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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D3.17

Integration to demonstration cases

Document Identification	
Due date	31 January 2022
Submission date	31 January 2022
Revision	1.0

Related WP	WP3	Dissemination Level	CO
Lead Participant	UPS-IRIT	Lead Author	Célia Martinie (UPS-IRIT)
Contributing Beneficiaries	CNR, KAU, KUL, UM, UMU,UPS-IRIT, VTT	Related Deliverables	D3.5, D3.7, D3.10, D3.16

Abstract: This document presents the deliverable "D3.17 – Integration to demonstration cases". WP3 provides the common research support for the different WPs, and, in particular, coordinates with WP5 to apply the research outputs to the WP5 demonstration cases. Within WP3, the main objective of Task 3.6 is to provide recommendations and guidelines on how to ensure the usability of security and privacy policies. Whereas the previous deliverables focus on the generic research results on usable, human-centred cyber security, the D3.17 deliverable focuses on the concrete integration of the T3.6 with WP5 demonstration cases. This document describes the integration of the WP3 T3.6 assets with the WP5 demonstration cases. T3.6 assets have been integrated within most of the WP5 demonstration cases, but also with another external demonstration case (Smart Campus). This document presents the main approach undertaken to identify relevant integration opportunities and to implement the integration. This document describes the integration that the T3.6 partners actually carried out within the demonstration cases, as well as the integration of all of the assets which are envisioned in a unified scenario built from the Smart Campus demonstration case.

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

The main goal of the CyberSec4Europe project is to promote collaboration between industrial and academic participants by fostering research and development to identify and analyse cybersecurity challenges in the selected sectors and develop innovative solutions addressing them. This project specifically targets seven application domains: open banking, supply chain, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange, and smart cities. Work Package 5 (WP5) drives the design and development of demonstrators in these seven application domains, and targets to produce prototypes of cybersecurity solutions, products, or services that are secure by design. WP3 is responsible for the definition of common research, development and innovation for the next generation of cybersecurity technologies, applications and services. WP3 provides the common research support for the different WPs, and, in particular, coordinates with WP5 to apply the research outputs to the WP5 demonstration cases.

Within WP3, the main objective of Task 3.6 is to provide recommendations and guidelines on how to ensure the usability of security and privacy policies. The following set of deliverables have been produced previously to reach this objective: “D3.5 Usable Security & Privacy Methods and Recommendations”, “D3.7 Usability Requirements Validation”, and “D3.16 Security Requirements and Risks Conceptualization”. The deliverable D3.17 follows these past deliverables and is the last deliverable of the task T3.6. Whereas the previous deliverables focus on the generic research results on usable, human-centred cyber security, the D3.17 deliverable focuses on the concrete integration of the T3.6 with WP5 demonstration cases.

This deliverable presents how the T3.6 assets have or can be integrated within WP5 demonstration cases, which is one of the project's goals, but also how the assets have been integrated in an external demonstration case, which is the Smart Campus demonstration case. First, the deliverable presents the systematic approach that has been applied to identify possible integration opportunities and to select the most relevant ones. Then, the deliverable describes how the relevant integration opportunities have been implemented or can be implemented with the WP5 and external demonstration case. At last, the deliverable presents a unified scenario to highlight how the T3.6 assets inter-play.

This deliverable highlights the collaborative effort made to integrate the T3.6 assets within WP5 demonstration cases, as well as the collaborative effort made to envision additional possible integrations.

This document is organised into 9 main sections. One section is dedicated to the presentation of the main integration process. Five sections are dedicated to the presentation of the integration of one or several assets with a WP5 demonstration case. One section focuses on an external demonstration case, which has been used to produce a unified scenario for the integration of all of the assets at the same time.

The results of the research work on the integration of the T3.6 assets within WP5 demonstration cases are:

- A set of conclusions on how privacy notifications can enhance usable transparency in the context of privacy and identity management and to what extent the cultural context and other parameters (demographics, usage characteristics, the option for intervenability, and modality of privacy notifications) can have an impact on their perceived usefulness.
- A proposal for the combination of the authentication methods TATIS, AuthGuide, Keycloak and EEVEHAC to protect the MISP incident reporting platform.

- An extension of the MITIGATE maritime risk management method to identify additional threats by including task modelling in the risk assessment process of the method.
- A usable identity management user interface for smartphone users in smart cities.
- A user-centered tool to support the security analysis of smart cities.
- A user-centered template to support IT services to manage the GPDR compliance when collecting user data on a smart campus.
- A proposal for the integration of all of the T3.6 assets within a unified scenario in the context of a smart campus.

Document information

Contributors

Name	Partner
Manuel Cheminod	CNR
Simone Fischer-Hübner	KAU
Davy Preuveneers	KUL
Marko Kompara	UM
Jesús García Rodríguez	UMU
Rafael Torres Moreno	UMU
Célia Martinie	UPS-IRIT
Outi-Marja Latvala	VTT

Reviewers

Name	Partner
Sunil Chaudhary	NTNU
Stephan Krenn	AIT

History

Version	Date	Authors	Comment
0.01	2019-03-28	Célia Martinie (UPS-IRIT)	1st draft, structure proposal
0.02	2021-03-23	Célia Martinie (UPS-IRIT)	Added possibility to describe an integration with an external demonstration case
0.03	2021-05-19	Célia Martinie (UPS-IRIT)	Added section on integration of all of the assets within a unified scenario
0.04	2021-10-03	Davy Preuveneers (KUL)	Draft breakdown of section 3 on demonstration case 4
0.05	2021-10-05	Outi-Marja Lavatla (VTT)	Content in section 3
0.06	2021-10-22	Jesús García and Rafael Torres (UMU)	Content in section 6
0.07	2021-10-26	Simone Fischer-Hübner (KAU)	Completed section 2
0.08	2021-10-28	Davy Preuveneers (KUL)	Update section 3
0.09	2021-11-10	Célia Martinie (UPS-IRIT)	Completed introduction and section 7
0.91	2021-11-11	Marko Kompara (UM)	Section 6.1
0.1	2021-11-15	Célia Martinie (UPS-IRIT)	Migration to Word, modified main structure, added executive summary
0.11	2021-11-19	Célia Martinie (UPS-IRIT)	Integrated partners' suggestions of modifications, modified executive summary, added a figure in section 8 and conclusion.
0.12	2021-11-30	Simone Fischer-Hübner (KAU), Davy Preuveneers (KUL), Célia Martinie (UPS-IRIT), Jesús García (UMU), Manuel Cheminod (CNR), Marko Kompara (UM)	Added sections state of the art and beyond state of the art. Completed executive summary with research results
0.13	2022-01-05	Célia Martinie (UPS-IRIT)	Integrated proposal for modifications from internal reviewers (Sunil Chaudhary and Stephan Krenn)
0.14	2022-01-06	Marko Kompara (UM), Célia Martinie (UPS-IRIT), Davy Preuveneers (KUL)	Corrected Table 1, Section 3 and Figure 14.
0.15	2022-01-14	Célia Martinie (UPS-IRIT)	Corrected date on front page.
1.0	2022-01-31	Célia Martinie (UPS-IRIT)	Corrected formatting issues.
1.0	2022-01-31	Ahad Niknia (GUF)	Final check, preparation and submisiion

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**API**	Application Programming Interface
C	**CNR**	Consiglio Nazionale Delle Ricerche, Italy
D	**DC**	Demonstration Case
	DDoS	Distributed Denial of Service
	DPIA	Data Protection Impact Assessment
E	**EEVEHAC**	End-to-end Visualizable Encrypted and Human Authenticated Channel
G	**GDPR**	General Data Protection Regulation
H	**HAKE**	Human Authenticated Key Exchange Protocol
	HAMSTERS	Human-centered Assessment and Modelling to Support Task Engineering for Resilient Systems
I	**IAM**	Identity and Access Management
	IdM	Identity Management
	IdP	Identity Provider
	IoT	Internet of Things
	ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
K	**KAU**	Karlstads Universitet, Sweden
	KUL	Katholieke Universitet Leuven, Belgium
M	**MFA**	Multi-factor Authentication
P	**p-ABC**	privacy attribute-based credentials
	PIN	Personal Identification Number
	pp-IdM	privacy-preserving Identity Management
S	**SMT**	Satisfiability Modulo Theories
	SSI	Self-Sovereign Identity
U	**UX/UI**	User Experience / User Interface
	UM	Univerza V Mariboru, Slovenia
	UMU	Universidad de Murcia, Spain
	UPS-IRIT	Université Paul Sabatier Toulouse III
V	**VTT**	Teknologian tutkimuskeskus VTT Oy, Finland

1 Introduction

The research activities led in T3.6 focused on the usability of security and privacy policies. Several assets have been used and developed to go beyond the state of the art on the research topics covered by this theme. Some of these assets have been validated using case studies that are different from the WP5 demonstration cases. However, they have or can be applied to WP5 demonstration cases. This deliverable presents how the T3.6 assets have been integrated or may integrate with WP5 demonstration cases. This deliverable also presents the implementation of a T3.6 asset within an external demonstration case, the Smart Campus demonstration case. The external demonstration case Smart Campus provided foundations to build a unified scenario that includes all the T3.6 assets and that highlights how they interplay.

1.1 Motivation

This deliverable is the last one of the set of deliverables produced during the activities of Task T3.6. It follows three previous deliverables produced in this task: “D3.5 Usable Security & Privacy Methods and Recommendations”, “D3.7 Usability Requirements Validation”, and “D3.16 Security Requirements and Risks Conceptualization”. Whereas the previous deliverables focus on the generic research results on usable, human-centred cyber security and especially on three themes (data privacy and protection, eliciting and fulfilling security requirements and enhancing the human understanding of security solutions), the D3.17 deliverable focuses on the concrete integration of the T3.6 with WP5 demonstration cases. The T3.6 assets enable to support the usability of security and privacy policies. Their integration with WP5 demonstration cases is manifold. First, it shows that T3.6 assets have or can be adopted in the demonstration cases, which is one of the project's goals. Then, it allows us to highlight the collaborative effort made to integrate them and to envision additional possible integration. It also enables us to show their added value to the demonstration cases. Lastly, it provides an additional opportunity to validate the assets, using other case studies and application domains different from the ones with which the assets were originally validated.

1.2 Document Structure

This document is organised as follows. Section 2 presents the main integration process that we followed. Sections 3, 4, 5, 6 and 7 are dedicated to a WP5 demonstration case, and describe which asset(s) have been integrated as well as, the goal and scope of the integration, the part of the demonstration case involved in the integration (most of the demonstration cases have several use cases and the assets are not straightforwardly integrated to all of the DC use cases), a short description of the involved asset(s), and the description of the integration with the involved demonstration case. Section 6 does not have the same structure and does not present the details of the integration with DC6 because this integration possibility, although relevant and planned, has not been yet performed. Section 8 presents the integration of the asset Guidelines for GPDR Compliant User Experience with the Smart Campus demonstration case, as well as a conceptual view on how all of the T3.6 assets integrate together in a Smart Campus unified scenario.

Each section highlights the following points:

- the main research goals and challenges related to the integration, and
- how the integration goes beyond the state of the art.

2 The approach for integrating T3.6 assets with WP5 demonstration cases

2.1 Overview of the approach

Our approach consisted of three main steps, presented in Figure 1. First, we collected information about the T3.6 assets. For that purpose, each partner produced a set of slides containing a presentation of the key concepts and features of its asset(s). These presentations were meant to provide an overview of all of the T3.6 assets to all the T3.6 partners as well as to the WP5 partners. The second step was to analyse the demonstration cases in the light of the main characteristics of the assets, this to identify possible relevant opportunities for integration. The last step was to select a subset of the integration possibilities by identifying the most relevant ones amongst the identified opportunities. The main criteria for selection were: the adequacy of the features of the asset with the main research problems addressed in the demonstration case, the possible mapping between the asset and the demonstration case use(s) case(s), and the adequacy between partner research objectives and the main research problem addressed in the demonstration case. These opportunities have been presented during joint WP3-WP5 meetings.

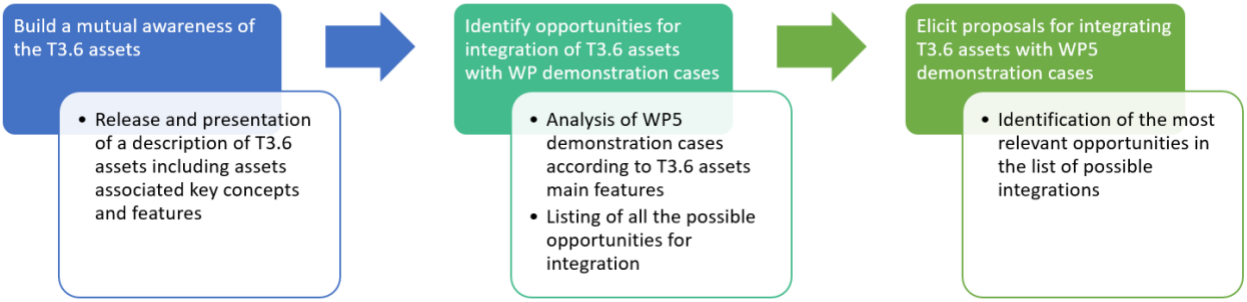


Figure 1. Three steps process applied to identify relevant integration opportunities

In addition to the WP5 demonstration cases, the asset GPDR Compliant User Experience has been integrated into a demonstration case that is not part of WP5: the Smart Campus demonstration case. At last, in order to show the relevance of the integration of all of the T3.6 assets, we built a unified scenario using the Smart Campus demonstration case. We named this scenario the Smart Campus unified scenario. This unified scenario highlights the synergy of the T3.6 assets in addressing usability and user experience of security and privacy policies.

2.2 The main identified relevant opportunities

Table 1 presents these most relevant identified opportunities. The first column presents the T3.6 lead partners in charge of the integration. The second column presents the involved assets. Columns 3 to 10 present the involved demonstration cases:

- DC1 – Open banking deals with potential threats on open banking API. These API are used to connect banks and third-parties to simplify data exchanges between banks and their customers.
- DC2 - Suply Chain Security Assurance deals with security of data exchanges in the manufacturing supply chain.

- DC3 – Privacy Preserving Identity Management is an identity management application that uses anonymous credentials and provides the users with the possibility to selectively reveal part of their personal information.
- DC4 – Incident reporting is an incident reporting system that collects information about security incidents.
- DC5 – Maritime Transport deals with maritime supply chain services which involve several various distributed and inter-connected organizations, infrastructures, and human actors belonging to those organizations and infrastructures.
- DC6 – Medical Data Exchange deals with increasing the trustworthiness between stakeholders when sharing medical data through a marketplace platform thus generating new business opportunities.
- DC7 – Smart cities deals with the setup and deployment of a user-centric sensor-based infrastructure to support personal data exchange.
- External DC – Smart campus deals with interconnected services and applications on a smart campus.

The last column presents the section in the document associated with the integration opportunity, where applicable.

The following presentation rules apply:

- The cells with a green shaded background represent the assets that have been actually integrated at the implementation level or at the conceptual level.
- The cells with a green-shaded background and text displayed in *Italic* represent an integration possibility which has not yet been completed, but is currently under investigation.
- At last, the cells with no green-shaded background represent the integration possibilities that have been abandoned.

