific functionality of their demonstrator. The exact mechanisms of interaction are still under discussion and will be defined better during the second cycle of the project.

We gave a first description of the demonstrators’ user interface functionalities. They are, however, still in their early stages, therefore we invite the reader to acknowledge the possibility that one or several functionalities may change as the project advances. We will report these changes (if any) in future deliverables.

Finally, we highlighted the relationship between the demonstrators and WP3’s assets, in order to facilitate, promote, and strengthen the collaboration between the two work packages.

10 Bibliography

[1] A. Sforzin, “CyberSec4Europe D5.1: Requirements Analysis of Demonstration Cases Phase 1,” European Commission, 2019.

[2] E. Markatos, "CyberSec4Europe D4.3: Research and Development Roadmap 1," European Commission, 2020.

[3] A. Skarmeta, “CyberSec4Europe D3.1: Common Framework Handbook 1,” European Commission, 2019.

[4] S. Krenn, “CyberSec4Europe D3.2: Cross Sectoral Cybersecurity Building Blocks,” European Commission, 2020.

[5] D. Preuveneers, “CyberSec4Europe D3.3: Research challenges and requirements to manage digital evidence,” European Commission, 2020.

[6] L. Pasquale, “CyberSec4Europe D3.4: Analysis of key research challenges for adaptive security,” European Commission, 2020.

[7] K. Halunen, “CyberSec4Europe D3.5: Usable security & privacy methods and recommendations,” European Commission, 2020.

[8] B. Crispo, “CyberSec4Europe D3.7: Usability Requirements Validation,” European Commission, 2020.

[9] European Union, “Directive 2006/42 ec of the european parliament and of the council of 17 may 2006 on machinery, and amending directive 95/16/ec (recast).,” *In Official Journal of the European Union,* vol. 9.6.2006, pp. 24-86, 2006.

[10] NIST, “Framework for improving critical infrastructure cybersecurity,” NIST, 2018.

[11] E. Conway, N. Luu and E. Shaffer, “Best practices in cyber supply chain risk management - cisco managing supply chain risks end-to-end,” NIST, 2015.

[12] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski and J. McCarthy, “Cybersecurity framework manufacturing profile nistir 8183,” NIST, 2019.

[13] P. Kasinathan and J. Cuellar, “Securing Emergent IoT Applications,” in *Engineering Trustworthy Software Systems: 4th International School, SETSS 2018, Chongqing, China, April 7--12, 2018, Tutorial Lectures*, Springer International Publishing, 2019, pp. 99--147.

[14] P. Kasinathan and J. Cuellar, “Workflow-aware security of integrated mobility services,” in *In Computer Security - 23rd European Symposium on Research in Computer Security, ESORICS 2018*, Barcelona, Spain, 2018.

[15] N. Zupan, P. Kasinathan, J. Cuellar and M. Sauer, “Secure Smart Contract Generation Based on Petri Nets,” in *Blockchain Technology for Industry 4.0*, Singapore, Springer, 2019, pp. 73-98.

[16] C. Frøystad, K. Bernsmed and P. H. Meland, “Protecting Future Maritime Communication,” in *In Proceedings of The 12th International Conference on Availability, Reliability and Security (ARES'17)*, Reggio Calabria, Italy, 2001.

[17] K. Bernsmed, G. Bour and R. Borgaonkar, “D4.1 PKI Prototype Specification.,” CySiMS Service Evolution project deliverable (to be published), 2020.

[18] P. Kasinathan and J. Cuellar, “Securing Emergent IoT Applications,” in *Engineering Trustworthy Software Systems: 4th International School, SETSS 2018, April 7--12, 2018, Tutorial Lectures*, Chongqing, China, Springer International Publishing, 2019, pp. 99--147.

[19] A. r. b. t. U. g. c. s. adviser, “Distributed Ledger Technology: Beyond Blockchain,” UK Government Office of Science, United Kingdom, 2016.