Table 1: Summary of the opportunities for integration identified as relevant.

Lead partner	Asset	DC1 – Open banking	DC2 – Suply Chain Security Assurance	DC3 – Privacy Preserving Identity Management	DC4 – Incident reporting	DC5 – Maritime Transport	DC6 – Medical Data Exchange	DC7 – Smart cities	External DC – Smart campus	Associated section in the doc.
CNR	SYSVER					Presentation of simplifies risk analysis results		Presentation of relevant information to admin users		6
KAU	Usable Privacy & Identity Management Guidelines			Design of the privacy notifications				Design of the privacy notifications		3
KUL	TATIS +AuthGuide				Enhanced authentication for threat intelligence sharing					4
UM	Guidelines for GPDR compliant user experience						*Develop Data Protection Impact Assessment*		Develop Data Protection Impact Assessment	7
UMU	Usable SelfSovereign-PPIdM							Usable authen-tication		6
UPS-IRIT	HAMSTERS					Support risk analysis using task models				5
VTT	EEVEHAC	User understandable authentication key exchange	User understandable authentication key exchange		User understandable authenti-cation key exchange					4

3 Integration with Demonstration Case 3

Demonstration case 3 is an identity management application that uses anonymous credentials and provides the users with the possibility to selectively reveal part of their personal information. In particular, DC3 targets university students as a type of user. They receive digital credentials upon completion of their academic degrees, and can selectively reveal parts of this information during the job application process. Such a privacy-preserving identity management system aims to avoid age discrimination for example. Applicants can present the name, type of degree, or issuing university during the first phase of the application, but hide information such as birth date or issuance date of the degrees they own. Such type of identification requires to setup user interactions to make the user aware and understand which personal information may be disclosed.

3.1 Goal and Scope

Privacy notifications are a means for enhancing transparency by providing users with information about the processing of their personal data. Privacy notifications that inform users about the planned data processing and related privacy implications before they disclose personal data (i.e. ex ante) can provide important building blocks for privacy-preserving identity management systems enabling data subjects to make informed decisions. Similarly, more detailed information about the data processing that already took place and privacy implications that arose or could arise from it can be provided via notifications by an ex-post transparency tool as part of a privacy and identity management system.

3.2 Part of demonstration case 3 involved in the integration

The integration possibilities concern all use cases of DC3 where the user is directly involved: course registration (IDM-UC1), degree issuance (IDM-UC2), degree presentation (IDM–UC3), certificate renewal (IDM-UC6), and de-registration (IDM-UC7). For the execution of these use cases, the user may be able to make a partial and selective presentation of their personal information. Moreover, for degree presentation use case, the user may be able to make a partial and selective presentation of their obtained degrees during an application process.

3.3 State of the Art

Related work on ex post privacy notifications, which users receive after having disclosed personal data, are e.g. provided targeting Android app permission settings [1], and the usability of a feedback mechanism for contextual messaging [2]. However, they cover a smaller set of notifications than our work and are not discussed in relation to culture dimensions in privacy and identity management. Wu et al. [3] researched the impact of the design of security notifications on users' perceived security, user acceptance and usability. We extended this work by investigating user preferences for privacy notifications in order to propose design guidelines for privacy notifications to be perceived as meaningful for the users and to facilitate usable transparency.

3.4 Challenge Beyond the State of the Art

Whereas multiple facets of notification preferences had been investigated by us earlier in isolated contexts [4], we now provide a more holistic study of the determinants of privacy notifications including the cultural context and discuss implications for privacy and identity management.

To the best of our knowledge, this is the first study that analyses to what extent users find different types of privacy notifications useful, and to what extent the cultural context and other parameters (demographics, usage characteristics, the option for intervenability, and modality of privacy notifications) can have an impact on this, and how privacy notifications can enhance usable transparency in the context of privacy and identity management.

3.5 Description of the integrated asset Usable Privacy and Identity Management Guidelines

Our guidelines for user-centred privacy notifications that we provided for the mHealth and fitness tracking context have been published in [5]. While they were kept on a generally high level and we can assume that they will also be valid in general, further follow-up research needs to be done for refining them to the DC3 use cases.

3.6 Description of integration with DC3

Privacy notifications can help users of DC3 to make informed choices about selective disclosures, e.g. about potential consequences of hiding or showing different attributes. Moreover, users of DC3 could also be notified ex post about privacy breaches or receive tips on how they can better protect or secure their data.

Moreover, DC3 could in future be extended with an interveneability functionality for users to pseudonymously exercise their data subject rights. For this, a user should first be authenticated as the "owner" of a pseudonym under that the user disclosed data, and thus as the respective data subject, via a zero-knowledge proof, before the user can exercise his/her data subject rights. Ex post privacy notifications may then also guide the users about how they can "intervene", e.g. by pseudonymously requesting the correction or deletion of their data.

Preference of the type (breach notifications, notifications about privacy consequences and notifications providing privacy tips) and modalities of privacy notifications may however differ very much among individuals and may be dependent on their cultural background, gender, or other personal attributes.

Particularly, a recent Eurobarometer survey [6] showed that citizens from different EU countries feel to different degrees in control and well or badly informed about conditions of collection and further use of their data on the Internet. Moreover, they have different practices in terms of reading privacy notices.

In a research study presented in [5], we analysed to what extent users find different types of privacy notifications useful. Moreover, we analysed to what extent the cultural context and other demographics, the option for intervenability, as well as the type, timing, and modality of privacy notifications serve as determinants that help predict suitable notification settings for users.

The context of our research was mhealth services and the cultural comparison of English and German speaking user groups. However, we assume that our study also allows to derive more general conclusions.

Our findings showed that UK users were less concerned and found privacy notifications less useful than German-speaking users which can be explained by Hofstede's cultural comparison findings [7] [8] showing that the UK has a low score on uncertainty avoidance, while German-speaking countries are uncertainty avoidance cultures. Thus, UK citizens are higher risk-takers who feel more confident with ambiguity and thus are less interested in transparency and control. In contrast, German-speaking countries are cultures that feel more uncomfortable due to ambiguous or unknown situations, and may therefore perceive privacy notifications providing awareness and guidance as more useful. This is also in line with the findings by Trepte et al. [9], which show that users from uncertainty avoidance countries specifically desire to avoid privacy risks. UK users on the other hand preferred more diverse signalling modalities (emails, pop-ups, and system notifications) than German speaking users. This suggests that cultural context might serve as a determinant of notification settings.

From our study, we can conclude that privacy notification should consider cultural variations of preferences. Culture-specific notification preference profiles that users could choose or that are enabled by default should further be considered, which also allow fine-grained customisation, for both ex ante and ex post privacy notifications. This means that in addition to transparency information that need to be provided pursuant to the GDPR, users could receive further privacy related notifications based on their preference profiles, which may by choice, by default or via customisation consider cultural notification preferences as well.

Our research can ultimately lead to Human Computer Interaction guidelines for usable consent and usable ex post transparency functionality for the demonstration use case 3. As mentioned, this should however preferably also be based on follow up end user research studies related to the employment/educational context of privacy preserving identity management.

4 Integration with Demonstration Case 4

Demonstration case 4 targets an incident reporting system that collects information about security incidents (e.g.~ransomware via a phishing email, DDoS attack on an e-banking website, etc.). This information enables relevant stakeholders to evaluate the severity of the incident and to produce a report towards concerned authorities. This demonstration case combines different assets to manage the complexity of multi-factor authentication (MFA) for such a threat intelligence system.

4.1 Goal and Scope

The scope of this demonstration case is to offer guidance to security administrators that are faced with complex decisions when setting up single-factor, two-factor or multi-factor authentication for their online applications, such as this incident reporting system. Their configuration choices will have an impact on the overall security, privacy and usability of the solution, but analysing the trade-offs for a given authentication configuration is not straightforward. The goal of the demonstration case is to offer guidance based on the NIST SP 800-63B specification [10] on authentication, analyze a given authentication configuration w.r.t. the NIST guidelines and preferred assurance levels, and simplify the configuration of a state-of-practice identity and access management system that is linked with the incident reporting system.

Authentication methods are based on cryptographic operations, which in turn are derived from complicated mathematical constructions. They are not understandable to human users that need to interact with cryptosystems; the human users are left out of the loop of establishing trust in the digital world. In general, the study of human-machine interactions has advanced greatly in the recent past, but within the field of cryptography, progress has been slow. In our research, we aimed to bridge this trust gap. We wanted to construct a communication channel so that the human user is able to infer the integrity of the channel from visual cues and the behaviour of the server they are communicating with. There are some existing cryptographic techniques and protocols that have been published before, but they have not been applied to full communication channels between two parties yet.

4.2 Part of demonstration case 3 involved in the integration

This demonstration case uses MISP as the incident reporting platform, but the latter has limited authentication capabilities. However, with our asset TATIS that acts as a reverse proxy for MISP, we can extend this functionality by leveraging state-of-practice identity and access management platforms that will handle the (multi-factor) authentication on behalf of MISP. For demonstration purposes, we use RedHat Keycloak as an open source IAM platform. Our second asset AuthGuide, helps with the creation of an MFA authentication configuration and workflow to protect TATIS, which in turn protects MISP. Finally, the third asset, EEVEHAC, can be used as an authentication method for KeyCloak.

4.3 State of the Art

This demonstration case combines different assets with two different purposes, i.e. (1) the management of cyber threat intelligence and (2) the enhanced support for multi-factor authentication including novel authentication modalities.

The state-of-the-art on cyber threat intelligence and supporting platforms is beyond the scope of this document, as it has already been addressed as part of Task 3.4 and reported in deliverables "D3.3: Research Challenges and Requirements to Manage Digital Evidence" and "D3.14: Cooperation With Threat Intelligence Services For Deploying Adaptive Honeypots".

The research carried out within the frame of AuthGuide and EEVEHAC focuses on enhanced authentication and has also been reported on in a deliverable associated with this Task 3.6, in particular, deliverable "D3.16 Security requirements and risks conceptualization".

The state of the art can, as such, be clustered into two lines of research, that both target enhanced authentication, but with a clear focus on the human factor:

- Many relevant works on cryptography focus on provable security properties and are well-suited for machine-to-machine interaction, but tend to leave out human factors when defining security models. Several notable research directions that aim to address this challenge are (1) visual cryptography [11], (2) visualizable encryption [12], (3) hash visualization [13] and (4) the use of human computable functions in cryptography [14].
- Many two-factor and multi-factor authentication solutions have been proposed in the literature[15]. They often aim to increase the security, but often ignore usability and privacy threats, or are subject to a variety of threats that jeopardize the security of the application or system it aims to protect when the strengths and weaknesses are poorly understood by end-users [16].

We refer the reader to sections 4.2 and 4.4 of deliverable D3.16 for a more detailed discussion on the relevant state-of-the-art and state-of-practice.

4.4 Challenge Beyond the State of the Art

The first challenge addressed in this demonstration case shows how we get beyond the state-of-the-art by leveraging human computable functions to realize an end-to-end visualizable encrypted and human authenticated channel. More specifically, the asset EEVEHAC combines two techniques in an innovative way to realize this capability: a human authenticated key exchange (HAKE) protocol based on [14] and a visual encrypted channel based on EyeDecrypt [12].

Many state-of-the-art authentication solutions have been proposed in the scientific literature, including how they can be combined to enhance the protection of systems and applications. Various guidelines, such as[17], have been proposed to document best practices for authentication. With AuthGuide, our research goes beyond the state-of-the-art by leveraging this knowledge into a tool that can create actionable insights as well configuration support for state-of-practice identity and access management systems.

A summary of the capabilities of the assets is provided in the next subsection, as well as in the associated deliverable D3.16.

4.5 Description of the integrated assets

4.5.1 TATIS: Trustworthy APIs for Threat Intelligence Sharing

Our asset TATIS [19] [20] [21] developed within the frame of Task 3.4 enhances MISP, a state-of-practice cyberthreat intelligence platform, by protecting sensitive content with advanced encryption and other privacy enhancing techniques before the information is shared with other parties or communities. More

specifically, TATIS aims to share the gathered data among different organizations, such that only certain entities can decrypt the threat intelligence if the attributes used to construct their individual decryption key match the encryption policy of the ciphertext. TATIS operates as a reverse proxy for MISP, and as such it also augments the authentication and authorization capabilities of the underlying threat intelligence platform for users aiming to access either the interactive dashboard or the RESTful APIs offered by MISP. TATIS leverages Redhat Keycloak, a contemporary identity and access management suite, to offer more sophisticated multi-factor authentication capabilities beyond the standard password-based authentication of MISP. Being open source, it is possible to offer new ways of authentication (e.g.~EEVEHAC) by implementing the proper Service Provider Interfaces (SPI) of Keycloak, and more specifically the Authenticator and AuthenticatorFactory interfaces.

4.5.2 AuthGuide: Analyzing security, privacy and usability trade-offs for MFA

Security administrators are often faced with a large number of configuration options when setting up MFA for their users, and the implications of an administrator's choices on security, privacy and usability for the end-user are not always well-understood. AuthGuide [21] assists security administrators with configuring their IAM platforms by mapping individual options in AuthGuide onto a specific IAM workflow of authentication steps for registration and login. AuthGuide analyzes (1) the security, privacy and usability implications of different authentication factors, (2) their combination in an MFA configuration, and (3) the consequences of granting some flexibility on authentication factor selection to the end-user. Our solution builds upon the NIST set of technical requirements [22] to evaluate the assurance level of MFA implementations, as well as their impact on privacy and usability by checking the compliance with `SHALL' and `SHOULD' requirements (including the negative forms), the degrees of freedom offered to the end-user, as well as influences of external elements beyond control of the security administrator of an IAM and/or end-user.

4.5.3 EEVEHAC

EEVEHAC [23], or End-to-End Visualizable Encrypted and Human Authenticated Channel, is a proof-of-concept implementation of a communication channel. It combines a human authenticated key exchange method with a visualizable encryption that can be utilized in an untrusted environment, so that the human user can oversee the execution of the entire communication process.

4.6 Description of integration with DC4

Beyond the analysis of the different requirements in the NIST special report, AuthGuide also has the capability to generate a custom specialized script to configure MFA for Keycloak and this in line with the options selected within AuthGuide. After executing this script, the corresponding realm of TATIS in Keycloak has been set up with MFA.

When using EEVEHAC, the first step is to register yourself with the server as a new user. Keycloak has the Client Registration Service that could be used to fulfill this need. Next, the human authenticated key exchange protocol and password authenticated key exchange combination used in EEVEHAC could be developed further so that it can be used as an authentication protocol in Keycloak. This protocol involves human interaction and mental effort for choosing the right responses for the server's challenges, therefore it will never be as quick to run as regular authentication protocols. Therefore, the first phase of the system establishes short term keys that can be used more easily in the second phase of the system. These keys could be adapted into tokens used in Keycloak. There is a "technology preview" of Token Exchange in Keycloak.

With this more experimental approach, we could exchange the short term keys of EEVEHAC into tokens that could be used in different applications outside of the original visualizable encryption usage of EEVEHAC.

5 Integration with Demonstration Case 5

Demonstration case 5 is maritime transport, and in particular maritime supply chain services. Such services involve several various distributed and inter-connected organizations (e.g. carriers, customs, port authorities, etc.), as well as several infrastructures (e.g. port infrastructures, carrier facilities, IT and SCADA services, etc.), and human actors belonging to those organizations and infrastructures (e.g. carrier agents, customs agents, ship agents, port operators) with different business and operational goals [24].

Maritime transport sector is considered the backbone of the globalized trade and manufacturing supply chains, as it mostly incorporates distributed, and digital services which are highly interconnected, offering increased volumes carried by sea and decreased delivery time. Nowadays, maritime supply chain services are a prime target for various threat agents such as cybercriminals or cyberterrorists.

5.1 Goal and Scope

The main research goal is to demonstrate that human task modeling techniques support the identification of cyber threats on maritime supply chain operators' tasks. We went beyond the state of the art by integrating the asset HAMSTERS (task modelling technique) with the asset MITIGATE (maritime supply chain risk assessment methodology).

The International Maritime Organization (IMO) provides guidance for maritime cyber risk management [25], in order to "support safe and secure shipping, which is operationally resilient to cyber risks" and defines a set of high-level recommendations for the identification and mitigation of cyber threats (e.g. to identify personnel roles and responsibilities, to identify systems, assets, and to implement risk control process). It also points out additional guidelines, such as the NIST guide on conducting risk assessment and the ISO 27001 standard on requirements for information security management systems [26]. In addition, as several organizations are involved in the supply chain, the risk management methods need to deal with several information and require data arising from all of them to be able to identify cyber threats on the entire maritime supply chain [27].

5.2 Part of demonstration case 5 involved in the integration

The integration with DC 5 involves the use case UC551. This use case is the Threat Modeling and Risk Analysis for Maritime Transport Service that enable the involved actors to collaboratively and securely exchange threat and risk related information, to define the scope of the assessment, to model their continuously evolving threat landscape, to assess their relevant cybersecurity threat, vulnerability, impact and risk, and to make informed decisions related with risk mitigation.

5.3 State of the Art

In the literature, few work has focused on the relation of human task modelling of maritime supply chain applications. Yang studied the risk management for container security in Taiwan's supply chain [28]. In particular, this work focuses on investigating the utility of the loss exposure matrix and bow tie diagram during the risk assessment. Chang et al. [29] proposed and apply an empirical approach for the identification and analysis of risks in container shipping operations. The main philosophy is to gather feedback from operators via interviews and questionnaire surveys. Both contributions are limited to a specific type of

operation and to a specific subset of infrastructure assets. MITIGATE [27] aims to assess the risk of supply chain services requiring the interaction of assets from various stakeholders (or business partners). The asset MITIGATE supports the identification of the relevant attack paths and assesses their cumulative risk level for various cyber threats. However, the effect of human tasks on the identification of threats is not examined with respect to the identification of human related threats. Beyond the maritime supply chain application domain, the HEART-IS human reliability analysis technique [30] supports the evaluation of human error-related security incidents. It supports the identification of the main operators' task types for any application domain, as well as possible human errors for these tasks and their likelihood of occurrence, but it does not explicitly support the systematic identification of all operators' low-level tasks. Boender et al. [31] proposed a modelling technique to describe possible human behavior using higher order logic. It focuses on insider attacks and supports the modelling of infrastructure and organisation, which enables to model check the possibility of an insider attack. Finally, Garbacz et al. [32] applied model-based analysis to assess the security of a deposit return system. It supports the identification of the actors involved in the operations as well as of the workflow, but it does not support the description of interconnecting assets and operators' low-level tasks.

5.4 Challenge Beyond the State of the Art

Several types of threats may weaken the maritime transport supply chain. The goal of external attackers is to bring down the supply chain or part of it, or to steal/corrupt data.

They may perform different types of attacks:

- Attack directly the assets in the supply chain (such as software and hardware components). Examples of such attacks are Denial of Service (DoS), phishing, malware and cyber extortion.
- Attack the operators who perform tasks with interactive systems. Examples of such attacks are eavesdropping (i.e. video recording, shoulder surfing, keylogging, etc.) while an operator is interacting with a system to accomplish her/his mission in the supply chain. Such attacks aim to gain information about planned deliveries, content of cargos, authentication credentials, etc. They can then be used for direct cyber-attacks or physical attacks on the supply chain.

Attacks may have a large impact on the supply chain as well as on the financial health of maritime companies. For example, in 2017, several terminals of the shipping line Maersk were attacked by malware, resulting in disrupted operations for several weeks and costing 300 million USD.

Internal (supply chain) operators such as ship agents or port agents have specific jobs' tasks and procedures to apply in order to accomplish their respective mission, (e.g. gather cargo information for a ship agent or book port resources for a port agent.) However, they may:

- Make errors: they may perform tasks in a way that they will not reach the one or several missions of their job. Examples of such errors may be to input the wrong number of containers or the wrong gross weight of the load. These errors may be the root cause of a security incident and as such are referenced as a potential source of threats
- Intentionally deviate from the planned tasks and act as malicious insiders. Examples of such deviations may be to modify manifest records or steal manifest records.

Human errors also may have a catastrophic impact on the supply chain. For example, an agent who makes an error while performing the task of editing information in a manifest, such as the number of containers,

load weight or the number of passengers can lead to insufficient arrangements concerning safe navigation. This may put in danger the whole supply chain performance, including its crew members, passengers and loads, by causing injuries to crew members and passengers, as well as damages on the loads.

There is thus a need to account for cyber threats on human operators' tasks, and this in a detailed way, in risk assessment methodologies.

5.5 Description of the integrated asset HAMSTERS

HAMSTERS (Human – centered Assessment and Modelling to Support Task Engineering for Resilient Systems) is a tool-supported task modelling notation for representing human activities in a hierarchical and temporally ordered way [33].

Task models are precise and unambiguous descriptions of user tasks. In the proposed approach for integration with demonstration case 5, they enable to describe the maritime transport supply chain operators' tasks. In this section, we highlight how they are the cornerstone of the proposed approach, by enabling the identification and representation of threats on operators' tasks.

Task models consist of an abstract description of user activities structured in terms of goals, sub-goals, and actions. The task models that result from task analysis will differ according to the features of the selected modelling language or notation. These modelling differences are likely to highlight (or filter out) different aspects of the user tasks. Therefore, it is important to choose the most suitable task modelling technique, i.e. the notation with the most suitable expressiveness, which highlights the aspects that are relevant to the goals of the analysis.

In the case of supply chain services, human tasks strongly rely on motor, cognitive and perceptive abilities and actions. The tasks performed also strongly rely on interactions with computing systems as well as on information processed by the business partners. A task modelling notation that supports the description of tasks to provide supply chain services requires embedding elements to represent motor, cognitive, perceptive and interactive actions, elements to represent the temporal ordering of actions, and elements to represent manipulated objects and information. The notation HAMSTERS we have adopted in the current research work fulfills these requirements.

Figure 2. Main types of tasks in HAMSTERS

Figure 3. Refined types of user tasks in HAMSTERS notation

The notation enables to represent tasks in a hierarchical temporally ordered way. A task model looks like a tree diagram with nodes being either a task (described hereafter in the paragraph) or a temporal ordering operator (e.g. ">>" stands for sequence, "|=|" stands for order independent, "[>" stands for deactivation…). The original aim of HAMSTERS was to support the modelling of large sets of elements [34]. HAMSTERS can be used to represent abstract tasks, user tasks, interactive tasks and system tasks (depicted in Figure 2. Refined types of user tasks are: motor, perceptive and cognitive (depicted in Figure 3). Cognitive tasks can also be refined into cognitive analysis tasks and/or cognitive decision tasks (on the right in Figure 3).

In addition, HAMSTERS can model the collaboration between different types of users, and in particular cooperative tasks (a task in a task model for a type of user that has a corresponding task in another task model for another type of user, e.g. a cooperative task "send a message" in a user task model will have a corresponding cooperative task "receive a message" in the task model of the collaborator user) [33]. Finally, HAMSTERS supports data representation, such as information, knowledge and objects manipulated by users [33]. Information, knowledge, and objects (which can be physical objects or software objects) are depicted using labels preceded by the abbreviation of the type of data. Figure 6 shows examples of such representation, where the software object "Manifest" is required to complete the interactive input task "Store the manifest on the customs server". Arcs between data and tasks represent how the data is used. In Figure 6, from the left, the arrow from the software object "Manifest" to the interactive output task "Display manifest" (in the bottom left) means that the task requires the software object labelled "Manifest". The arrow from the information labelled "Actual value of data fields" to the cognitive decision task "Decide that manifest is ready" means that the task requires the information "Actual value of data fields". The arc from the perceptive task "See content" to the information "Actual value of data fields" means that perceptive task produces the information "Actual value of data fields".

Task models, because they embed precise information about operators' actions and the interactions between operators and systems, they support systematic and precise identification of potential human errors and potential threats on tasks. Human errors' root causes lie in the potential malfunction of human information processing [35]. Humans make errors because they perceived wrongly their environment (perception malfunction), or because they forgot an information (cognitive malfunction), or because their finger slipped from the keyboard (motor malfunction). Being able to describe operators' tasks at the perceptive, cognitive and motor level supports the systematic identification and representation of errors' root causes and impact [36]. The same philosophy can be applied to cyber threats. Part of the cyber threat detection process lies in the possible and expected interactions between operators and interactive systems [37]. Operators may be key logged while they type information on their desktop (interactive input task) or their screen may be shot while the desktop screen displays information (interactive output task). The identification and representation of threats in task models, whether their source is human errors or attacks, thus require elements of notation to express refined types of tasks (perceptive, cognitive, motor, interactive input, interactive output) and data (information, knowledge), as well as elements of notation to express a root cause for error and to express threats.

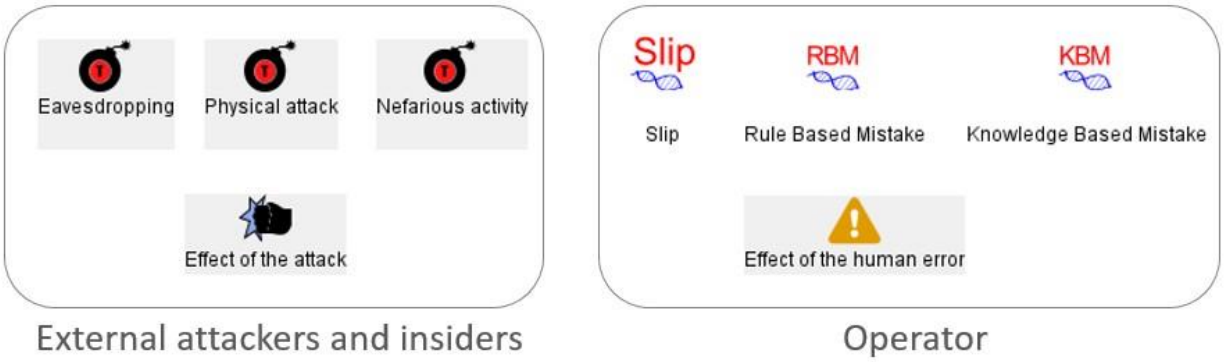


Figure 4. Elements of HAMSTERS notation for the modelling of threats and their effects

Figure 4 presents the main elements of the HAMSTERS notation that aims to represent possible threats and their effects.

The types of cyber threats (eavesdropping, physical attack and nefarious activities) that are represented derive from the ENISA taxonomy of cyber threats [38]. Using this ENISA taxonomy, the HAMSTERS tool provides automatically a list of concrete threats for each of the types of threats, which can be selected at runtime. The types of human root causes of errors derive from the GEMS taxonomy of human errors [35]. Using this GEMS taxonomy, the HAMSTERS tool provides automatically a list of possible concrete human root causes of errors according to the types of tasks for each task described in the task model. An example of task models with embedding representation of such threats is presented in Figure 7 and Figure 8.

5.6 Description of integration with DC5

We integrated the use of the HAMSTERS task modelling notation within the MITIGATE methodology to support the risk assessment of threats that may arise from operators' tasks and errors, during the maritime supply chain operations.

MITIGATE is a collaborative evidence-driven Maritime Supply Chain Risk Assessment approach. MITIGATE captures various threats arising from the Supply Chain (SC) environment, including threats associated with sectorial infrastructure interdependencies, and the associated cascading effects. MITIGATE extends Medusa methodology [39] and is compliant with the ISO/IEC 27000 [40] information security and the ISO/28000 SC security management international standards. It decomposes in four steps that are gradually undertaken to evaluate risks.

- Step 1. Supply Chain Service (SCS) analysis: aims to identify the boundaries of the risk assessment process, identify the under examination SCS of the maritime transport sector, analyse and model its generic components, i.e. SCS processes, involved business partners and assets operating within the SCS processes. It produces the SCS process models, the SCS asset inventory and the SCS asset inter-dependencies graph.
- Step 2. Cyber threat analysis: aims to identify and assess all cyber threats that are related to the identified assets of the under examination maritime transport SCS. The outcome is a list of cyber threats assessed in a qualitative threat level from the following list of threat levels: "Very Low" ("VL"), "Low" ("L"), "Medium" ("M"), "High" ("H"), "Very High" ("VH"). This threat level is the probability of occurrence of a cyber threat.

- Step 3. Vulnerability analysis: identifies the system vulnerabilities. It supports the estimation of the possibility of vulnerability exploitation for an asset (individual vulnerability assessment) as well as the cascading effects and propagation of the vulnerability to the interconnected SCS assets concerning the accessibility to an SCS asset (cumulative vulnerability assessment), and the attacker capacity to infiltrate the SCS asset network (propagated vulnerability assessment). It also produces possible attack paths revealed from attack graphs. The list of security threats is elicited from the NIST vulnerability database [26]. Each SCS asset has a corresponding Common Platform Enumeration (CPE) identifier that is used to identify the possible corresponding existing Common Weaknesses Enumeration (CWE slice of the NIST database).
- Step 4. Impact analysis: It estimates the effect that can be expected as a result of the successful exploitation of a vulnerability that resides in a given SCS asset. The step delivers the impact levels for each identified vulnerability to the SCS assets.
- Step 5 and 6. Risk Assessment and Mitigation: predicts the risk level for the identified assets, taking into account the produced threat level, vulnerability level and impact level from the previous steps.

HAMSTERS task modelling technique supports the MITIGATE methodology in several ways. The precise description and representation of operators' tasks enable to complement step 1 (SCS analysis) of the MITIGATE methodology by refining knowledge about operators' activities and assets involved in these activities. HAMSTERS also enables to find additional threats (in steps 2, 3, 4) by identifying possible operators' errors, and possible attacks on operators' tasks, whether they are performed by external attackers or insiders. The integration of operators' task models in the risk management methodology should then help to increase the coverage of potential threats, vulnerabilities and their impact.

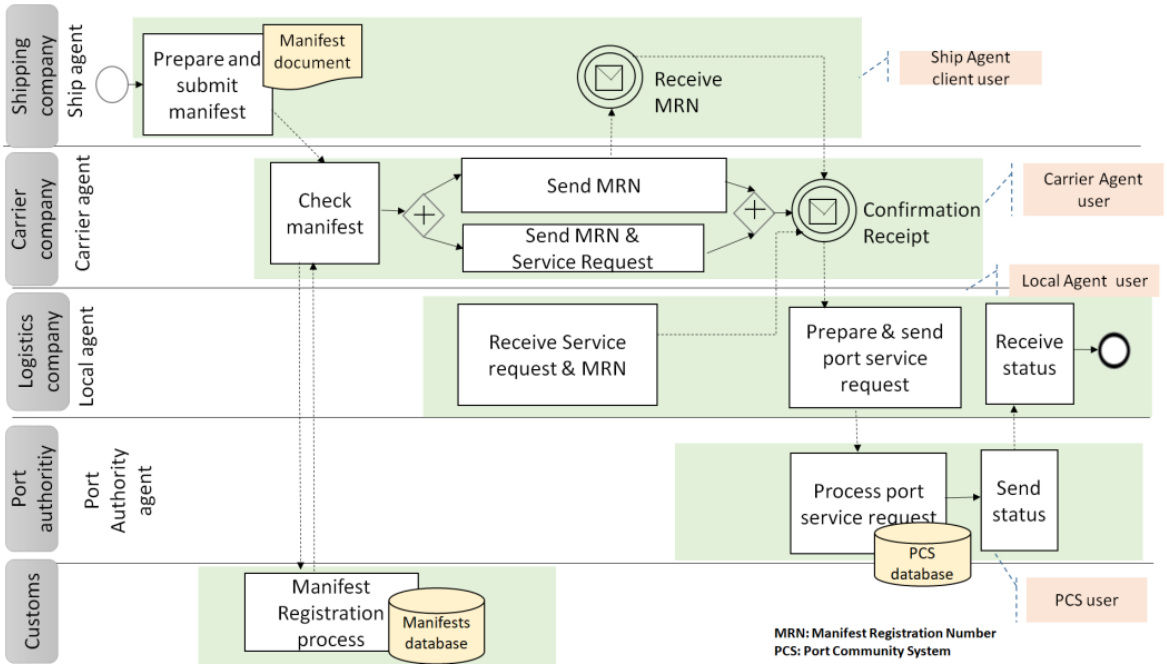


Figure 5. BPMN diagram for the manifest declaration to port service request and preparation process

We applied this integration to the risk analysis on the process "Manifest declaration and port service request preparation". A manifest file contains information about the port of embarkation, port of disembarkation,

ship's content, passengers, date of departure, date of arrival, carrier code, nationality of transport code, total number of bills, total number of containers, total gross weight, etc. The manifest is first prepared by a ship agent, then verified and submitted to the custom by a carrier agent. Once approved by the custom, it is then used by port agents to prepare logistics in port. The main expected outcome is to identify potential threats on the use of cargos' manifest and to identify potential vulnerabilities and their impact on the service provision, infrastructures operations and business partners tasks.

Figure 5 presents the business process model depicting the SCS process interactions between business partners to prepare the vehicle transport starting from manifest creation ending to port service request preparation. It highlights the main types of stakeholders involved in the process (ship agent, carrier agent and local agent). The process model is developed using the BPMN 2.0 modelling language.

Integration of HAMSTERS within SCS Analysis (step 1). We added the identification and description of operators' tasks to this step. The output is a set of task models for each operator that contain all the tasks that an operator is supposed to perform. Figure 6 is an example of such output and describes the tasks of the carrier agent to check and register a manifest.

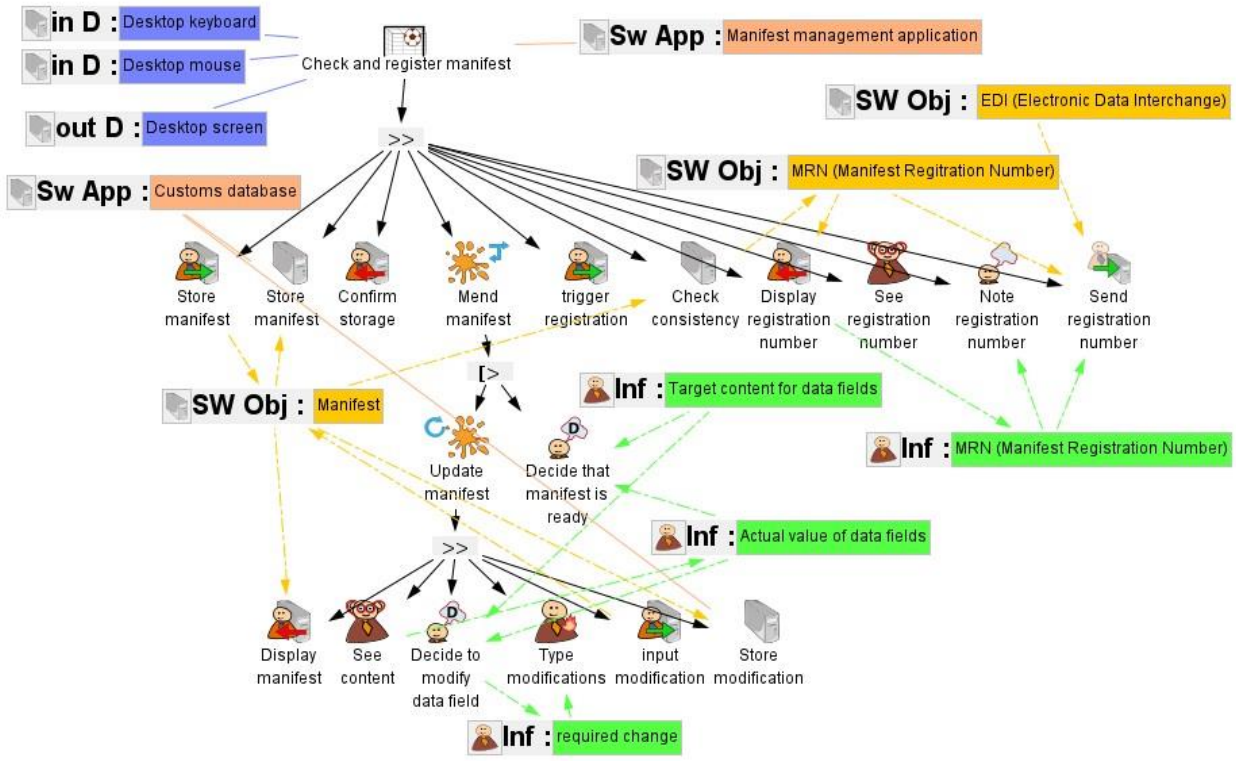


Figure 6. Task model of the sub-goal "Check and register manifest" of a carrier agent

Identification and representation of additional cyber threats (step 2). The application of task model based techniques for systematic identification of human errors [36] outputs a new version of task models including possible human errors (root causes and potential consequences). Figure 7 and Figure 8 are extracts of such models. Using task models with the technique for identifying user threats and effects, we produced a new version of task models that embed possible threats on users interacting with computer applications and their impact. Figure 7 provides an example of such a model. It presents an extract of the task model "Check and

register manifest" with the representation of a subset of threats and their associated impact. For example, the interactive input task "input modification" can be keylogged or video (threats connected to the task labelled "Eavesdropping video recording attack" and "Eavesdropping keylogging") recorded by an attacker to steal the content (impact connected to the threats labelled "Information leak from manifest content"). The user motor task "type modification" can be wrongly per-form by a nefarious insider to falsify information in the manifest.

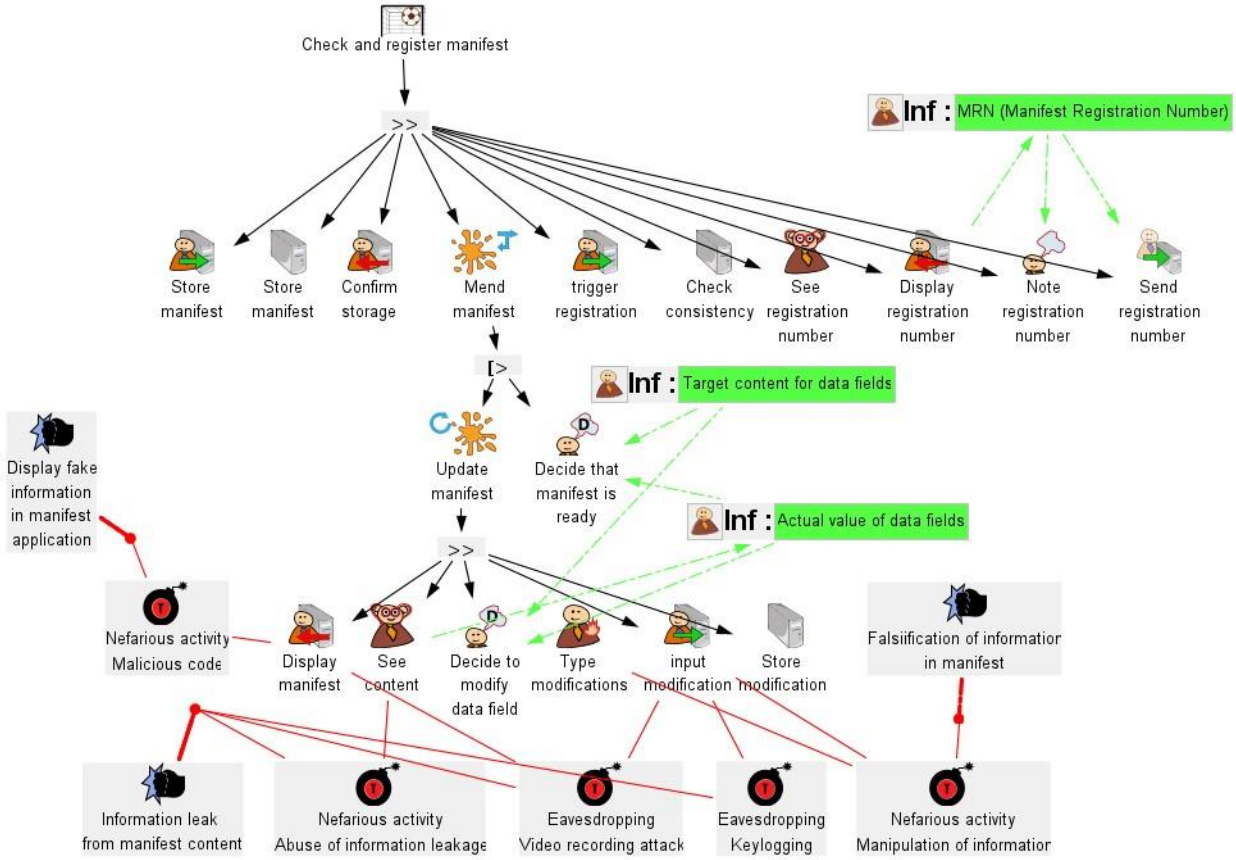


Figure 7. Extract of the representation of external attackers & insiders threats ("Check and register manifest")

In the same way for human errors, using task models with the technique for identifying human errors and their effect, we produced a new version of task models that embed possible user errors and their impact. Figure 8 is an extract of the task model "Check and register manifest" with the representation of a subset of possible errors. The motor task "Type modification" may trigger two possible root causes of error: an interference error meaning that operators' fingers may input a different value than the targeted one (root cause connected to the task labelled "Slip interference error inputs a different value"), and a lapse error, meaning that the operator can be interrupted by an event in the room and forgot to type (Lapse root cause connected to the task labelled "Lapse Omissions following interruption do not type modification"). Both root causes may lead to wrong information in the manifest, which may cause a wrong arrangement of services and an unsafe navigation (effect connected to the root causes and labelled "Wrong information in manifest Insufficient arrangement for safe navigation").

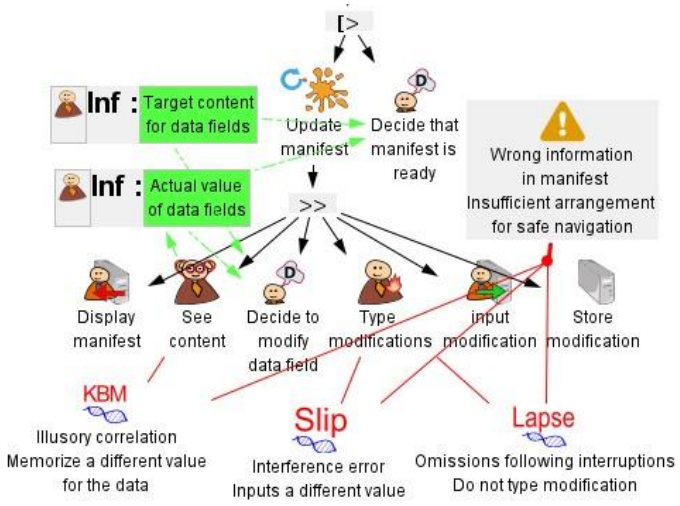


Figure 8. Extract of the representation of human error threats ("Check and register manifest")

Table 2 presents a subset of the list of additional potential threats that have been identified using task models. In the following paragraphs, we detail a potential operator error that has been identified additionally thanks to the integration of HAMSTERS within MITIGATE, as well as an external attacker threat that has been identified additionally thanks to the integration of HAMSTERS within MITIGATE (both are highlighted in grey in the table).

Table 2. Extract of the table of vulnerabilities caused by operators' tasks for the "Update manifest" sub-goal of the task model "Check and register manifest" for the carrier agent.

Source	Type of threat	Threat	Task	Type of task	Impact
Operator errors	Slip	Double capture slip: operators inputs the number of containers that s/he has been used to input most of the time	Type modifications	Motor	Wrong information in manifest, in sufficient arrangement for safe navigation
	Rule based mistake	Misapplication of good rule: grant access to manifest editing to an operator that has not the accreditation for editing	Decide to grant editing permission	Cognitive	Grant unappropriate access rights to agent
	Knowledge based mistake	Illusory correlation: Memorize a different value for the data	See content	Perceptive	Wrong information in manifest, in sufficient arrangement for safe navigation
	…				
External attackers and insiders	Eavesdropping	Keylogging: external attacker records key presses performed by the operator	Input modifications	Interactive output	Information leak from manifest content
	Nefarious activity	Abuse of information leakage: insider operator memorizes data	See content	Perceptive task	Information leak from manifest content
	Nefarious activity	Malicious code: external attacker injects code in the presentation page	Display manifest	Interactive output	Display fake information in manifest application
	…				

Analysis of vulnerabilities and impact (steps 3, 4). The identified threats have corresponding entries in the NIST vulnerability database. The rule-based mistake "Misapplication of good rule" on cognitive task

“Decide to grant editing permission” (line 2 in the "Operator errors" upper part in Table 2 matches the CWE 842, which expresses the threat “Placement of User into an Incorrect Group”. This threat is triggered through vulnerability CVE-2010-3716, which allows remote authenticated users to gain privileges via a crafted POST request that creates a user account with arbitrary group memberships. This threat may also engender another weakness, CWE-403, related to the threat “Exposure of File Descriptor to Unintended Control Sphere”. CWE-403 is manifested through the vulnerability CVE-2004-1033, in this case, a file descriptor leak might allow an unauthorized user to view restricted files. The additional identified nefarious activity “Malicious code” on interactive output task “Display manifest” (line 3 in the "External attackers and insiders" lower part in Table 2) matches the threat CWE-79, which allows the “Improper Neutralization of Input During Web Page Generation”. This threat is expressed through CVE-2008-4450, a Cross-site scripting (XSS) vulnerability in adodb.php in XAMPP for Windows 1.6.8 that allows remote attackers to inject arbitrary web scripts. CWE-842 affects the asset Manifest Database asset, while CWE-403 and CWE-79 affect the Manifest Management application.

6 Integration with Demonstration Case 7

Demonstration case 7 addresses Smart Cities and focuses on the setup and deployment of a user-centric sensor-based infrastructure to support personal data exchange. The main focus of DC7 is to build an ecosystem capable to foster business models based on personal data exchange and usage in Smart City and Public Services, while properly managing the related cyber threats and being compliant with regulation.

6.1 Goal and Scope

The main research objective of this demonstrator is to show how privacy-preserving techniques can be applied in smart city scenarios by incorporating usability techniques that make it easier for users to interact while keeping their data from being compromised. In that sense, one of the specific goals is establishing an implementation of privacy preserving identity management and the corresponding policies so they are user-friendly.

To that end, we go beyond the state of the art thanks to the results presented in D3.16, where guidelines for what users want in that field are presented. Namely, we increase the security and privacy of the identity management system by distributing the role of the identity provider with minimal effect on developers or users. Additionally, we establish the means for users to choose the level of verbosity when interacting with policies, and a framework for added trust in the solution and services that partake in it.

6.2 Part of demonstration case 7 involved in the integration

Demonstration case 7 is centred on Smart Cities and technologies enabling the secure and privacy-preserving management of that kind of platform. In this section, we focus on the integration of the related assets into the Smart City scenario. The manner of integration will vary for each asset, with a close relationship with the classification established in D3.16. In particular, the Self-Sovereign pp-IdM, as a user layer asset, will be directly integrated into the platform for enabling privacy-preserving authentication and authorization. The SYSVER asset, which is part of the analysis layer, is shown as a possible supporting tool for security analysis of the Smart City platform, addressing the complexity of the system while keeping usability.

6.3 State of the Art

In deliverable D3.16 (which can be read for more detail), we described the state of the art on identity management focusing on the aspects related to privacy and usability, as they are most relevant to the work developed within this task. We remarked on the privacy issues of current federated solutions, which are even then the most attractive for users because of their convenience. Recent proposals for secure and private identity management have not been able to attract users because of their poor usability. This challenging situation is (if possible) even more relevant in the context of Smart Cities. The amount of data managed in Smart Cities makes privacy-by-design solutions critical, and the high volume of interactions between users and the platforms only aggravates the usability demands of users.

The security analysis of large and heterogeneous systems like a Smart City is a complex task. In particular, for what concerns the access control policies and their verification, the difficulty arises from the complex relationships between the possibly large number of different agents and actors involved in the Smart City.

In the broad context of policy analysis, several approaches are available [41]. In particular, given the networked nature of the considered systems, a focus on potential anomalies in protection policies is relevant [42]. The approach followed while considering the peculiarities of the considered Smart City scenario, is one based on a formal analysis of the correctness of the service implementations and their relationships with respect to complex users' activities and related access control policies. The results obtained with this approach are complex and difficult to present and manipulate by a human user [43]. Moreover, besides the representation, there is the necessity to provide the system administrator with possible solutions, based on the analysis results, to help him fix the problems.

6.4 Challenge Beyond the State of the Art

In the scope of privacy-preserving identity management, we go beyond the state of the art by considering the user studies results presented in D3.16 to develop a usable, secure, and privacy-aware solution. Namely, we increase the security and privacy of the identity management system by distributing the role of the identity provider with minimal effect on developers or users (the change is transparent except for conceptual understanding). Additionally, we establish the means for users to choose the level of verbosity when interacting with policies, and a framework for added trust in the solution and services that partake in it.

For what concerns the policy analysis results representation and usage, the challenges here are to be able to take into account the complexity of service relationships in the considered Smart City scenario, by means of formal models, and to be able to represent in a usable form the obtained results so that the system administrator is actually supported in understanding and prioritizing the problems and finding possible solutions.

6.5 Description of the integrated assets

6.5.1 Usable Self-Sovereign PPIdM

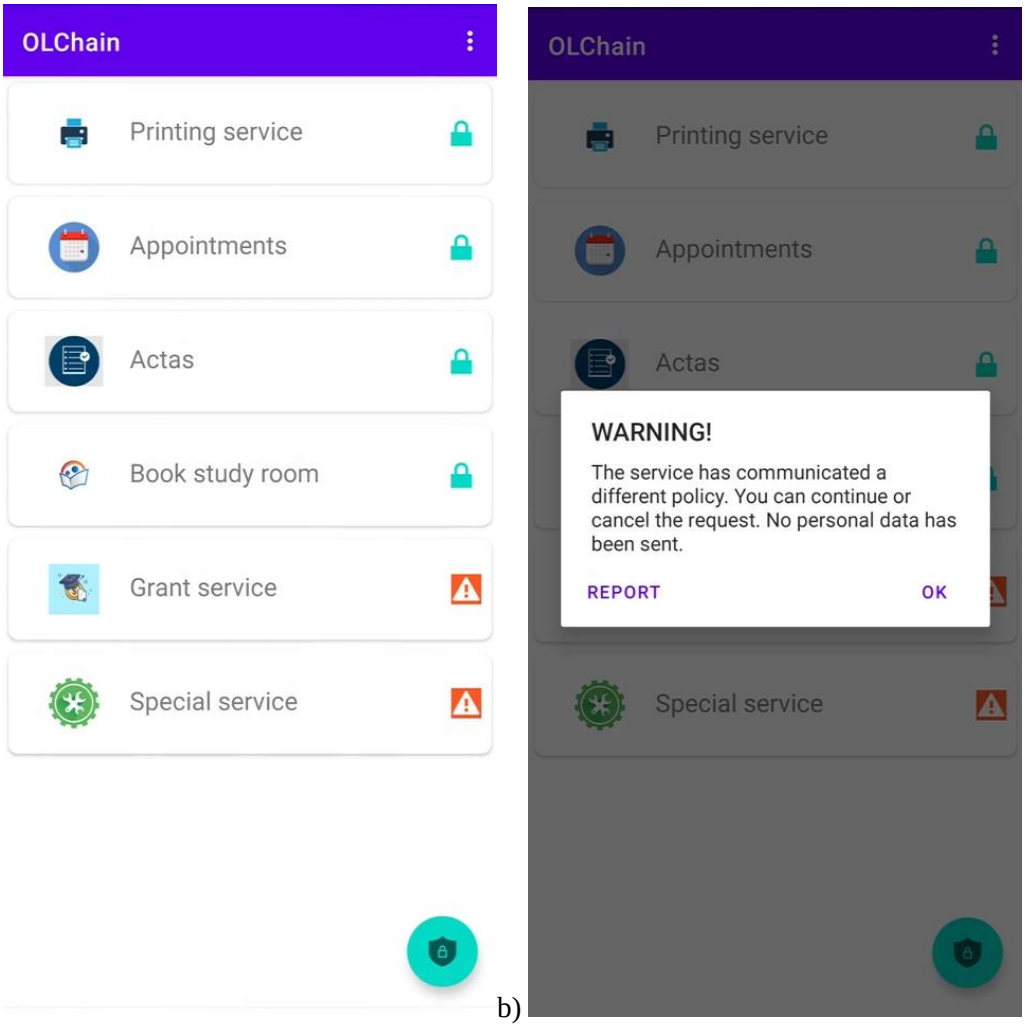
This asset leverages the OLYMPUS[1] virtual identity provider, which is comprised of multiple individual IdPs, to manage user identities and authentication. It relies on distributed p-ABCs to offer privacy-preserving (minimal disclosure and unlinkability) and authentication (presentation of attributes). Moreover, the asset proposes a trust framework based on Blockchain to complement the usage of credentials, including the public offer of services that can define their behaviour (e.g., which access policy they request). For extra information on the asset, the interested reader can check D3.13.

In this deliverable, we will focus on the steps taken to increase the usability of the asset. We will support the description with images taken from the mobile application developed to demonstrate this functionality. Usability does not only apply to users, but developers also benefit from the solution as they do not have to worry about the fact that IdPs are distributed. This property is completely transparent to them as well as to the users, thanks to the OLYMPUS client interfaces.

In addition, the inclusion of blockchain allows to improve not only the discovery of services but also adds discovery of IdPs involved in the scenario and allows to keep track of the behaviours declared by service providers thanks to the monitoring of access policies. Thus, it serves as backbone support for increasing

[1] https://olympus-project.eu/

user trust in the general solution and the services that take part in it. For instance, Figure 9 shows services included in the demo, with two of them being marked as potentially harmful because of a discrepancy between the policy sent and the one declared on the ledger (a), and the warning shown when trying to interact with them (b).



a) b)

Figure 9. Services included in the demo (a), and the warning shown when trying to interact with them (b)

Lastly, the main efforts have been focused on the visualization aspects and the ease of management of access policies on the user application. The main idea is to give users the option to adjust the verbosity level. By default, they have to read (encouraged by adding a checkbox that has to be accepted to be able to continue the process) and explicitly consent to every policy, though the decision can be remembered for some time (Figure 10 a)). However, users have the option to activate preferences on identity attributes (this configuration is protected behind biometric authentication). If they choose to do so, they can select three levels for each attribute (Figure 10 b)):

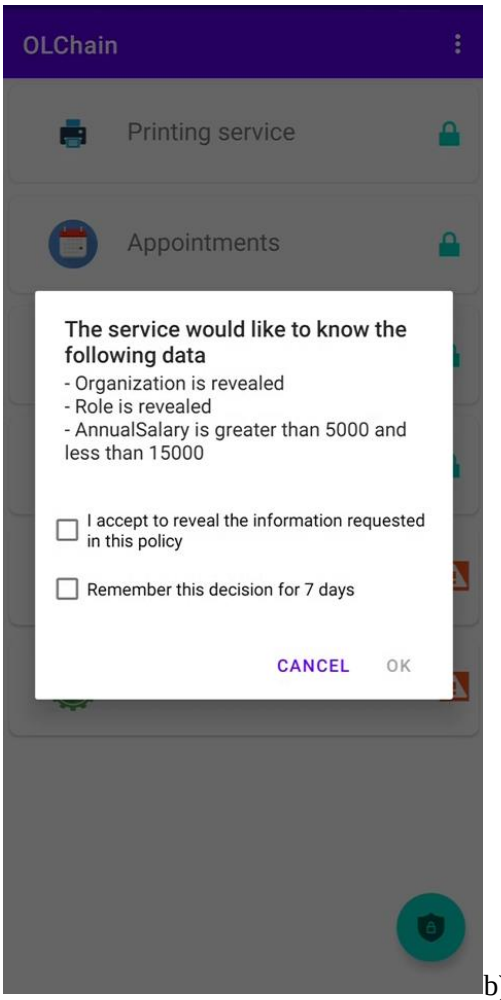
- NOTHING: If the attribute appears in the policy, you will be explicitly asked for consent.
- PREDICATE: If the policy asks for a predicate over the attribute (e.g., greater than) it will comply with the preference, but if it implies revealing the value of the attribute, you will be explicitly asked for consent.

- REVEAL: You consent to automatically reveal any information (predicate or explicit value) about the attribute.

For each policy asked by a service, the acceptance process will be automatic if **all** the attributes involved follow the preferences. In any other case (or if the service was marked as untrustworthy because of a policy change), the policy will be shown to the user and he/she will have to explicitly read the contents and consent.

For example, a policy asking to reveal the role and prove that the date of birth was before the year 2000 would comply with the preferences and the process of accepting the policy would be automatic (consent was given previously). On the other hand, if the same policy would ask for any information about the annual salary, or even for the revelation of the date of birth, it would be shown to the user to collect the consent in the same instant.

a)



b)

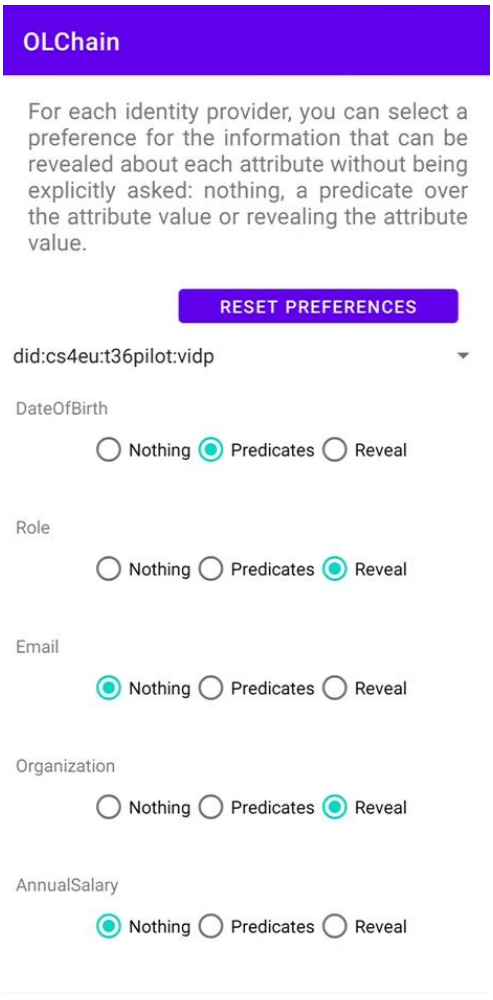


Figure 10. Policy shown to user (a), and screen to configure the verbosity preferences on identity attributes

6.5.2 SYSVER

SYSVER, standing for ``SYSstem VERification, is a software tool that performs a formal analysis based on models of a complex networked system, in order to verify the correct implementation of high-level access control policies. The context in which this tool is used, is one in which a large networked system connects several services and services components provided by different service providers and in which different

types of users/agents need to interact, with different privileges, with the resources (physical and logical) of the system. In this kind of scenario, elements that are considered correct in isolation, could show unexpected behaviours when combined in heterogeneous systems. The focus of the SYSVER asset is exactly at this level of abstraction.

Figure 11 shows the high-level architecture of the tool. A set of formal models compose the inputs of the tool. In particular, models of the system and its resources (both physical and logical) and models of the operating agents are considered and are fed to the core reasoning engine. This module performs an exhaustive analysis approach and combines all the provided inputs in order to build, for each agent, an automaton which includes all the possible sequences of actions that the agent can perform, using his/her initial and acquired knowledge. Further details of the SYSVER architecture are available in the D3.15 deliverable (``Proactive approaches for secure software development").

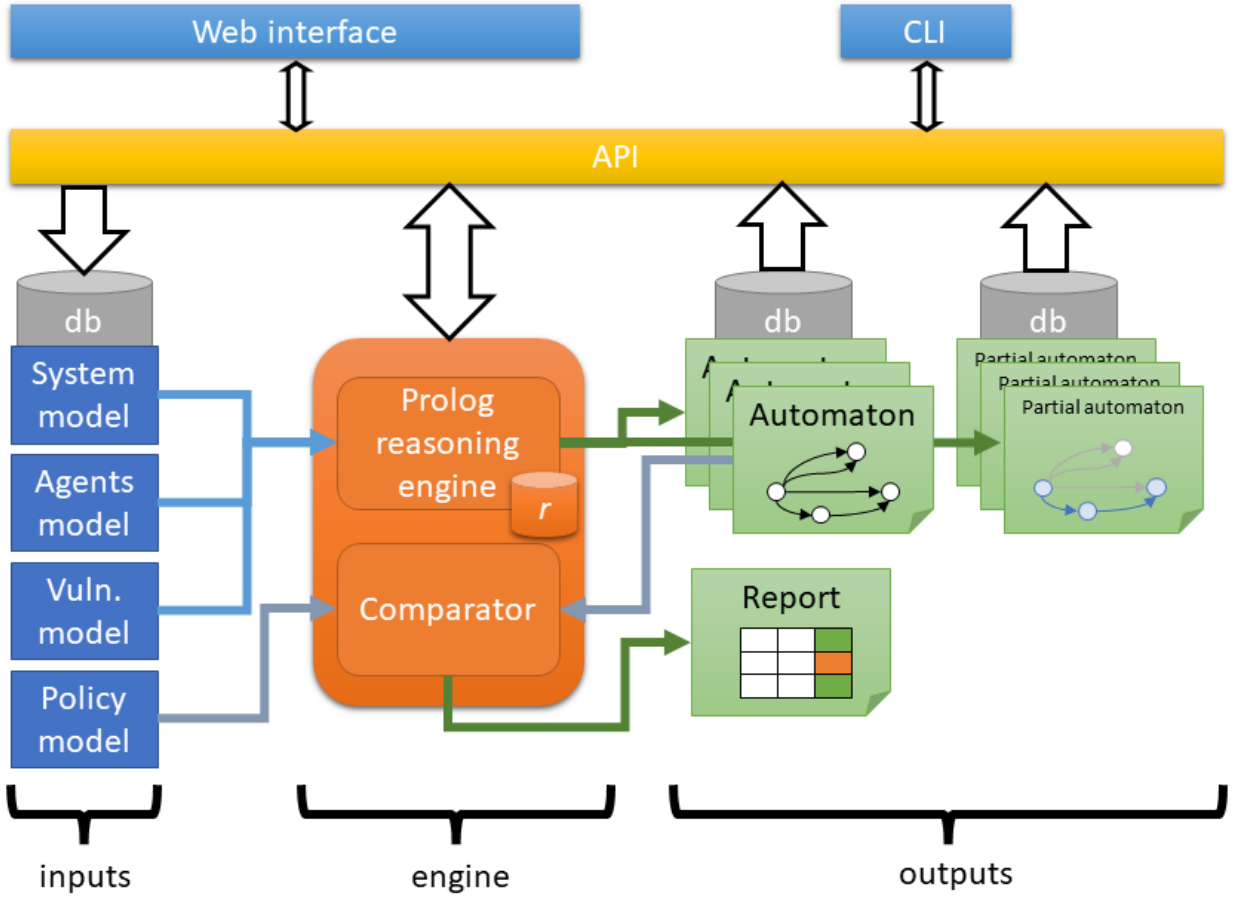


Figure 11. SYSVER architecture

In this deliverable, we focus on a usability issue derived from the exhaustive nature of the analysis performed. The raw provided results (the automata for each user) are typically very large, and although they contain all the required information to understand if the system is correct with respect to the defined access control policy, it is, however, very difficult for the system administrator to effectively grasp the potential policy violations and to imagine how to solve them.

Figure 12 provides an example of the complexity of a produced automaton.

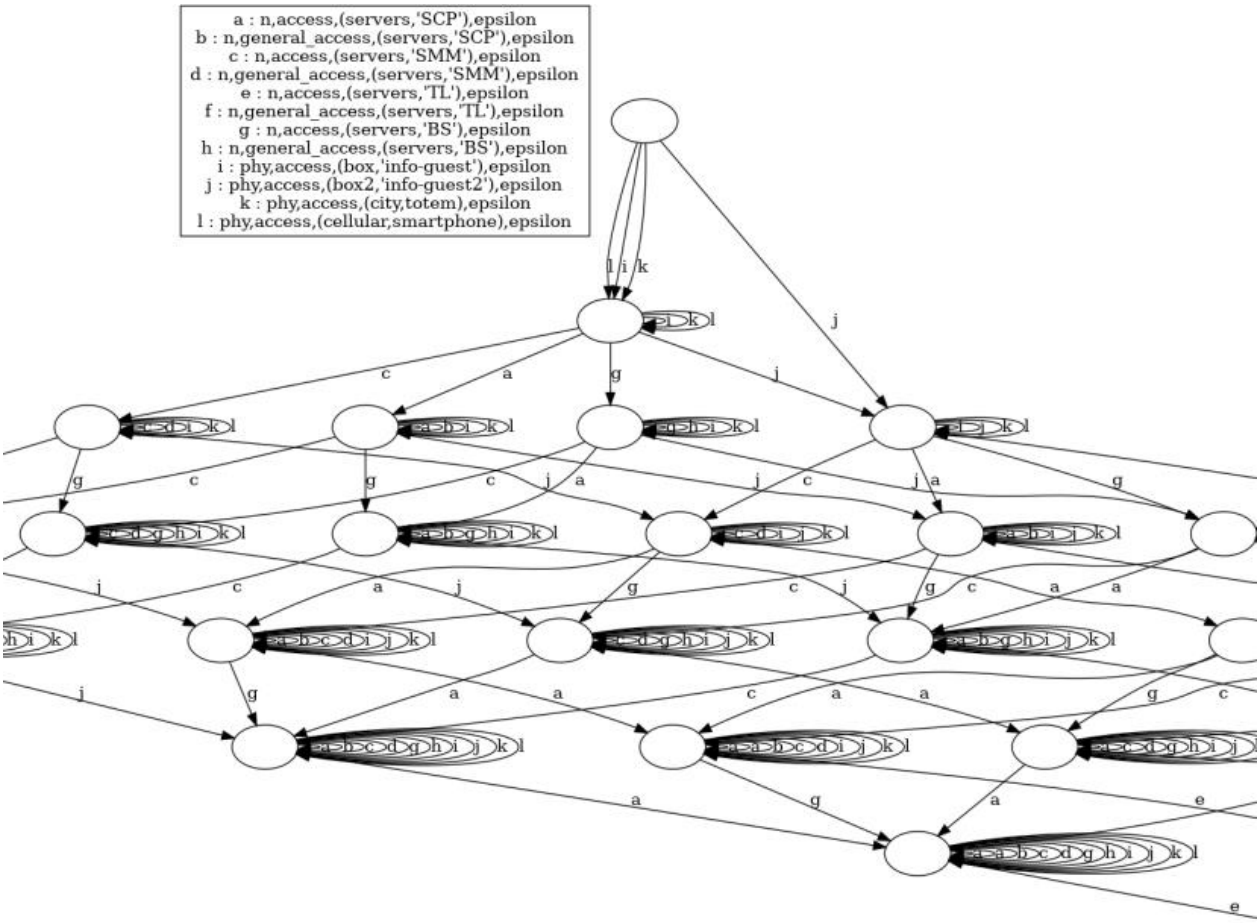


Figure 12. Example of resulting automaton

To mitigate this issue, we followed an approach based on a set of complementary views at different levels of abstractions. The objective here is to hide part of the complexity of the analysis output so as to present only specific aspects that help the administrator choose the correct resolution approach.

The first, and highest, level of abstraction used is a “table” representation where, from each automaton, we collect the set of transition labels that correspond to the set of actions that each agent can perform, in some way. Then we compare this set against the access control policies where each action on specific resources is allowed or denied. This simple analysis allows to report, for each action, if this is correct or a violation of some policy. Then, since this information is not enough for an administrator, to understand *why* the violation was possible, we proceed by building a “minimal” automaton. This kind of structure is built by analysing the automaton extensively while keeping track of the causation relationships between actions and preceding groups of actions. In this way, we provide the administrator with a view of the dependencies between actions. This allows to more effectively identify the most critical paths bringing to a policy violation.

Finally, this last type of graph is further translated into a corresponding set of logical formulas. In fact, alternative paths (ie. sequences of actions) that lead to a critical action can be represented as disjunctions of conjunctions of predicates, representing the satisfaction of action preconditions. This kind of representation

helps the administrator in understanding how to solve the problems identified by the analysis. In particular, since these formulas combine the preconditions of the agent's actions, a specific SYSVER module leverages an SMT solver in order to suggest which set of preconditions to invalidate, in order to block one or more violations. Using specific types of constraints (eg. minimal size of changed precondition set) it is possible to guide the administrator towards a (sub-)optimal resolution of the policy violations.

6.6 Description of integration with DC7

6.6.1 Description of the integration of asset Usable Self-Sovereign PPIdM in DC7

The ppIdM asset is directly integrated with the Smart City platform as a tool for identity management. The Smart City platform has an authorization framework based on XACML, where policies about user identity attributes are established for evaluating requests for access to services and information. If a request is approved, a capability token representing the authorization is generated, and future access to the platform (during the token's lifetime) will be allowed.

For the operation of this system, it is necessary that users are able to present information about their identity in a way that allows the platform to trust that information. In addition, user privacy must be considered. With that in mind, the ppIdM asset is proposed for the task. Users will act as clients of the ppIdM's identity provider, while the Smart City authorization component will act as a relying party, accepting tokens generated from p-ABCs issued by the virtual Identity Provider for user proofs over their identity.

Most related to the usability discussion of this document, users will be able to rely on the developed mobile application for interacting with the services (and, specifically, the platform's authorization framework). Thus, in addition to enjoying the privacy advantages of using the ppIdM asset (minimal disclosure, unlinkability…), they will take advantage of the usability advantages described in the previous section.

6.6.2 Description of the integration of asset SYSVER in DC7

The SYSVER asset has been leveraged in a Smart City scenario, based on the DC7 detailed case, and extended in the D3.15 deliverable ("Proactive approaches for secure software development"). In order to highlight the relevance of the SYSVER approach in the context of a complex system (the Smart City), a more complex networked system has been built upon the elements of the DC7 case. More details are available on the D3.15 deliverable. A quick glance of the considered scenario is provided in Figure 13.

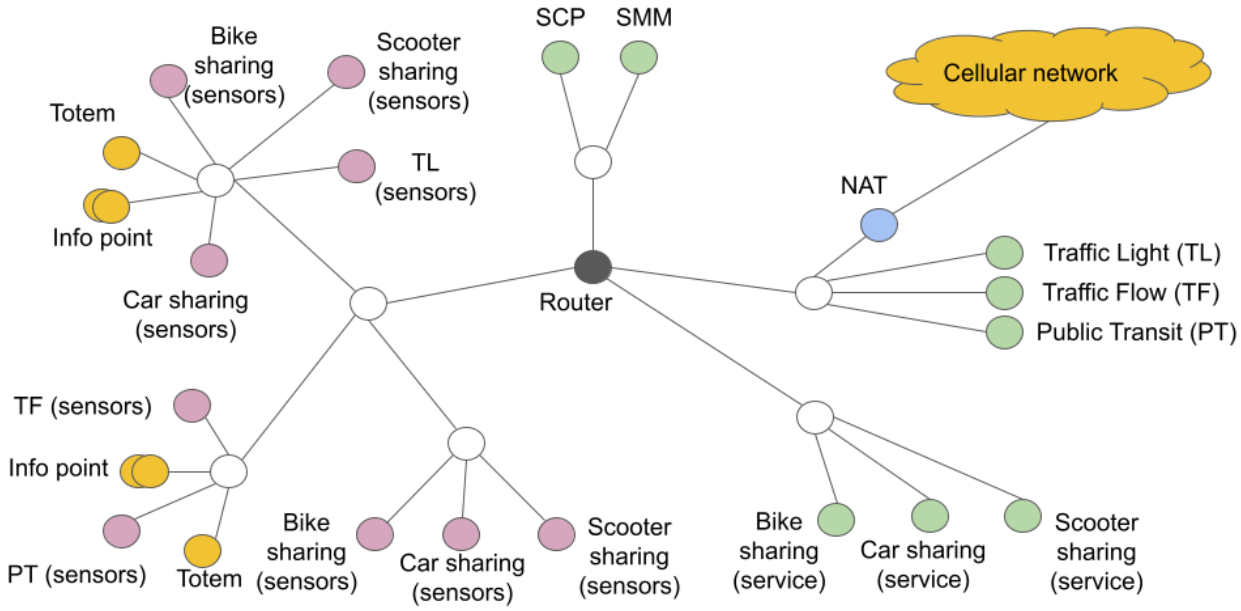


Figure 13. Overview of the DC7 based scenario

This scenario has been successfully analysed in combination with another asset (Polito's VEREFOO) in D3.15, showing how different assets could be used in the context of a Smart City scenario.

Besides the specific Policy Analysis aspect, this kind of integration of the SYSVER asset in the DC7 context has been used to validate the approaches discussed here, so as to improve the usability of the tool and in particular to overcome the obstacle of complex results that cannot be directly manipulated by a human administrator.

7 Integration with External Demonstration Case (Smart Campus)

The Smart University Campus demonstration case provides a common setting and is used to connect all the assets demonstrated in this deliverable. We use the Smart Campus example to engage and integrate all of the assets relevant to T3.6 in one environment. This shows that assets can be used together to support larger solutions with security (they are not tied to the demonstration cases in WP5) while helping make the security more usable, user friendly, and accessible. The Smart University Campus demonstration case is also used for assets that will not be or, as is the case here, have not yet been integrated into the WP5 demonstrator. The asset Guidelines for GPDR Compliant User Experience is therefore integrated and demonstrated in this common demonstration case, in particular for the production of the Data Protection Impact Assessment (DPIA), as required by the GDPR.

7.1 Integration of the asset Guidelines for GPDR Compliant User Experience

7.1.1 Goal and scope

A Data Protection Impact Assessment (DPIA) must be performed before any type of processing is carried out and is an ongoing process that has to be regularly reviewed and brought up to date. The purpose of the DPIA is to systematically analyse, identify and minimise the impact the identified risks could have on the privacy of the data subjects. A finished and properly performed DPIA will also help an organisation evaluate, document, and later show how they comply with all the personal data protection requirements. Here we will prepare a DPIA example based on Slovenian regulations and law. It should therefore be taken as a sample of how such a DPIA could look like, but it should not be blindly applied to other situations.

The DPIA template was already demonstrated in the D3.13; however, we will use a different use case in this demonstration. Additionally, the DPIA template was extended upon in the D3.16. The demonstration in this deliverable will include the content from that addition and will represent a different use case from the demonstration in the D3.13, and therefore give the users of the template a different example to model their own DPIAs on. This is important because the content of the assessment can vary depending on different circumstances, and the same structure is not always necessarily the best for everybody. That is why the template is fairly soft on the structure and encourages users to change, expand, and upgrade the given template to suit their own organisation requirements and circumstances better. This, together with the pre-prepared (and in D3.16 updated) list of potential risks that have to be addressed in the assessment and the self-assessment form for the users to check and evaluate their work, are the main elements that distinguish this template from other similar tools designed to support the process of performing the DPIA. We have discussed other similar tools in D3.11 (Section 3.1.1) and mentioned some additional ones in D4.5 (Section 5.6.1.6).

7.1.2 Part of the demonstration case involved in the integration

The overarching Smart Campus scenario will be the same as in the previous demonstration of the DPIA template (D3.13). However, while there the demonstrated example for this asset was based on the enrollment of students at a university, where the basis for the processing of personal data is the legislation for higher education that dictates the data that must be collected, here we will use an example where the collection of personal data is based on the data owners consent. Specifically, we will produce an example DPIA for collecting personal data in surveys or questionnaires. The need to perform surveys is very general and widely applicable. In our demonstration, we will model the DPIA on a case where a University is collecting personal

data (e.g. name, education, personal experiences in the field of further education, etc.) for the purpose of evaluating current knowledge level and learning focus from individuals who are looking to enrol in special classes for adults. This is not a part of formal education and does not have a legal basis. In this example, the University is the data controller, while individual Faculties that would be performing the surveys are the processors. Because the collection of such data is not legally required, an option is to collect it based on the consent of the participants. The resulting demonstration DPIA should be significantly different from the previous demonstration and not too specific to a certain set of circumstances for it to offer the users a different perspective and an example of the template's use.

7.1.3 State of the Art

There are many other similar free and commercial tools. We have compiled a list of other freely available tools and templates for supporting a DPIA and compared them to our DPIA template in D3.11 (Section 3.1.1) and in D4.5 (Section 5.6.1.6).

7.1.4 Challenge Beyond the State of the Art

Like many other similar tools, the DPIA template also provides the user with guidance on deciding whether a DPIA is necessary and then guiding them through the process of performing and documenting a DPIA. However, what sets this solution apart from others is the pre-prepared (and in D3.16 updated) list of potential risks that have to be addressed in the assessment, together with rules on when some of these risks are not applicable and therefore do not need to be assessed. Additionally, the DPIA template also uniquely includes a self-assessment form for the users to check and evaluate their work. The template is also not hard to adopt and easy to modify to the user's requirements. All of this is done to specifically cater to smaller organizations with fewer resources for performing DPIAs.

7.1.5 Description of the integrated asset Guidelines for GPDR Compliant User Experience

GDPR compliant user experience is an asset and a deliverable D3.6 combined from two sections. The first is the Guidelines for General Data Protection Regulation (GDPR) which presents the regulation's requirements through the GDPR principles. The second part of the enabler is the Data Protection Impact Assessment (DPIA) template. As the name suggests, this part of the enabler can be used to help guide the user through the process of doing a DPIA and also serve as documentation for the performed analysis. It is the DPIA template we will demonstrate in this section.

The DPIA is one of the fundamental mechanisms of the GDPR towards more responsible handling of personal data. The principle of accountability in the GDPR complements the basic principles of personal data protection, and its significance is in preventive action and avoidance of breaches. Violations in the field of personal data protection can have very serious, often irreparable consequences for both individuals and the organisation that process their personal data. In the event of breaches of the law, controllers and processors of personal data can count on negative media coverage, costly and time-consuming corrective actions, high sanctions and loss of trust of their clients. No responsible organisation wants this, and DPIAs are designed to help avoid unwanted consequences.

Regulation (EU) 2016/679 of the European Parliament and of the Council or more commonly known as General Data Protection Regulation (GDPR), is a legal framework that sets guidelines for the collection and processing of personal information. The regulation was designed to strengthen the rights of individuals across the EU and ensure uniform and coordinated action across the Member States. The GDPR has caused a significant amount of panic and confusion among businesses. This can be attributed to multiple factors, such as high fines, applying to all organisations (as long as they process personal data) equally regardless

of size or amount of data they process, often vague or open to interpretation requirements, etc. Therefore, the goal was to create something to help, especially smaller organisations, understand the requirements GDPR demands from them and support them in carrying some of the demanded tasks out.

Guidelines for GDPR Compliant User Experience is a deliverable that was produced as D3.6 in the CyberSec4Europe project. As its name implies, it is a collection of guidelines, best practices and recommendations for achieving GDPR compliance. However, here we will focus on a specific section of the deliverable, which was designed to serve as a template for the process of performing a Data Protection Impact Assessment (DPIA). We will refer to it as the DPIA template. The template is like a to-do list with guidelines on how to perform specific tasks and some pre-prepared structures to support the user. DPIA template is a combination of a guide and pre-prepared content in the form of table templates that personal data controllers can use to perform the DPIA. This solution aims to be primarily of use to the smaller organisations having problems performing or having questions about the assessment's specific steps by giving them a starting point on which they can build.

DPIA is meant to identify and minimise personal data protection risks by systematically analysing the processing of personal data. Unlike most other risk analysis, DPIA is concentrated on the prevention of harm to data subjects, individuals, and overall society rather than the risk to the organisation itself. A DPIA is a legal requirement under the GDPR when the processing is likely to result in a high risk to natural persons' rights and freedoms. This is an excellent example of a condition set by the GDPR for which it is difficult to instinctively know whether it applies or not because there is no definition for "likely to result in a high risk" and the type of issue the enabler is meant to resolve.

The major elements of the DPIA template are presented in Figure 14. The DPIA template aids with the initial decision on the necessity of performing a DPIA. If the circumstances demand the organisation to perform the assessment, then the template describes and provides guidelines for the DPIA steps. The "Conduct the self-assessment" (bottom left former in the figure) is optional and the last step in the DPIA. Before the solution/process can be implemented in the organisation, it is important to also make sure all other GDPR requirements are met, which is the purpose of the more broad GDPR compliant user experience enabler. DPIA template contains all the basic information about the assessment as well as many recommendations and good practices on how to perform it.

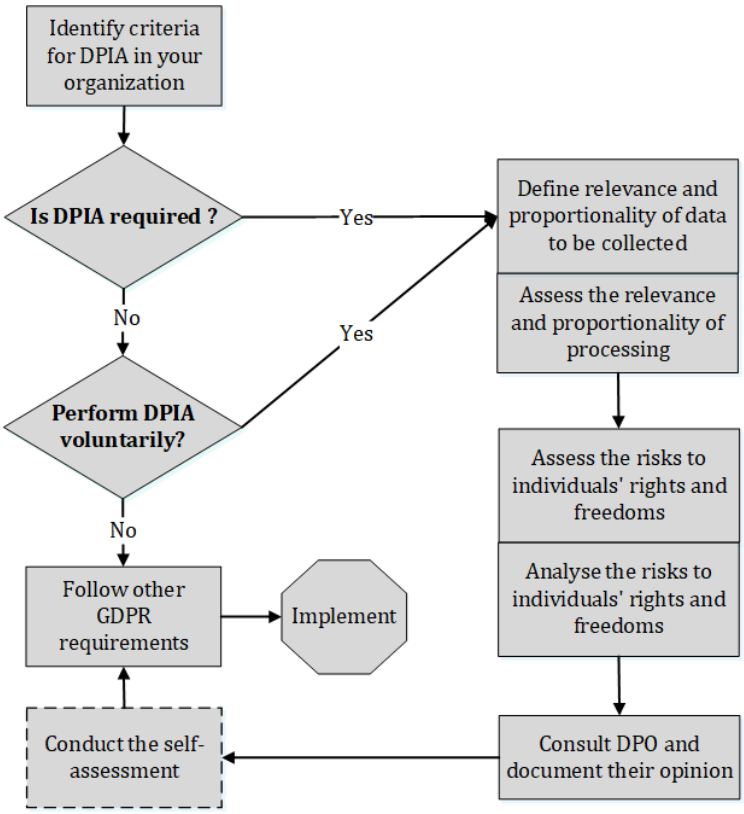


Figure 14. The main steps in the DPIA Template

The first step of performing a DPIA is determining if a DPIA is required. The DPIA template provides a list of criteria based on the GDPR and recommendations given by the Article 29 Working Party and endorsed by the European Data Protection Board. The template requires the users to answer a few questions about the type of processing they intend to perform. Based on the answers, the template enables the user to make an easy judgment about the necessity of the DPIA, given the users' circumstances. This decision process can also be beneficial to show an organisation has performed the DPIA voluntarily. Performing DPIA when not necessary can improve the trustworthiness and reputation of an organisation, assist in ensuring that the best practices for data security and privacy are being utilised, and help minimise the organisation's liability.

The next major component of the DPIA is focused on risks arising from the processing of personal data. The first step is to establish what type of personal data will be processed, whether data processing is proportional/necessary, for how long it will be stored, and on what legal basis it will be collected. From this information, compliance with the GDPR can be determined. The template helps establish compliance levels based on the collected information. The DPIA template provides instructions on how to measure risk based on the severity and probability of threats. The risk assessment methodology is aligned with the ISO 31000:2018 and ISO 31010:2011 and can be directly used to assign risk levels to all identified threats. The DPIA template provides the users with a template to fill this data into, but more importantly, it already includes a long list of personal data processing threats related to the GDPR requirements. The list was additionally updated, and the option to identify irrelevant risks for a given situation was added in D3.16. Users can freely add other threats specific to their organisations, circumstances, used processes, etc. Finally, the risk to individuals' rights and freedoms are evaluated.

GDPR requests that the Data Protection Officer (DPO) provides an opinion on the assessment if one is appointed. The template suggests when a consultation with a DPO might be beneficial. These opinions should be documented.

The final part of the template provides a form for self-assessment. This step of the DPIA is optional and not required by the GDPR. The prepared self-assessment can help organisations track the work they have done and learn from it. Based on their performance, they can improve future work on DPIAs for other processes/services. An example of self-assessment was shown in the previous demonstrator and was not included in this demonstrator.

7.1.6 Description of the integration of the asset Guidelines for GPDR Compliant User Experience

Data Protection Impact Assessment (DPIA) is not always mandatory, but only when it is likely that the type of processing, given the nature, scope, circumstances and purposes of the processing, could pose a significant risk to the rights and freedoms of data subjects. Controllers often encounter a problem with the performance of the DPIA because they do not know what the key elements that a DPIA must contain are. When compiling a DPIA, it is first necessary to determine whether the DPIA is necessary or not. In order to determine whether a DPIA is mandatory, the controller must review the relevant applicable legislation. If the controller does not come from the field of law, this can be difficult. The controller must therefore study the legislation in the field of personal data protection and compare it with their work.

A DPIA must be done when the controller assesses that processing of personal data, even if it is not on the list of cases where DPIA is required, could pose a significant risk to the rights and freedoms of individuals. The requirements for impact assessments are defined in Article 35 of the GDPR. The mere fact that the conditions triggering the obligation to carry out a DPIA are not met does not remove the controller's obligation to take measures to adequately manage the risks to the rights and freedoms of data subjects. In practice, this means that controllers must constantly assess the risks arising from their processing activities in order to determine when a significant risk to the rights and freedoms of individuals might manifest. The aim of the DPIA is to systematically examine new situations that could pose major risks to the rights and freedoms of individuals.

Conducting such a DPIA analysis with the help of a pre-prepared template is much easier. It guides the controller through the entire process in such a way that it does not leave out any steps and produces a complete DPIA. With the help of a pre-prepared template, controllers can quickly identify possible violations, as they often overlook the little things that are crucial to the effective protection of personal data. The template facilitates the creation of DPIA by anticipating details that controllers often omit or do not pay much attention to when protecting personal data. The created template already contains guidelines, on the basis of which the controller will quickly determine whether a DPIA is necessary in their case or not. The template thus saves the controller time required to study and analyse the need to do a DPIA. The template is primarily intended to identify risks in a timely manner and to take appropriate risk management measures to enable controllers to prevent violations of the law. Namely, violations bring financial penalties, the obligation to report detected violations (in certain cases also informing all affected individuals), which can lead to demanding corrective measures, sanctions, negative publicity and loss of trust.

All of this is demonstrated in a full DPIA on an example of collecting personal data from individuals through a questionnaire. Individuals looking to further their education can choose to join afternoon lessons

performed at a university. Before they do that, they have to fill out a survey designed to measure their skill level on the subjects they are looking to continue their education on. Their lessons are then adjusted based on the evaluated skills. The collection of data is done based on consent (the university does not have a legal basis for collecting this data, and depending on how the education is offered, other bases for collection might not be appropriate). The assessment is based on Slovenian legislation; however, the structure and points covered will serve as a good guide and example in any Member State. The example is not meant to be directly applied but as a way to give the users a better understanding of how the template is to be filled out and what they are trying to achieve.

A minor drawback of the template is that different situations might call for minor or even major deviations in conducting a DPIA. The template serves as a basis for all and users themselves must anticipate where their risks are greater and take appropriate measures to protect personal data. The developed template is general and is not adapted to the individual specifics of an individual sector, but it certainly serves as a good tool and a guide on how to professionally tackle conducting a DPIA. The template thus leaves a certain degree of flexibility according to the specifics of each sector. Risks, measures, technology and other circumstances can be very different in individual sectors, but in any case, a pre-made template makes it easier for controllers to conduct a DPIA.

The provided demonstrator of the DPIA documentation for the described scenario can serve more as a blueprint on what anybody using the template should aim to produce using the enabler. It gives the users a better understanding of how the template is to be filled out and what they are trying to achieve. The actual demonstrated DPIA can be found in [44].

7.2 Description of the unified scenario within the Smart Campus Demonstration Case

The unified scenario takes place in a smart campus. There are lots of people around, with different mindsets toward security and privacy and all of them need usable solutions for their everyday tasks. Some parts of the campus are public space, available for everyone, upstanding citizens and malicious actors alike. Other parts are restricted to authorized personnel only. The unified scenario focuses on two main types of users: students and IT services administrators. The scenario is split into two parts, i.e. the two following paragraphs, according to these two roles.

The students authenticate to the university services (e.g. website, smartphone or tablet application). Once identified, the students search for additional courses to register to, or try to use other services enabled by the smart platform. They may wish to join lessons performed at a university that are not part of the main curriculum of their current degree. Before registering, they are asked to fill out a survey designed to measure their skill level on the subjects they are looking to continue their education on. Their lessons are then adjusted based on the evaluated skills.

The IT services administrators of the smart campus are in charge of managing cyber security and privacy policies. For that purpose, they use systems on which they have to be securely identified. Once they are logged in, they can use a set of tools to ensure that security policies are correctly implemented, and also to ensure that privacy and user data protection policies are correctly implemented. Moreover, they can manage incident reporting. Their tools also support them to anticipate potential threats that never occurred, whether their root cause is malicious activities or user errors.

7.3 Description of the possible integration of all of the assets within the unified scenario

In order to support the understanding of the possible integration of all of the assets in the Smart Campus scenario, we illustrate both parts of the scenario, i.e. the students' perspective and the IT admins' perspective in Figure 15. The students identify to the university services using the asset **Usable Self-Sovereign PPIdM** (label S1 in Figure 15), which supports their privacy by disclosing the minimum set of information, ensuring unlinkability, and allowing customization features. In addition, thanks to the asset **Usable Privacy and Identity Management Guidelines**, the privacy notifications they receive (label S2 in Figure 15) will help the students to make informed choices about selective disclosures, i.e. about potential consequences of hiding or showing different attributes.

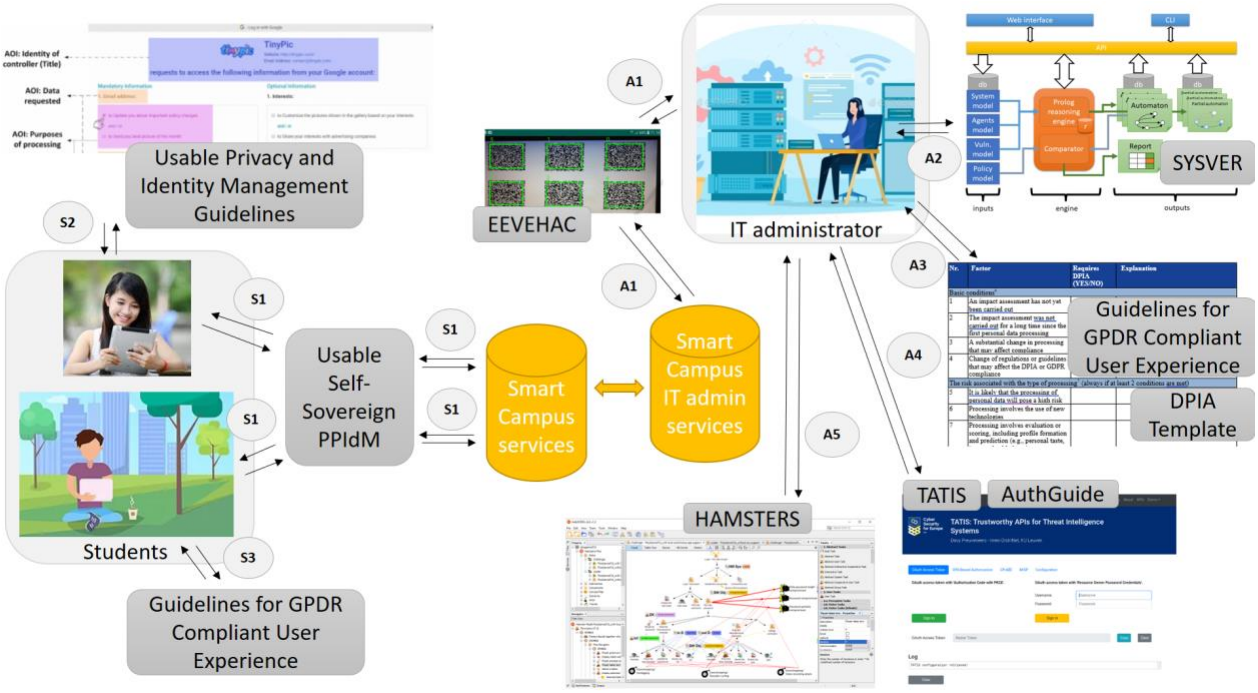


Figure 15. Schematic view on the integration of the T3.6 assets within the Smart Campus unified scenario

Once identified, the students search for additional courses to register to. They wish to join lessons performed at a university that are not part of the main curriculum of their current degree. Before registering, the students are asked to fill out a survey designed to measure their skill level on the subjects they are looking to continue their education on. While the students fill in the form, they feel satisfied because they are informed that the service is GPDR compliant and that the survey has gone through a process for protecting personal data using the asset **GPDR Compliant User Experience** (label S3 in Figure 15).

The IT services administrators of the smart campus authenticate (label A1 in Figure 15) using the multi-factor authentication KeyCloak, which has been extended with **EEVEHAC** in order to increase its usability. The asset **SYSVER** supports the IT services administrators by performing an analysis to check that the implementation of the high-level access control policies is correct and to identify the potential policy violations (label A2 in Figure 15). It also helps them to understand how to solve the problems identified by the analysis. The asset **Guidelines for GPDR Compliant User Experience** support them with identifying

and minimising personal data protection risks by systematically analysing the processing of personal data (label A3 in Figure 15). It helps with identifying possible violations of GPDR and ensures efficient and effective compliance with the regulation for the data processors. It also provides a template, which facilitates the creation of DPIA, with a special focus on identifying and evaluating data processing risks. The asset is useful for IT service designers and developers, but it ultimately helps protect individuals' personal data. The asset **TATIS** helps them to manage incident reporting (label A4 in Figure 15). The asset **AuthGuide** supports them in the creation of an MFA authentication configuration and workflow to protect the incident reporting platform (label A4 in Figure 15). The asset **HAMSTERS** supports the IT services administrators to identify a list of concrete threats as well as a list of possible concrete human errors that could happen given the tasks that have been identified and described in the task model (label A5 in Figure 15).

8 Conclusion

We presented how the T3.6 assets have or can be integrated into WP5 demonstration cases, which is one of the project's goals. We also presented how we envision the integration of all of the T3.6 assets in a unified smart campus scenario.

In this deliverable, we have presented the process that we applied to identify integration possibilities and select the most relevant ones. Then, for each demonstration case, we presented the integrations that have been actually performed, or are going to be performed, or could be performed at the conceptual level. In the case of the integration that has been performed, we presented the results of the integration. The results of this integration work are:

- For demonstration case 3, a set of conclusions on how privacy notifications can enhance usable transparency in the context of privacy and identity management and to what extent the cultural context and other parameters (demographics, usage characteristics, the option for intervenability, and modality of privacy notifications) can have an impact on their perceived usefulness.
- For demonstration case 4, a proposal for the combination of the authentication methods TATIS, AuthGuide, Keycloak and EEVEHAC to protect the MISP incident reporting platform.
- For demonstration case 5, an extension of the MITIGATE maritime risk management method to identify additional threats by including task modelling in the risk assessment process of the method.
- For demonstration case 7, a usable identity management user interface for smartphone users in smart cities, and a user centered tool to support the security analysis of smart cities.
- For the smart campus demonstration case, a user centered template to support IT services to manage the GPDR compliance when collecting user data on a smart campus.

At last, we presented the envisioned unified scenario to integrate all of the T3.6 assets. The unified scenario was the opportunity to go deeper in the understanding of the interplay of the T3.6 assets. This scenario complements the overview on the T3.6 assets presented in the deliverable “D3.16 Security Requirements and Risks Conceptualization”. In this overview, the T3.6 assets are classified according to layers: analysis, user and guidance. A T3.6 asset may support to analyse security or usability of a security mechanism (analysis layer), to use an asset in a secure and usable way (user layer), or to be guided while using an asset (guidance layer). The unified scenario provides additional information by highlighting how the assets inter-connect and inter-execute in a concrete application domain, and this for concrete and different types of users. It is the opportunity to exemplify how the T3.6 assets can support end users tasks, as well as IT systems administrators’ tasks.

The integration of the T3.6 assets within the WP5 demonstration cases is one of the objectives of the CyberSec4Europe project. This integration effort enabled to consolidate collaborations within the consortium, but also to initiate additional collaborations.

9 References

[1] B. Liu, M.S. Andersen, F. Schaub, H. Almuhimedi, S.A. Zhang, N. Sadeh, Y. Agarwal, A. Acquisti, Follow my recommendations: A personalized privacy assistant for mobile app permissions, in: Proc. of the Symposium on Usable Privacy and Security, 2016.

[2] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L.F. Cranor, Y. Agarwal, Your location has been shared 5,398 times! a field study on mobile app privacy nudging, in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2015.

[3] D. Wu, G. Moody, J. Zhang, P. Lowry. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention Inf. Manag., 57 (5) (2020).

[4] P. Murmann, D. Reinhardt, S. Fischer-Hübner, To be, or not to be notified – eliciting privacy notification preferences for online mhealth services, in: Proc. of the Int. Conf. on Information Security and Privacy Protection, 2019.

[5] P. Murmann, M. Beckerle, S. Fischer-Hübner, and D. Reinhardt. Reconciling the What, When and How of Privacy Notifications in Fitness Tracking Scenarios. Pervasive and Mobile Computing, 77:101480, 2021.

[6] EU Commission. Special Eurobarometer 487a – The General Data Protection Regulation. Technical report, 2019.

[7] G. Hofstede and G.-J. Hofstede. Lokales Denken, globales Handeln: Interkulturelle Zusammenarbeit und globales Management. Deutscher Taschenbuch Verlag, 2006.

[8] Hofstede Insights. https://www.hofstede-insights.com/country-comparison/austria,germany,switzerland,the-uk/ , accessed 06/2021, 2021.

[9] S. Trepte, L. Reinecke, and Nicole B. et A. Ellison. A cross-cultural perspectiveon the privacy calculus.Social Media+ Society, 3(1), 2017.

[10] P. Grassi, R. Perlner, E. Newton, A. Regenscheid, W. Burr, J. Richer,N. Lefkovitz, J. Danker, and M. Theofanos. Digital identity guidelines: Authen-tication and lifecycle management [including updates as of 03-02-2020], 2017-12-01 2017.

[11] M. Naor and A. Shamir, "Visual cryptography," in Workshop on the Theory and Application of of Cryptographic Techniques, 1994, pp. 1–12.

[12] A. G. Forte, J. A. Garay, T. Jim, and Y. Vahlis, "EyeDecrypt—Private interactions in plain sight," in International Conference on Security and Cryptography for Networks, 2014, pp. 255–276.

[13] H.-C. Hsiao et al., "A study of user-friendly hash comparison schemes," in 2009 Annual Computer Security Applications Conference, 2009, pp. 105–114.

[14] A. Boldyreva, S. Chen, P.-A. Dupont, and D. Pointcheval, "Human computing for handling strong corruptions in authenticated key exchange," in Computer Security Foundations Symposium (CSF), 2017 IEEE 30th, 2017, pp. 159–175.

[15] M. Blum and S. Vempala, "The complexity of human computation via a concrete model with an application to passwords," Proc. Natl. Acad. Sci., vol. 117, no. 17, pp. 9208–9215, 2020.

[16] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," Comput. & Secur., vol. 88, p. 101619, 2020, doi: https://doi.org/10.1016/j.cose.2019.101619.

[17] P. Grassi et al., "Digital Identity Guidelines: Authentication and Lifecycle Management [including updates as of 03-02-2020]." Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2017, doi: https://doi.org/10.6028/NIST.SP.800-63b.

[18] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, "Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood," in Proceedings of the 13th International Conference on Availability, Reliability and Security, {ARES} 2018, Hamburg, Germany, August 27-30, 2018, 2018, pp. 39:1--39:9, doi: 10.1145/3230833.3234514.

[19] D. Preuveneers and W. Joosen. Tatis: Trustworthy apis for threat intelligence sharingwith uma and cp-abe. In A. Benzekri, M. Barbeau, G. Gong, R. Laborde, and J. Garcia-Alfaro, editors,Foundations and Practice of Security, volume12056, pages 1–17. Springer International Publishing, 6 2020.

[20] D. Preuveneers, W. Joosen, J. B. Bernabe and A. Skarmeta. Distributed security framework for reliable threat intelligence sharing. Security and Communication Networks, 2020, 2020.

[21] D. Preuveneers and W. Joosen. Sharing machine learning models as indicators of compromise for cyber threat intelligence. Journal of Cybersecurity and Privacy, 1(1), 140–163, 2021.

[22] P. Grassi, R. Perlner, E. Newton, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker and M. Theofanos. Digital identity guidelines: Authen-tication and lifecycle management [including updates as of 03-02-2020], 2017-12-01 2017.

[23] J. Hekkala, S. Nikula, O. M. Latvala and K. Halunen. Involving humansin the cryptographic loop: Introduction and threat analysis of EEVEHAC. In 18th International Conference on Security and Cryptography, SECRYPT 2021, pages 659–664. SciTePress,2021.

[24] European Maritime Safety Agency EMSA. Analysis of marine casualties and incidents involving container vessels. v1.0. safety analysis of emcip data. September 2020.

[25] International Maritime Organization (IMO). (2017). Guidelines on Maritime Cyber risk management. MSC-FAL.1/Circ.3, 5 July 2017.

[26] National Institute of Standards and Technology (NIST). Guide for conducting risk as-sessments. NIST Special publication 800-30 Revision 1, September 2012.

[27] E-M Kalogeraki, D. Apostolou, N.Polemi, and S.Papastergiou. (2018) Knowledge management methodology for identifying threats in maritime logistics supply chains, Knowledge Management Research & Practice, 16:4, 508-524, DOI:10.1080/14778238.2018.1486789

[28] Y.C. Yang. Risk management of Taiwan's maritime supply chain security, Safety Sci-ence, Volume 49, Issue 3, 2011, Pages 382-393, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2010.09.019.

[29] C.H Chang, J.Xu and D.P. Song. An analysis of safety and security risks in container shipping operations: A case study of Taiwan, Safety Science, Volume 63, 2014, Pages 168-178, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2013.11.008.

[30] M. Evans, Y. He, L. Maglaras and H. Janicke. HEART-IS: A novel technique for evaluat-ing human error-related information security incidents, Computers & Security, Volume 80, 2019, Pages 74-89, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.09.002.

[31] J. Boender, M. G.Ivanova, F.Kammüller and G.Primiero. Modeling Human Behaviour with Higher Order Logic: Insider Threats, 2014 Workshop on Socio-Technical Aspects in Security and Trust, 2014, pp. 31-39, doi: 10.1109/STAST.2014.13.

[32] I. Garbacz, R. Giustolisi, K. Møller Nielsen and C. Schuermann. (2021) A Security Analysis of the Danish Deposit Return System. In: Groß T., Tryfonas T. (eds) Socio-Technical Aspects in Security and Trust. STAST 2019. Lecture Notes in Computer Science, vol 11739. Springer, Cham. https://doi.org/10.1007/978-3-030-55958-8_7

[33] C. Martinie, P. Palanque, E. Bouzekri, A. Cockburn, A. Canny and E. Barboni. Analysing and demonstrating tool-supported customizable task notations.volume 3, New York, NY, USA, June 2019. Association for Computing Machinery.

[34] C. Martinie, P. Palanque and M. Winckler. Structuring and composition mechanisms to address scalability issues in task models. volume 6948, Berlin, 2011. Springer.

[35] J. Reason.Human Error. Cambridge University Press, 1990.

[36] R. Fahssi, C. Martinie and P. Palanque. Enhanced task modelling for sys-tematic identification and explicit representation of human errors. volume 9299. Springer,Cham, 2015.

[37] N. Broders, C. Martinie, P. Palanque, M. Winckler and K. Halunen. A generic multimodels-based approach for the analysis of usability and security of authen-tication mechanisms. volume 12481, pages 61–83, 2020.

[38] European Union Agency for Cybersecurity ENISA. Threat taxonomy. 2016.

[39] N. Polemi and P. Kotzanikolaou. Medusa: A supply chain risk assessment methodology.Cyber Security and Privacy. Communications in Computer and Information Science, page79–90, 2015.

[40] International Standard Organisation ISO. ISO/IEC 27001:2013, information technology - security techniques - information security management systems- requirements, edition 2. October 2013.

[41] A. A. Jabal et al., Methods and Tools for Policy Analysis, ACM Comput. Surv., vol. 51, no. 6, 2019, doi: 10.1145/3295749.

[42] F. Valenza, C. Basile, D. Canavese, and A. Lioy, Classification and Analysis of Communication Protection Policy Anomalies, IEEE/ACM Trans. Netw., vol. 25, no. 5, pp. 2601–2614, 2017, doi: 10.1109/TNET.2017.2708096

[43] J. B. Hong, D. S. Kim, C.-J. Chung, and D. Huang, A survey on the usability and practical applications of Graphical Security Models, Comput. Sci. Rev., vol. 26, pp. 1–16, 2017, doi: https://doi.org/10.1016/j.cosrev.2017.09.001

[44] Addendum to D3.17 – Survey Data Protection Impact Assessment, https://cybersec4europe.um.si/Addendum to D3.17 – Survey Data Protection Impact Assessment.pdf, accessed in November 2021.